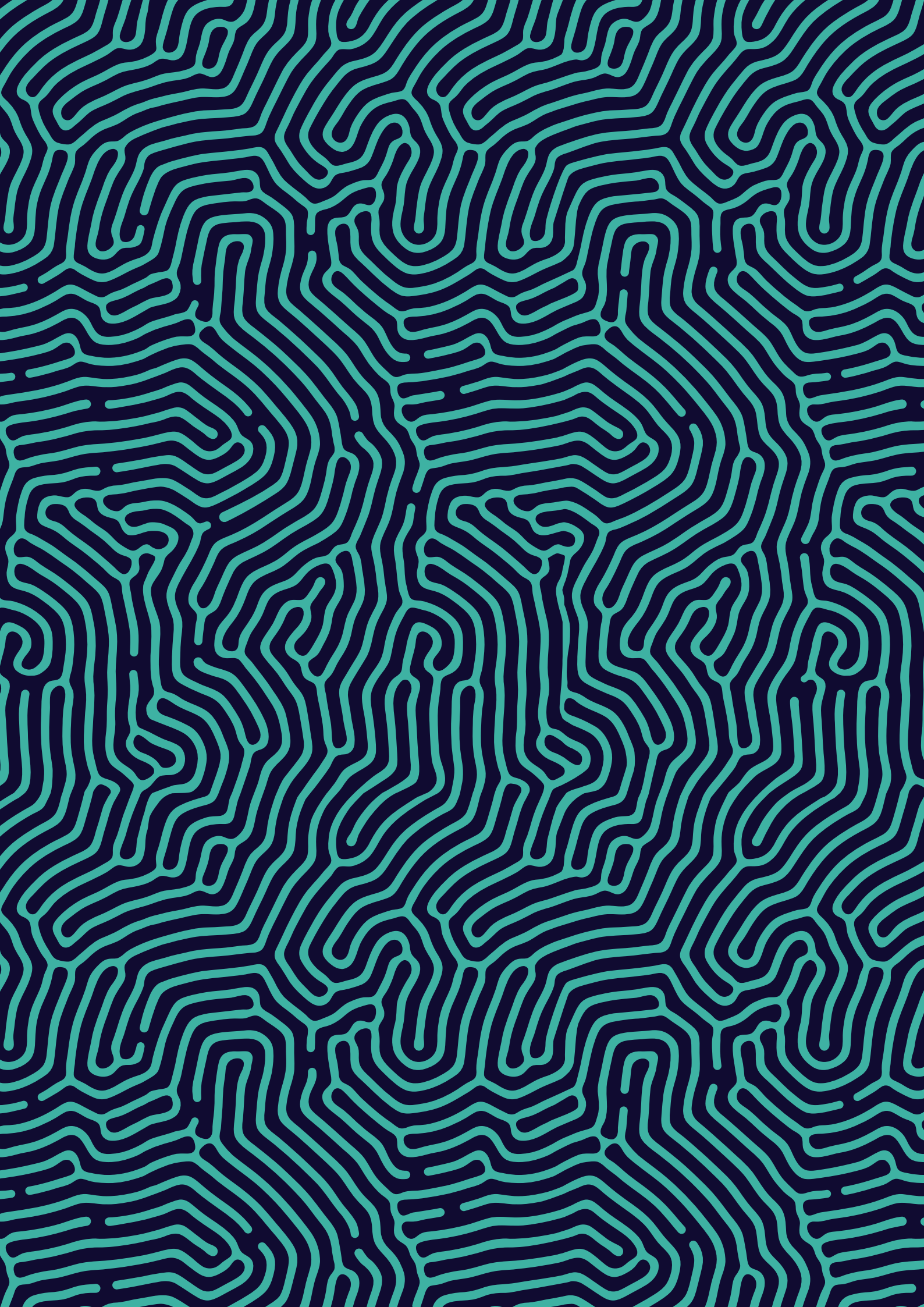
Global Internet Report 2016

Internet Society

Global Internet Report 2016

Table of contents

Note to the reader:
The definition of the green words can be found at the end of the report



Foreword

We are acutely aware of how the Internet impacts and transforms the world. It has the ability accelerate human progress, bridge the digital divide and build societies that drive innovation, entrepreneurship, and progress.

Today we are at a defining moment in the evolution and growth of the Internet.

Large-scale data breaches, uncertainties about the use of our data, cybercrime, surveillance and other online threats are eroding users' trust and affecting how they use the Internet. Eroding trust is also affecting the way governments view the Internet, and, is shaping the policy environment for the Internet around the world..

We face a situation where we risk undoing all of the progress we have made over the past three decades.

It is time to act.

In the 2016 Global Internet Report, we take a close look at data breaches, offer approaches to help prevent them, and how these measures will positively impact user trust and the global digital economy.

We approach the issue through an economic lens, and ask the hard question: Why are organisations not taking all available steps to protect those who entrust them with their personal information? We also explore market failures and their impact on organisations' data security.

We provide five clear recommendations for a path forward to address the increasing incidence and impact of data breaches.

We highlight that 'your breach is my breach' and that security is only as good as the weakest link. Whether a contractor, a client or someone else, one organisation's poor security could open the door for data breaches in other organisations. On the Internet, everyone is connected. Far too often, information stolen from one organisation is later used to breach another organisation's security. Thus, we have a collective responsibility to secure the data ecosystem, to protect not only ourselves but also the global Internet that we all depend on.

Through it all, we land on an overriding approach. One that puts Internet users at the heart of the solutions.

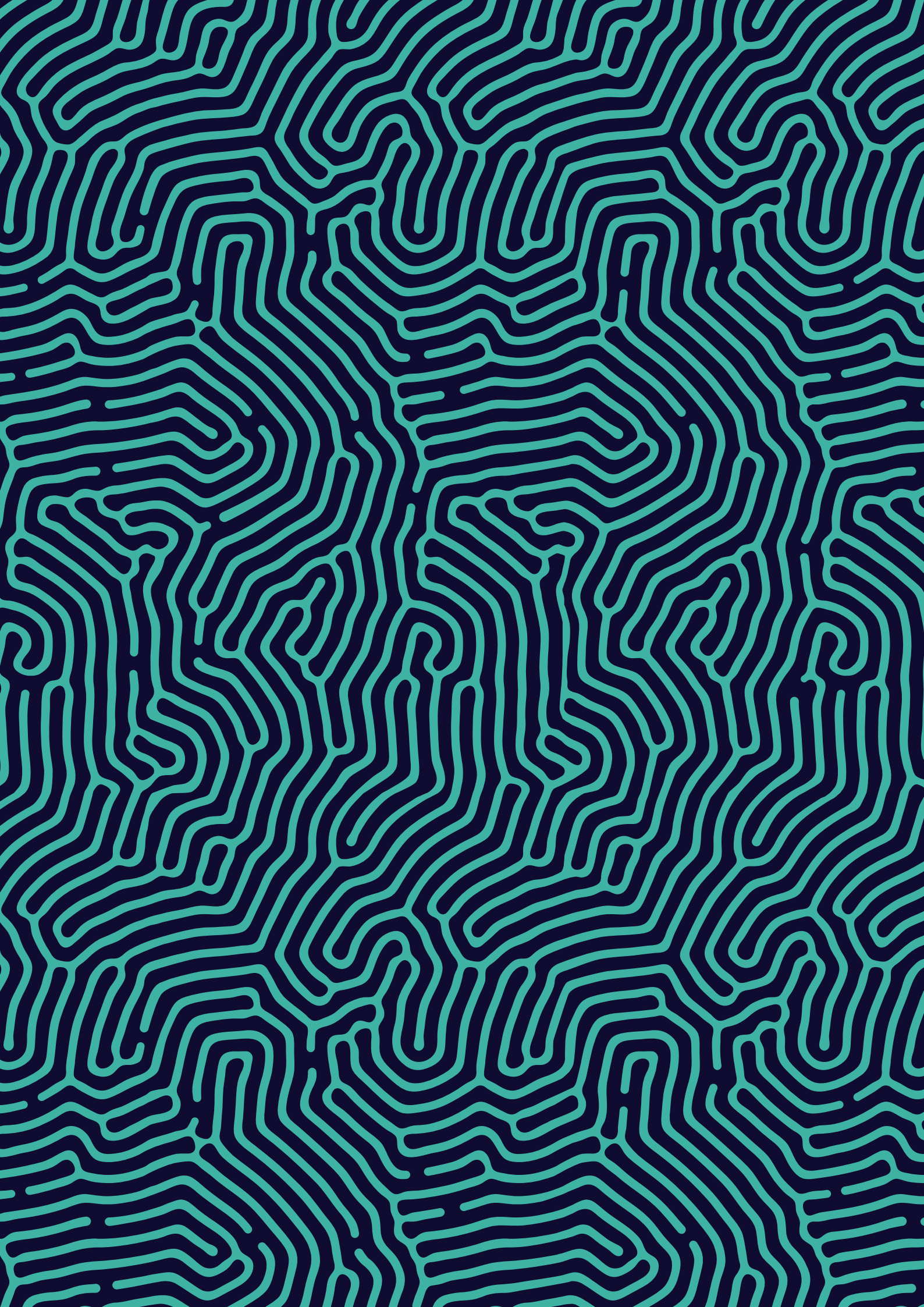
If there is a message that needs to be conveyed, it's that a trusted Internet is not achieved by a single treaty or piece of legislation; it is not solved by a single technical fix, nor can it come about because one company, government or individual decides security is important.

By providing an in-depth analysis and recommendations on how to better prevent and mitigate data breaches, this report offers some concrete steps that will contribute rebuilding trust online.

The promise of the digital economy - one that will bring innovation, growth and social prosperity - will not be met without an open, trusted Internet.

The responsibility lies with all of us and it's one we can take on together.

Kathy Brown
President and CEO
Internet Society



Acknowledgements

Author's Notes and Acknowledgements

It is with great pleasure that I introduce this third edition of the Global Internet Report, covering the economics of data breaches. There have been a regular stream of data breaches in the news – many for financial gain, some to simply to demonstrate hacking prowess, and recently, targeted to impact current events - the US presidential election and world sport. The report aims to identify the causes of the breaches and, through an economic lens, present recommendations for increasing data security.

This topic clearly sits within one of the Internet Society's two overarching goals, to promote and restore trust in the Internet. However, there is also a relation to the other goal – connecting the unconnected – because without trust in the Internet, those not yet online may find another reason to stay offline.

Like many of us, I bring personal experience to this topic, as one of my relatives was a customer of TalkTalk (the British broadband provider), and I was visiting when its latest and largest breach was announced. In trying to help, I shared in the frustration and uncertainty that these breaches create in users. Luckily, in this case, there was no long-term cost, other than the time needed to switch ISPs.

I can only imagine the dread felt by US government employees when they learned their confidential employment records had been obtained by unknown hackers, the embarrassment felt by Sony executives whose emails were read worldwide, or even the panic of Ashley Madison customers that their spouse would discover their affairs. The financial and non-financial cost of these and other breaches, all described in the report, may never be fully known.

In light of the profound impact of breaches on users, the greatest surprise for me in researching the report was how little users' interests played a part in studies on breaches. The studies tended to focus on the technical explanations for breaches, and the cost to organisations who have been breached. Users' direct costs from the breach are usually included, of course, and their business may be understandably lost. But there is little study of the short-term costs imposed on users in time and money of making their claims, the long-run risk and impact of identity theft resulting from the breach, or the non-financial harm. One of the goals of the report is to put users at the centre of the approach to tackling data breaches.

The other surprise for me was that more breaches are preventable than I had initially thought, yet at the same time a determined hacker can even breach the systems of companies whose own business is to provide data security solutions.

This leads to the two parallel questions the report seeks to answer. First, why more steps are not taken to prevent the preventable data breaches, and second, why more steps are not taken to mitigate the impact of the data breaches that do occur. Patches for known bugs are not always implemented; appropriate anti-malware software is not always used; too much personal information may be collected and stored; and it is often not encrypted.

The two questions are answered by examining the economic market failures that explain the current situation, and identifying the economic incentives to reduce the number and impact of data breaches.

The report is not a technical playbook for how to prevent a data breach; nor is it an economics textbook. Rather, it draws on examples we can all relate to. We do not have to be engineers to understand the challenges of passwords and updating our systems, and we do not have to be economists to understand how we respond to economic incentives such as lower costs or increased benefits.

I would like to thank Kathy Brown, Sally Wentworth, Olaf Kolkman, and Raúl Echeberría for their leadership and support for this report. Christine Runnegar provided valuable and insightful input on every draft of every section, along with Olaf Kolkman, Constance Bommelaer, Konstantinos Komaitis, Andrei Robachevsky, and Ryan Polk.

Special thanks and acknowledgements are owed to Christine Runnegar, who led the Internet Society steering committee for the development of the report. Christine leads the Internet Society's policy agenda on Internet trust, championing privacy for Internet users, and her work was an important input to the development of this report.

The report benefitted from two working groups that provided input throughout the development of the report. First, an internal Internet Society working group included Wende Cover, Noelle Francesca de Guzman, Lia Kiessling, Shernon Osepa, Maarit Palovirta, Bastiaan Quast, Karen Rose, Nicolas Seidler, Robin Wilton, Dan York, and Fernando Zarur.

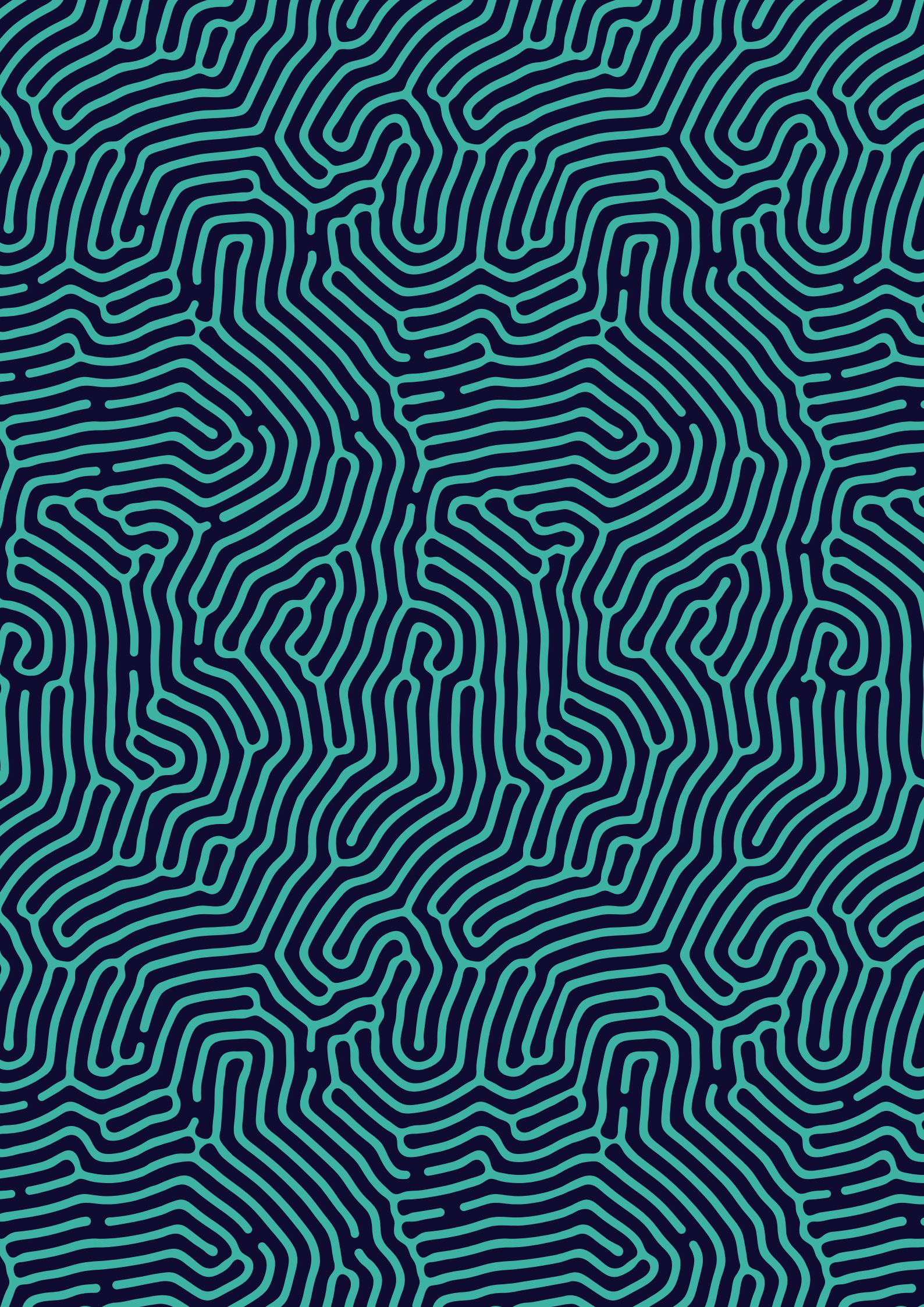
Another external group was formed from members of ISOC's Organization Members Advisory Council and Chapters Advisory Council, consisting of Nadira Alaraj, Babu Ram Aryal, Nabil Bukhalid, Jeff Brueggeman, Olga Cavalli, Olivier Crepin-Leblond, Glenn Dean, Avri Doria, Richard Hill, Scott Mansfield, Cheryl Miller, Douglas Onyango, Christoph Steck, Rudi Vansnick, David Vyorst, along with Joyce Dogniez, Ted Mooney and Carly Morris from the Internet Society.

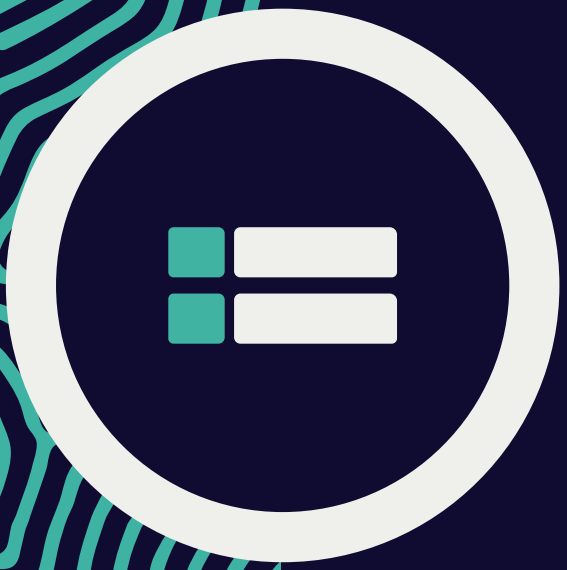
Both groups demonstrated, yet again, the depth and breadth of commitment and knowledge of the Internet Society's staff and membership, and their insight and knowledge is felt on every page of the report. We note that the views expressed in the report do not necessarily reflect the opinions of the members of the external working group.

I would also like to thank the communications team, including James Wood, Wende Cover, Allesandra de Santillana, Beth Gombola, Lia Kiessling, and Jairus Pryor, as well as Lincoln McNey, Henri Wohlfarth and Brenda Boggs from the IT team, for all their help in putting the report together and online, and organising the launch. And thanks to Erin McGann and Michele Robichaux for expert editing.

Finally, thanks to Blossom Communications for their beautiful interpretation of the new Internet Society brand in the report design, and development of the printed and online versions of the report. The Internet Society would also like to thank Telia Carrier for their sponsorship of the work of Blossom Communications.

Michael Kende
Senior Fellow
Internet Society





Executive Summary

Introduction

Data breaches are on the rise. The impact of data breaches on users – consumers, employees and organisations is profound and lasting, including significant financial and non-financial costs. Even worse, in many cases the data breach could have been prevented. And, even if it could not have been prevented, the harm could have been mitigated.

So the issue at the heart of this report is, in some ways, a simple one.

Why are organisations not taking all available steps to protect those who entrust them with their personal information? Is it because they do not bear all the costs of the data breaches? Is it because there is not enough benefit to them in better protecting their users' data? The answer to both questions is yes.

While users bear the lasting costs of each breach, the ultimate casualty is trust in the Internet. The vision of the Internet Society is that the Internet is for everyone, everywhere. Trust in the Internet is at the core of that vision. Without trust, those online are less likely to entrust their personal information to the Internet, and, those who are not yet online will have a reason to stay offline. The Internet economy will not grow as fast as it could, and the UN Sustainable Development Goals (SDGs) will be that much harder to achieve.

With this report, the Internet Society seeks to increase awareness on the topic of data breaches and our collective responsibility to help secure the data ecosystem. We make recommendations on how to reduce the number and impact of data breaches. Fundamentally, users should be at the centre of the discussion, as they are the ultimate victims of breaches. Their trust must be won and kept to help the Internet meet its full promise for everyone.

Data and Trends

Data breaches are trending upwards:

- A growing number of people are impacted by data breaches. Reported breaches are increasing, with a rising number of known records breached and even more that are unknown in number. The leading cause is outside attacks, mostly for financial gain. Most breaches appear to occur in the US, but that is likely because of data breach notification rules that lead to more disclosure.

- Surveys do not as yet indicate that reported data breaches are having a significant impact on non-users' willingness to go online. However, as more users are impacted by data breaches, such as by having their identity stolen for profit, more users will hesitate to use online services requiring personal information. They may also stop doing business with a company that has been breached. A widening breach of trust among users, in turn, could provide non-users with a reason not to go online.

- Organisations are spending more on prevention, but this has not yet noticeably lowered the number of breaches, or the impact and cost of breaches when they do occur. In turn, the cost of breaches, when calculated, typically only include the cost to the organisation, and not the full cost for the users who were the ultimate victims of the breaches.

These trends cannot be allowed to continue without significant harm to individuals' privacy and users' trust in the Internet, resulting in lower and more selective use of the Internet.

Case studies

The report highlights some leading causes of data breaches, and their impact on organisations and users. The numbers are staggering: Target had 40 million customers' credit card numbers stolen and put on sale online; Ashley Madison's records on 37 million married users and their personal affairs were taken and published online; and the US Office of Personnel Management had records on 21.5 million past, present, and potential employees, stolen.

The impact of these breaches on consumers, users, employees and third parties who did not even know the organisations had their data is profound and lasting. Some users lost time and money protecting their finances and their identity from theft, some saw their marriages dissolve, and even committed suicide, and others may be subject to blackmail and exposure.

The case studies show how easy some attacks are, but also how difficult it is for organisations to protect against all threats. For users, the case studies highlight the increasing sense of insecurity online, requiring trust in organisations whose security users could not possibly assess. An ever increasing number of users have been directly or indirectly impacted by a data breach. The case studies make concrete the real and ultimate impact of these breaches on the users whose trust in organisations, as consumers or employees, is betrayed.

Issues

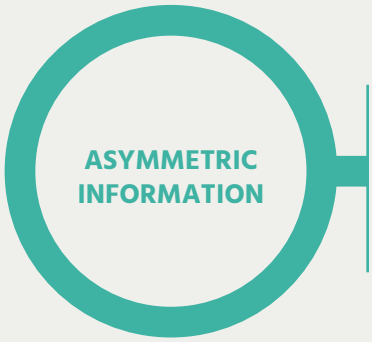
In the face of financial and non-financial costs highlighted by the data and case studies, it is puzzling that many of these breaches exploited known vulnerabilities, and were preventable. For some of these, there were patches available, but not used. Some involved social engineering attacks, in which employees were tricked into giving up their password or introducing an infection, typically in ways that could be prevented.

Of course, not all breaches result from attacks, and not all attacks are preventable. Some are the result of attacks using zero-day exploits not known before being employed. Others result from accidental disclosure of data, for example through the loss of a device containing sensitive data. While not preventable, given how common they are, such breaches are at least foreseeable. It is possible to mitigate the impact, by minimising the amount of data gathered, and encrypting the data that is stored and sent.

The question remains why, given the cost of breaches, more is not done by organisations to address the preventable ones, and to lower the cost and impact of foreseeable ones? This raises the issue of the economics of trust.

There is a market failure that governs investment in cybersecurity. First, data breaches have externalities; costs that are not accounted for by organisations. Second, even where investments are made, as a result of asymmetric information, it is difficult for organisations to convey the resulting level of cybersecurity to the rest of the ecosystem. As a result, the incentive to invest in cybersecurity is limited; organisations do not bear all the cost of failing to invest, and cannot fully benefit from having invested.

The breached organisation does not bear all of the costs of the breach – the cost borne by others is an externality that does not necessarily factor into its decisions on how to protect against data breaches. Further, the weight of data breaches impacts future trust, which is an externality, and from an economic perspective, there is no rational reason for organisations to account for this. However, this is an impact society cannot neglect.



Stakeholders do not have full information about the risks they may face online, making it difficult to take informed decisions. In particular, it is hard for organisations to benefit from taking the right steps to avoid data breaches, because they cannot convey their level of data security to customers. This limits the incentive to invest in data security.

Recommendations

The report highlights five recommendations for addressing the issues raised regarding the economics of data breaches.

R1 Put users at the centre of solutions; and include the costs to both users and organisations when assessing the costs of data breaches.

R2 Increase transparency through data breach notifications and disclosure.

R3 Data security must be a priority. Better tools and approaches should be made available. Organisations should be held to best practice standards when it comes to data security.

R4 Organisations should be accountable for their breaches. General rules regarding the assignment of liability and remediation of data breaches must be established up front.

R5 Increase incentives to invest in security by catalysing a market for trusted, independent assessment of data security measures.

The *first recommendation* is to put users at the centre of the solutions. As a way to kick-start this user-focused approach to data breaches, our second recommendation is to create increased transparency about the risk, incidence and impact of data breaches globally.

With increased awareness comes increased demand for better tools. Our *third recommendation* is that data security must be a priority. Better tools and approaches should be made available. Organisations should be held to best practice standards.

- **Prevention.** To avoid known vulnerabilities, security tools should be easier to use and update, including critical security patches. To prevent social engineering attacks, organisations should apply trusted tools and best practices to block phishing emails and embedded malware, and also train employees to help avoid these attacks

- **Mitigation.** Organisations should gather the minimal data needed to provide the desired services while preserving the rights and expectations of individuals. Organisations should also apply encryption for gathered and stored data that are in transit and at rest. Encryption must be made easy to use, and ideally implemented as a default, particularly for individuals.

Of course, as user-friendly as tools might become, they still cost time and money to implement, which not all organisations are willing to spend to prevent data breaches and to mitigate their impact when they cannot be prevented. The final two recommendations focus on how these market failures can be addressed through economic incentives, concerning both costs and benefits.

- **Recommendation 4.** Increased accountability. By imposing more of the externalities of the data breach on the organisations holding the data, their costs will go up, leading organisations to increase efforts to prevent them and mitigate their impact.

- **Recommendation 5.** Security signals. By enabling organisations to signal that they are less vulnerable, thereby reducing the asymmetry of information, organisations will be able to better compete for business, increasing the rewards of investing in preventing a data breach.

The five recommendations are summarised in the security circle.

Underpinning these five recommendations are two important principles: data stewardship and collective responsibility.

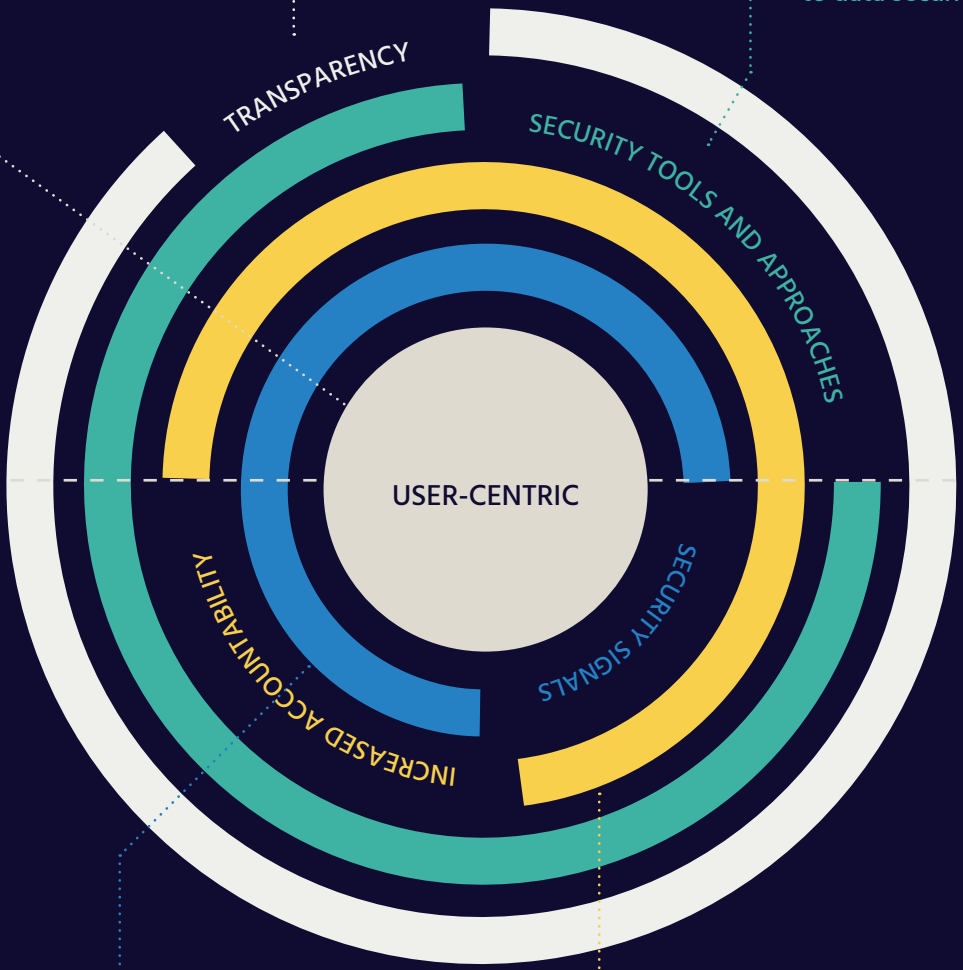
Data stewardship. Organisations should regard themselves as custodians of their users' data, protecting their data not only as a business necessity, but also on behalf of the individuals themselves. Organisations should apply an ethical approach to data handling, and understand that they can do well by doing good – protecting users should be a goal in its own right, which also protects the organisation.

Security Circle

1. Put users at the centre of solutions; and include both users *and* organisations when assessing the costs of data breaches.

2. Increase transparency through data breach notifications and disclosure.

3. Data security must be a priority. Better tools and approaches should be made available. Organisations should be held to best practice standards when it comes to data security.



TOOLS AND APPROACH

ECONOMIC INCENTIVE

5. Increase incentives to invest in security by catalysing a market for trusted, independent assessment of data security measures.

4. Organisations should be accountable for their breaches. General rules regarding the assignment of liability and remediation of data breaches must be established up front.

Collective responsibility. On the Internet, everyone is connected. One breach could lead to another (in other words, "your breach could be my breach"). Organisations have a responsibility to secure the data they hold. They also share a collective responsibility with other stakeholders to secure the data ecosystem as a whole. This includes vendors, employees, governments, and others. Should one of these links not function, the entire trust chain could be broken.

In summary, our message to organisations is:

- Personal data is precious and priceless – protect it!
- Collect only what is absolutely necessary and encrypt what you keep
- Restrict access to those who need to know
- Signal the level of data security you provide
- Destroy data when it is no longer in use
- Be more transparent about data breach incidents
- Be alert to breaches, prepare, notify and act immediately

Conclusion

Data breaches are a growing concern worldwide. To mitigate this problem and its economic impact, the report proposes a shift in the approach to data breaches, involving all stakeholders.

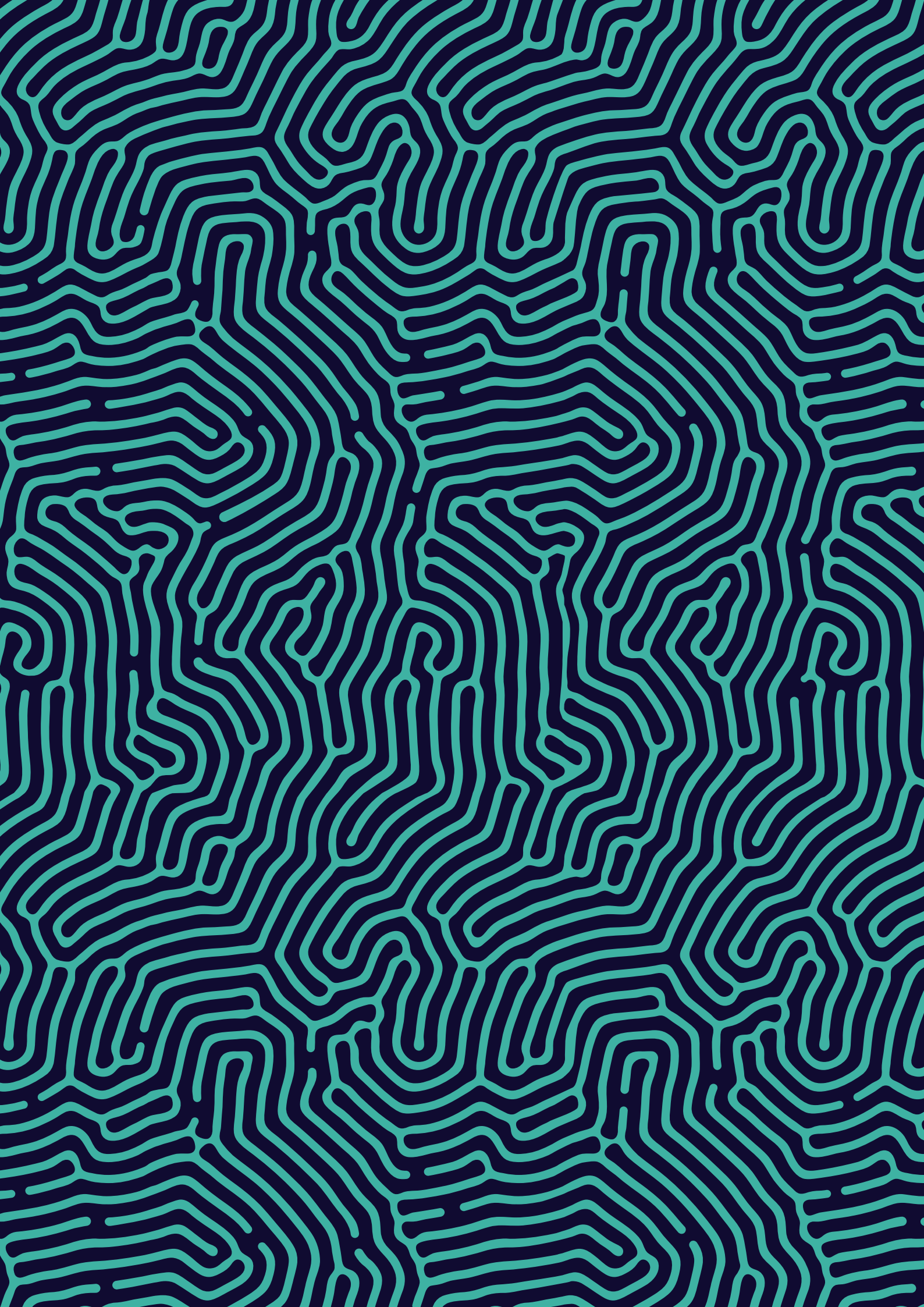
As users increasingly move their lives online, to achieve the full benefits of the Internet worldwide there must be user trust. That trust is dependent on how users' data is protected from breach. Each data breach creates a new group of users whose trust may have been betrayed, which spreads to their acquaintances through word of mouth, and more broadly through news reports, creating doubt, which undermines user trust at large.

With this report, the Internet Society's goal is to offer recommendations that will help to provide better data security. This, in turn, has the potential to increase use of the Internet, and raise the economic and social impact of the Internet on the broader economy and society. That, finally, will help meet the Internet Society vision that the Internet is for everyone, everywhere.

Internet of Things

Looking forward to a world of ubiquitous Internet of Things (IoT), vulnerabilities resulting in data breaches can also apply to IoT devices, with perhaps even greater impact on users. First, of course, connected devices such as baby monitors can contain sensors, including for video and audio, that can yield personal information about the owners. More broadly than a data breach, however, people may put their personal safety in the control of the connected devices, such as medical devices or connected cars. It is incredibly distressing to have one's health records stolen and sold. It is potentially fatal to have one's health devices hacked and overridden.

More broadly, many of our recommendations are valid for preventing or mitigating breaches of the full range IoT devices, not just for the data that they are gathering with their sensors, but also for a security breach that could lead to personal or public safety risks. As such, the Internet Society encourages the application of these findings to the range of relevant issues arising from the emerging IoT. While this is a broader issue than data breaches, the causes may be the same and should be considered in addressing the general security of these devices as a matter of priority.



CHAPTER 1

Introduction

Introduction

Data breaches are the oil spills of the digital economy.[1] Despite widespread recognition that they are a serious problem globally, data breaches continue to increase in number, size, and cost. They are toxic for user trust in the Internet, and their impact can spread across the whole data ecosystem affecting millions of users.

> What is a data breach? "A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a public electronic communications service."
>
> The Information Commissioner's Office (ICO) of the UK[2]

The ultimate casualty of data breaches is trust in the Internet. Would people continue to go to a store that let strangers shop with their credit cards? Go to a psychiatrist who disclosed confessed affairs in public? Work for a company that allowed anyone to access confidential personnel records? It is unimaginable.

Target had 40 million customers' credit card numbers stolen and put on sale online; Ashley Madison's records on 37 million married users and their personal affairs were taken and published online; and the US Office of Personnel Management had at least 21.5 million records, including highly sensitive security clearance records of past, present, and potential employees, stolen.

The impact of these breaches on consumers, users, employees and third parties, some of whom did not even know the organisations had their data, is profound and lasting. Users lost time and money protecting their finances and their identity from theft; others saw marriages dissolve and even committed suicide, and still others may be subject to blackmail and exposure. Also, the victims can never be sure that the impact has been contained.

All were let down by the very organisations they had entrusted with their personal information. Even worse, in many cases, the data breach could have been avoided. Some breaches occurred because the systems were not protected from known bugs; others because users were not trained in how to avoid being tricked into providing access. Even then,

steps could have been taken to avoid harm in the event of a breach, such as minimising the amount of data collected and encrypting the data that was kept.

The question this report seeks to answer is a simple one. Why are many organisations not taking even the basic steps to protect the personal information they hold? Is it because they do not bear all the costs of the data breach? Is it because there is not enough perceived benefit in better protecting their users' data?

The answer to both questions is yes. Organisations may only consider their costs and neglect the potential costs to their customers and others. It is also hard for an organisation to signal that they are better prepared against a data breach than others, reducing the benefit of investing in data security.

The Internet Society envisions an Internet for everyone, everywhere. Trust in the Internet is at the core of that vision. Without trust, those of us online are less likely to entrust our personal information to Internet services; and those not yet online will have another reason to stay offline. The Internet economy will not grow as fast as it could, and the UN Sustainable Development Goals (SDGs) will be that much harder to achieve.

To help build trust in the Internet, this report sets clear goals and recommendations to help organisations globally reduce the number and impact of data breaches.

With this report, the Internet Society proposes five recommendations to help address the issue of data breaches:

1. Put users at the centre of solutions; and include the costs to both users and organisations when assessing the costs of data breaches

2. Increase transparency through data breach notifications and disclosure.

3. Data security must be a priority. Better tools and approaches should be made available. Organisations should be held to best practice standards when it comes to data security.
4. Organisations should be accountable for their breaches. General rules regarding the assignment of liability and remediation of data breaches must be established up front.

5. Increase incentives to invest in security by catalysing a market for trusted, independent assessment of data security measures.

The ultimate goal is for organisations to take a position of data stewardship over the personal information they gather, and for all stakeholders, including consumers, to acknowledge they have a collective responsibility to help prevent data breaches.

Internet of Things

Online services are the main focus of this report, however, given the size and frequency of data breaches today, the Internet of Things (IoT), poses additional challenges if the lessons learned from present-day data breaches are not applied.

Forecasts show the IoT may grow to tens of billions of connected devices by 2020.[3] Many of these will act as sensors, gathering information about us, our homes, cities, and our environments. The data from IoT devices could greatly increase the harm caused by a data breach, as sensor data could include our location, health, and daily habits, including driving and shopping.

Worse yet, these devices could be taken over. The stream from an online camera intercepted; a baby monitor used by a stranger to talk to the baby; a health device sabotaged; a car hijacked.[4] In one chilling example, several security researchers recently showed a computer-targeted sniper rifle could be retargeted.[5]

As such, it's critical to highlight these issues now, so that we take the necessary steps to secure these devices and their data.[6]

Footnotes

[1] As has been pointed out, data, like oil, has its downsides, and in this light, data breaches are the new oil spills. See the following article by the Internet Society's Technical Outreach for Identity and Privacy, Robin Wilton, at https://www.internetsociety.org/blog/tech-matters/2014/10/they-say-"personal-data-new-oil"-thats-good-thing.

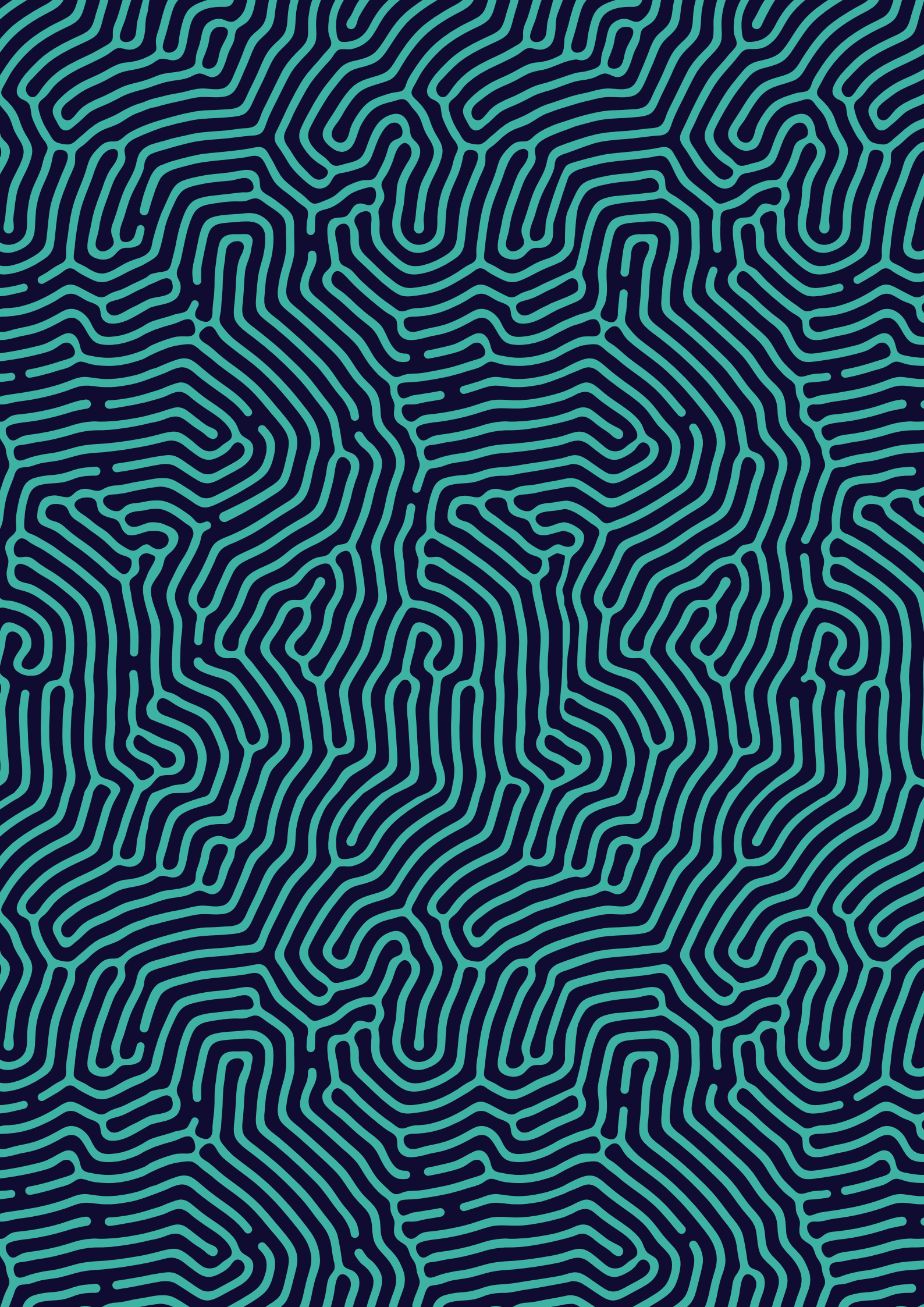
[2] See https://ico.org.uk/for-organisations/guide-to-pecr/communications-networks-and-services/security-breaches/.

[3] Some popular forecasts put the number at 50 billion. Recently Gartner put the forecast at 21 billion for 2020, up from just under 5 billion at the end of 2015. http://www.gartner.com/newsroom/id/3165317 Either way, there will soon be multiples of connected device per person globally.

[4] All of these things have already happened. Webcams: https://blog.kaspersky.com/2ch-webcam-hack/11961/; Baby Monitor: http://www.independent.co.uk/life-style/gadgets-and-tech/news/baby-monitors-hacked-parents-warned-to-be-vigilant-after-voices-heard-coming-from-speakers-a6843346.html; Insulin pump hacked: http://www.theregister.co.uk/2011/10/27/fatal_insulin_pump_attack/; Jeep hijacked (discussed further later in the report): https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

[5] The rifle has a WiFi connection to stream a video of a shot, which has a default password that allows for entry and reprogramming. As one of the researcher's states, "There's a message here for TrackingPoint [the rifle manufacturer] and other companies…when you put technology on items that haven't had it before, you run into security challenges you haven't thought about before." See https://www.wired.com/2015/07/hackers-can-disable-sniper-rifleor-change-target/.

[6] For more details, see the Internet Society's report The Internet of Things: An Overview, including a section on Security Issues, starting on page 31. See http://www.internetsociety.org/doc/iot-overview.



CHAPTER 2

Data and Trends

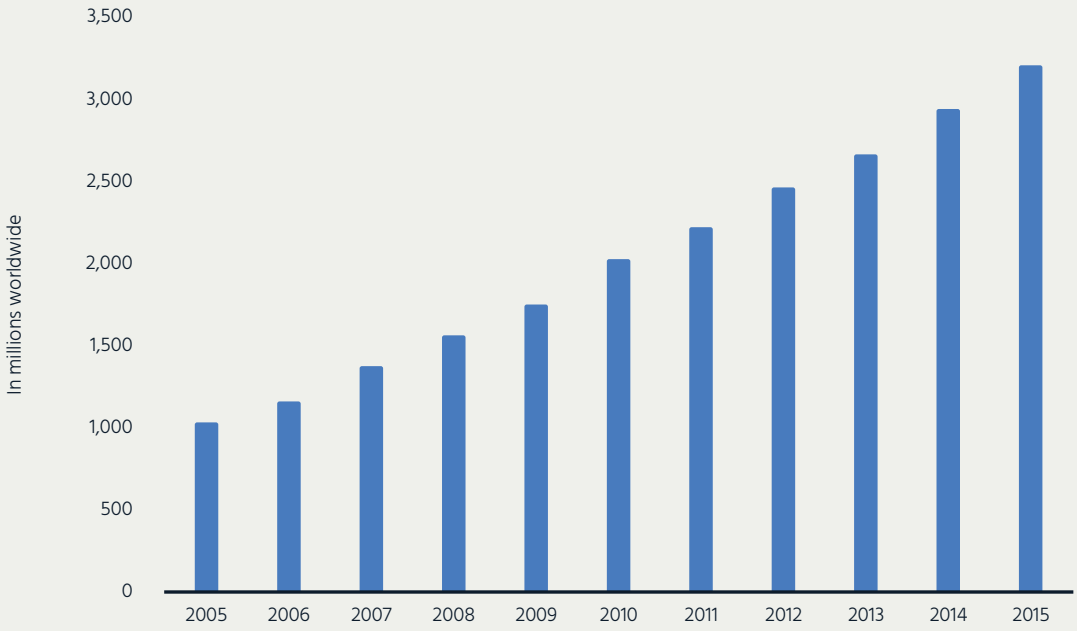
Introduction

According to the ITU, the Internet passed the 3 billion user milestone in 2015, with just over 3.2 billion users worldwide by the end of the year. While this highlights steady growth, there is work to be done to bring the Internet to everyone, particularly in certain regions.

As of 2015, more than half the world's population was not yet online (see below). Historical annual double-digit growth levels in the number of users dipped to 8% for 2015. The fact that growth rates keep falling with Internet penetration still below 50% is cause for alarm.

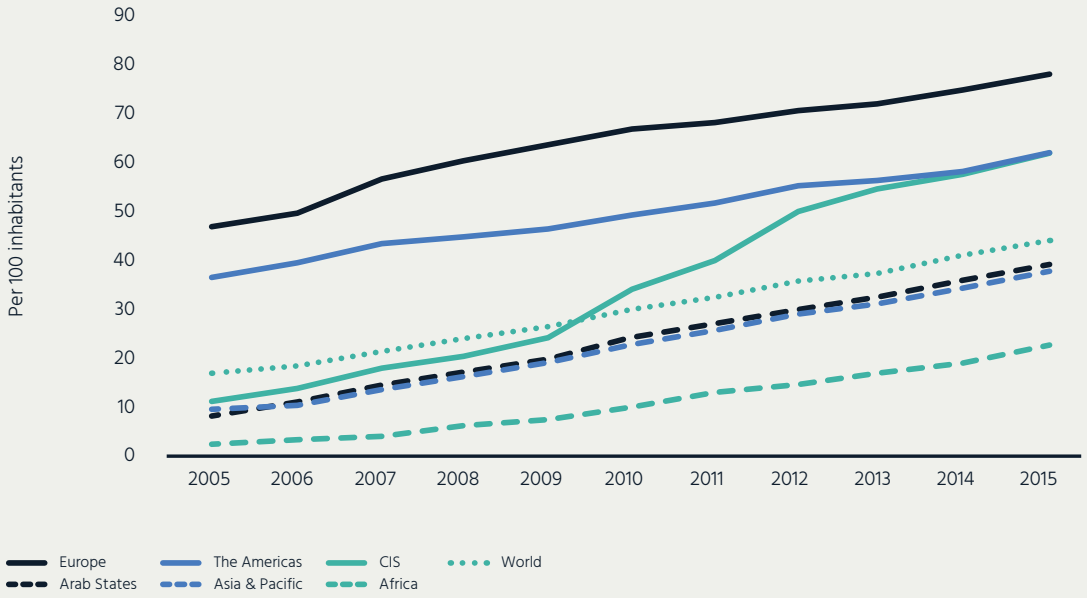
The story is not much better on a regional level. It might be expected that Europe, with a leading 76% of the population online, could withstand a dip in growth rates to 2%. But Africa, which just surpassed 20% of the population online, has also seen growth rates fall significantly, albeit to 15%. This slowdown suggests that connecting the unconnected will take significant and concerted efforts.[1]

Individuals using the Internet



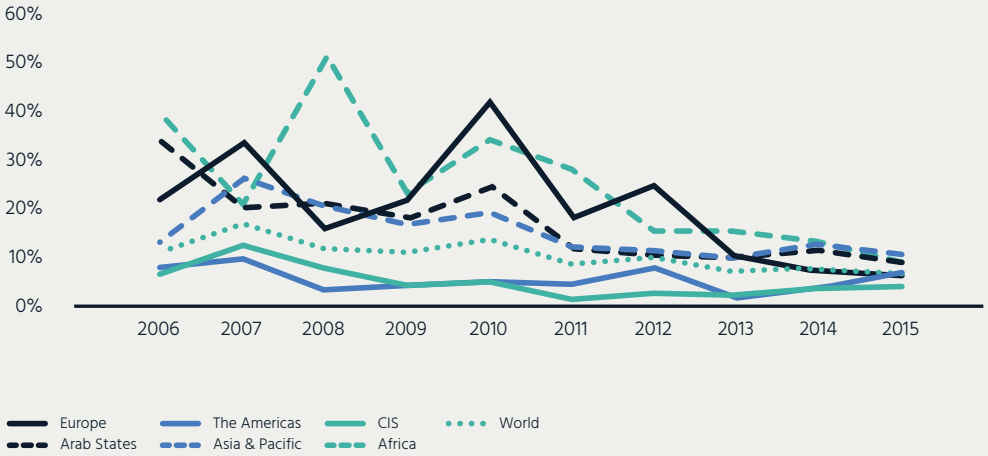
Source: ITU 2016

Individuals using the Internet



Source: ITU 2016

Internet user growth rates



Source: ITU 2016

The slowdown in Internet growth rates, particularly in regions that were already falling behind the global average, lends urgency to the Internet Society's objective to connect the unconnected. There is evidence that existing users are increasingly concerned about privacy and security issues worldwide, and this may start to spill over to new users, who might become more reluctant to go online. If people trust the Internet, they are more likely to use it. Trust is at the heart of the Internet economy, and more and more at the heart of economic growth.[2] This lends urgency to our objective to promote and restore trust in the Internet.

Users are increasingly aware of privacy and security issues in general, and specifically in relation to data breaches. The number of reported data breaches is increasing, while the full extent of breaches is unknown. The data shows the trend is for outside hackers to attack organisations to gather data for identity theft, which is a direct attack on the organisations' users.

These breaches have had an impact on users' trust. In particular, privacy and security issues seem to weigh most heavily on those who are already online. That may be because they have some understanding of the implications of the personal information they are providing to online services, or because they already have had a direct experience with a data breach. The surveys highlighted below show a persistent and growing segment of users who temper their use of certain online services because of privacy and security concerns.

This report also examines the cost of data breaches. At one level, organisations are not complacent about the increasing number of data breaches, which are a significant cost for organisations and society to address. Nonetheless, while spending on cybersecurity continues to rise, there is little available evidence breaches are slowing in number or size. There are also few studies of the direct costs of data breaches on the users themselves, who are often the ultimate victims.

Organisations do not bear all the costs of a data breach. They often do not bear all the financial cost imposed on other related organisations by the breach, and they do not bear all the cost imposed on users. In economic terms these unaccounted for costs are **externalities**. At the same time, organisations have a difficult time increasing user trust in their services because it is hard to convey how secure their services are to users. In economic terms, this difference in viewpoints is known as **asymmetric information**.

These economic issues help identify incentives for organisations to prevent data breaches, and form the heart of the issues and recommendations sections.

Data breach trends

The interest in data breach trends is fed by the increased number being reported, along with privacy rights activists and data protection authorities helping to raise awareness. A variety of yearly reports focus on data breaches, however they may be covering the tip of the iceberg.

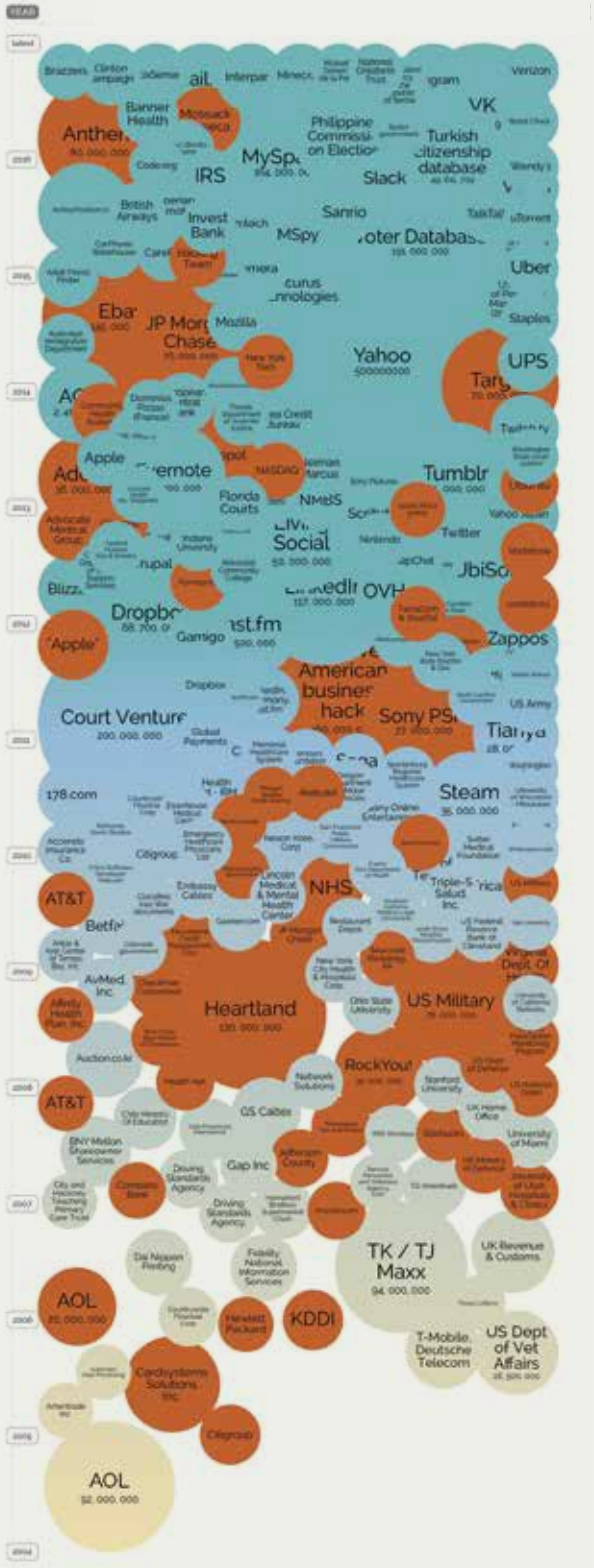
> 'There are two types of companies – those who have been hacked, and those who don't know they have been hacked.'
>
> Common cybersecurity saying

If a company has not detected a breach, it cannot report it. Even if a breach is detected, it still might not be reported. Not all countries require breaches to be reported. Even within those countries, it is unlikely all breaches are reported, as reporting requirements may only apply to certain types of data breaches. Even where reporting is compulsory, not all aspects may be reported. For instance, organisations increasingly do not report the number of records breached.

As a result, the numbers that follow certainly underreport the number and magnitude of breaches at a global level. Nonetheless, even the breaches reported paint a picture of almost steady increase over the past years.

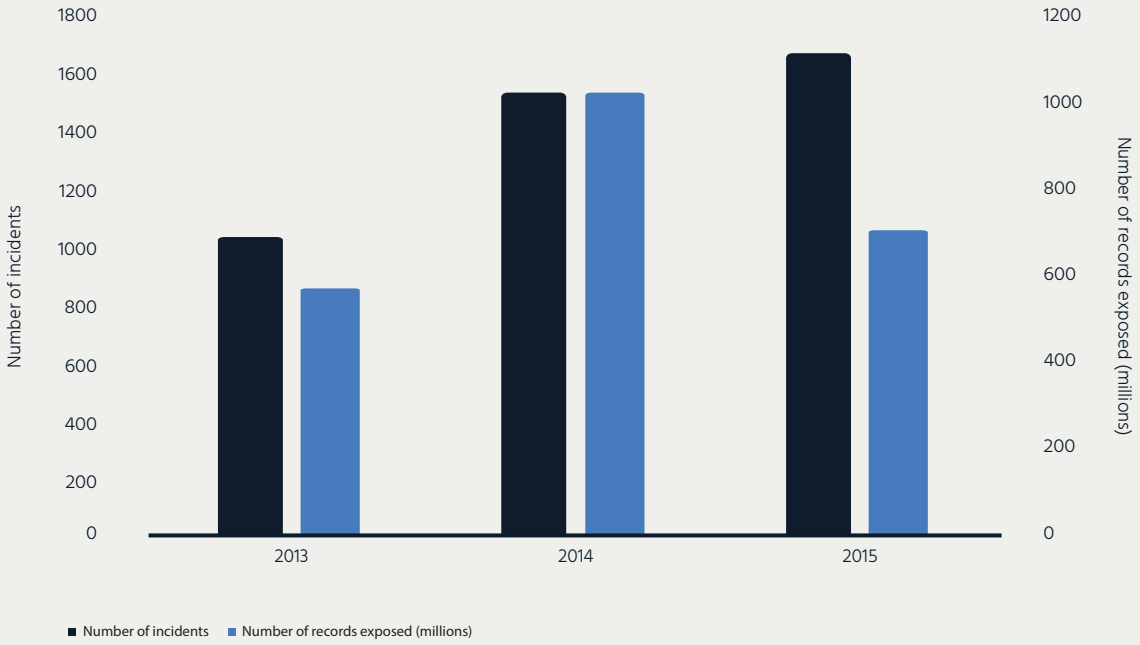
World's Biggest Data Breaches

Selected losses greater then 30,000 records
(updated 24rd September 2016)



Source: David McCandless, Information is Beautiful, http://www.informationisbeautiful.net

Reported global data breaches



Source: Breach Level Index, Gemalto, 2016

One representative source of data on breaches is the Breach Level Index from Gemalto. Gemalto reported 1,673 known incidents for 2015, with 707 million records known to be exposed. The total number of reported incidents is rising, while it appears the number of reported records exposed fell in 2015.[3]

However, Gemalto also noted in 47% of incidents in 2015, the number of records breached was not reported. As a result, the number of records breached could be much higher, and it is difficult to determine a trend in the number of records exposed over time.

Other sources reported similar trends. The Data Breach QuickView from Risk Based Security, Inc. shows 3,930 breaches globally with 736 million total records exposed for 2015.[4] They note in just under 29% of cases, the number of records reported exposed in a breach were 'unknown', up from just over 19% of breaches in 2014. Another source, the Internet Security Threat Report from Symantec, reported 291 known breaches for 2015, involving 429 million records, while in 39% of incidents the number of records breached was not reported.[5]

While each source reported a different number of incidents ranging from 291 to almost 4,000, at least 429 million individuals were impacted in 2015. It is likely far more were affected given the number of unreported incidents and those reports with unknown numbers of records.

The number of data breaches appears to be rising, along with the number of records breached. However, the numbers do not tell the full story.

It is clear the reports underrepresent the number of data breaches taking place, and the number of records breached, so the full extent of the breaches is not fully known. Many countries do not require breach notification, and even in countries that do, it is possible that not all breaches are reported. And, of course, not all breaches will have been detected. Further, when they are reported, the number and type of records are sometimes not reported or not even known.

Yet, the increasing number of breaches reported does not necessarily mean that organisations are more susceptible to breaches. The Internet continues to grow in the breadth of users and organisations that are online, and in the depth of use, resulting in ever more data collected. So, it is not immediately clear whether organisations are more susceptible to breaches, or whether organisations are better at protecting themselves, but there are more organisations to breach.

One study from the Global Commission on Internet Governance, sponsored by the Centre for International Governance Innovation (CIGI) and Chatham House, concluded, using a variety of metrics, that normalising cybercrime numbers based on growth shows the state of cybersecurity is better than indicated by the absolute numbers.[6]

Still, this report starts from the view of the user. From their point of view, the most striking argument may be they hear more about the increase in the absolute number of data breaches, and the implications for their personal data, with a corresponding impact on Internet trust levels.

The global number of incidents of data breaches in the Gemalto Breach Level Index are broken down along some key categories:

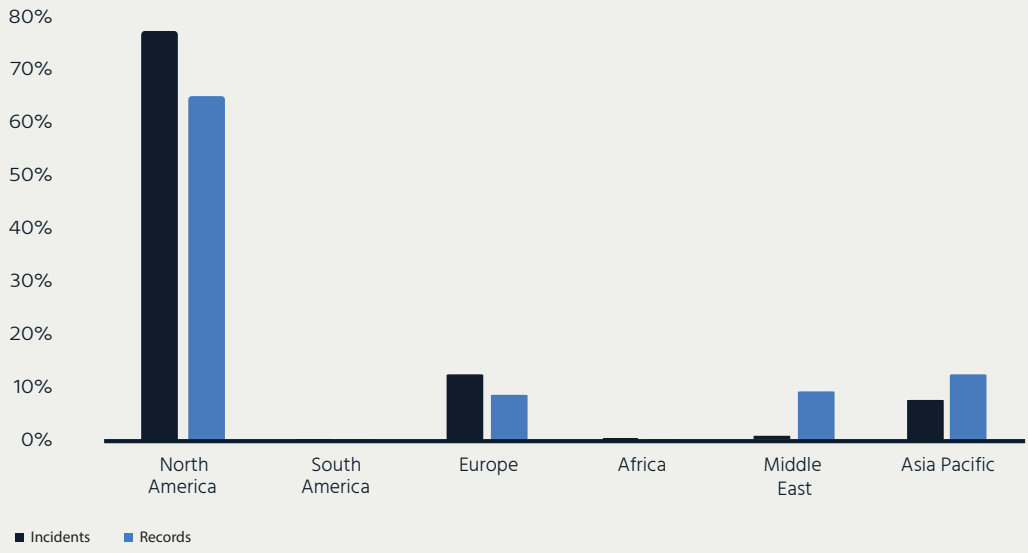
- Geography
- Source of breach
- Target of breach
- Type of data breached

Geography

The United States always weighs heavily in these reports, both for known incidents and reported records breached. As shown, the United States makes up 1,222 of the 1,287 incidents in North America (and 73% of the global total). Another report from 2015 shows the US at 40.5% of incidents out of 111 countries reporting at least one breach (with 20.2% unknown geography) and 64.7% of the records breached (with just 1.7% unknown).[7]

When asked why he robbed banks, it is said Willie Sutton responded, 'That's where the money is'. It is tempting to conclude from these data the US is where the records are stored, and there are a high number of data targets in the US, including non-US companies using US data centres. But, it is more likely that the ranking is due to more comprehensive data breach disclosure laws in the US.[8]

Geography of data breaches



Source: Breach Level Index, Gemalto, 2016

Source of breach

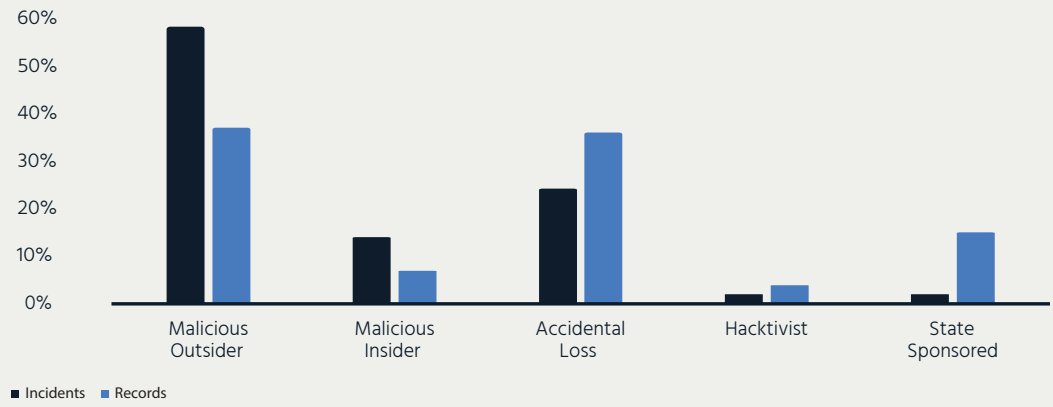
Understanding the source of data breaches is critical to efforts to prevent, detect, and rectify them. While different publications use somewhat different classifications, outside attacks are consistently the top source of data breaches followed by accidental release of data and insider breaches.[9]

Outside attacks often exploit known security vulnerabilities, many of which could likely be prevented. These include at one end, zero-day exploits that are unknown to the software developer until exposed (giving 'zero days' to fix the vulnerability). And, at the other end there are known vulnerabilities for which there are existing patches that have not yet been applied.

The exploited vulnerabilities can be internal to the target organisation, or a related organisation, such as a vendor, whose system is connected to the target and may be more susceptible. A common means to access any organisation is through social engineering, for instance using phishing to trick a user into providing their password or downloading malware.

Many of these outside breaches are preventable. This is discussed further in the issues and recommendations sections.

Source of data breaches



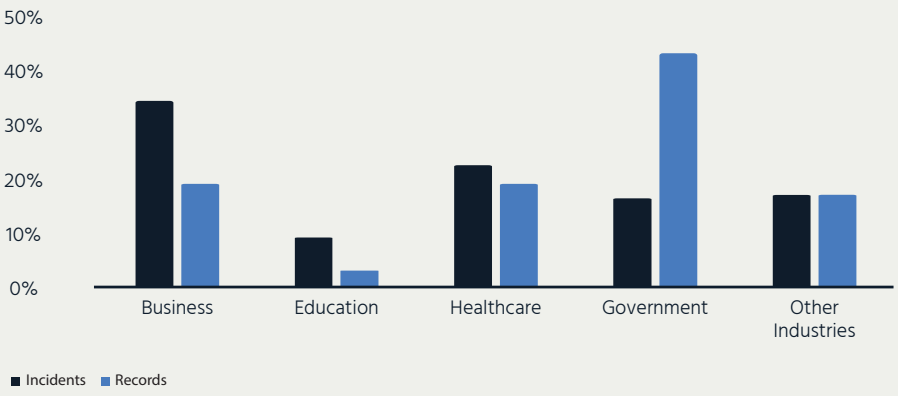
Source: Breach Level Index, Gemalto, 2016

Target of breach

The following graph indicates the targets of the reported breaches in 2015, as tracked by Gemalto. It shows businesses are the top targets, followed by the healthcare industry, and then government. While government had a lower number of breaches than the other sectors, it had a significantly higher number of known records breached, in part due to a small number of large government breaches in 2015.

Within business, the retail sector represents 13% of all breaches (and 6% of the records), financial services represents 15% of breaches (but just 0.1% of records) and technology represents 6% of breaches (and 12% of records). Other industries are not broken down in detail in this report.

Target of data breaches



Source: Breach Level Index, Gemalto, 2016

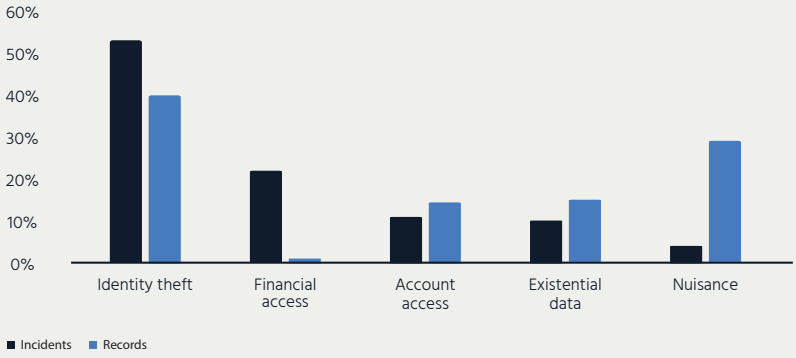
Type of data breached

The report reviews the type of data that has been targeted. Using Gemalto's definitions, the following categories are tracked:

- Identity theft, with both the most incidents and the most records
- Financial access (bank account and credit card), which has a high number of incidents, but relatively few records, at least for 2015.
- Account access, which represents usernames and passwords to online services such as social media, and sits at around 10% of incidents and slightly more records
- Existential data, defined as data with national security value or vital to the survival of the business, is also around 10% of incidents and slightly more records
- Nuisance data, consisting of email addresses and affiliations, is low in the number of incidents but amounts to almost 30% of records

From this report it appears financial access does not represent a significant amount of the total breached records, but the direct financial impact may be lower for the consumer given liability limits on credit cards. Arguably, identity theft is much more significant – also potentially existential for individuals – and represents a worrying number of breaches and breached records.

Information targeted in data breaches



Source: Breach Level Index, Gemalto, 2016

Impact on users' trust

The number of reported breaches and the number of records breached are rising, and a significant target is the information needed for identity theft. How does this increase in reported breaches impact Internet users who are often the ultimate victim? Does it affect non-users' willingness to go online in the first place? Does it impact existing users' willingness to use certain online services? The results of various surveys illustrate individuals' attitudes towards privacy and security, and how changes in attitude may impact their behaviour.

A wide range of surveys show existing online users are concerned about security, and claim it impacts their willingness to use services requiring personal information. This includes e-commerce, e-government, social media, and online banking and health services. This is an alarming trend for the growth of the Internet, but it is difficult to confirm whether it translates into lower or more selective usage.

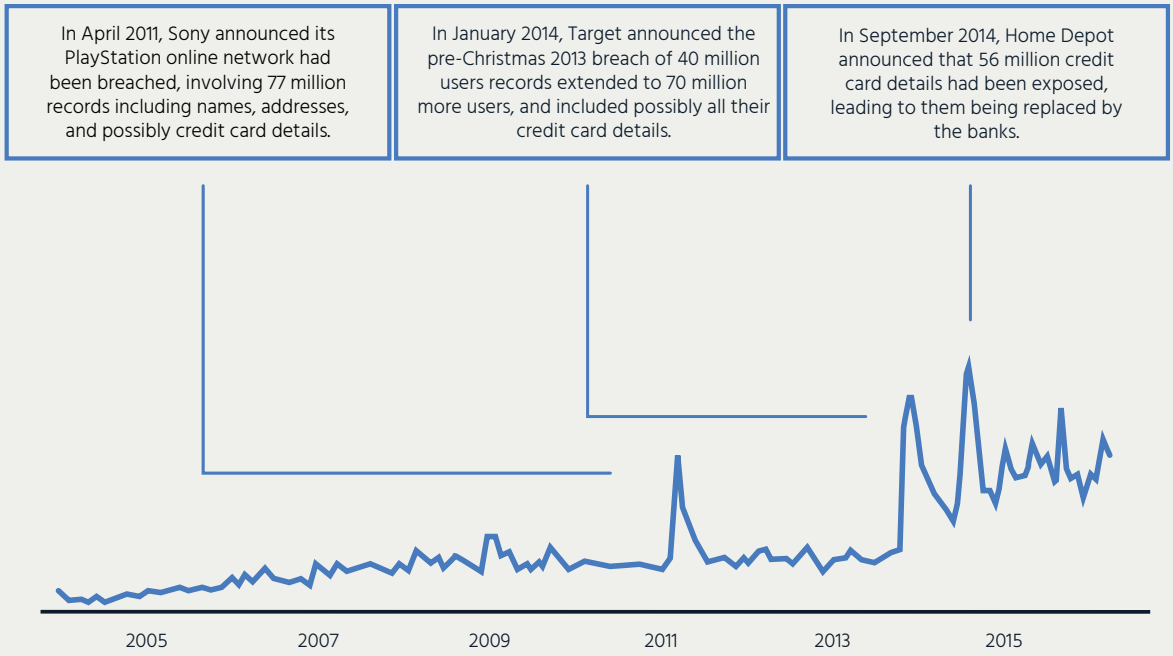
There have also been few surveys of non-users and why they are not going online, particularly in emerging markets. In Brazil, where there are extensive yearly surveys, there is a group of non-users concerned about privacy and security, as shown in the upcoming graph. Other evidence indicates Internet trust is an issue everywhere and may be more significant in emerging countries.

Users are subject to a wide variety of news about privacy and security issues in addition to data breaches. At a personal level, there are risks of viruses and spam that may not be connected to data breaches. The topic of pervasive surveillance clearly has gained significant attention, particularly since the Snowden revelations. It is hard to find out which privacy or security concern is foremost on users' minds as they answer surveys, or as they engage online.

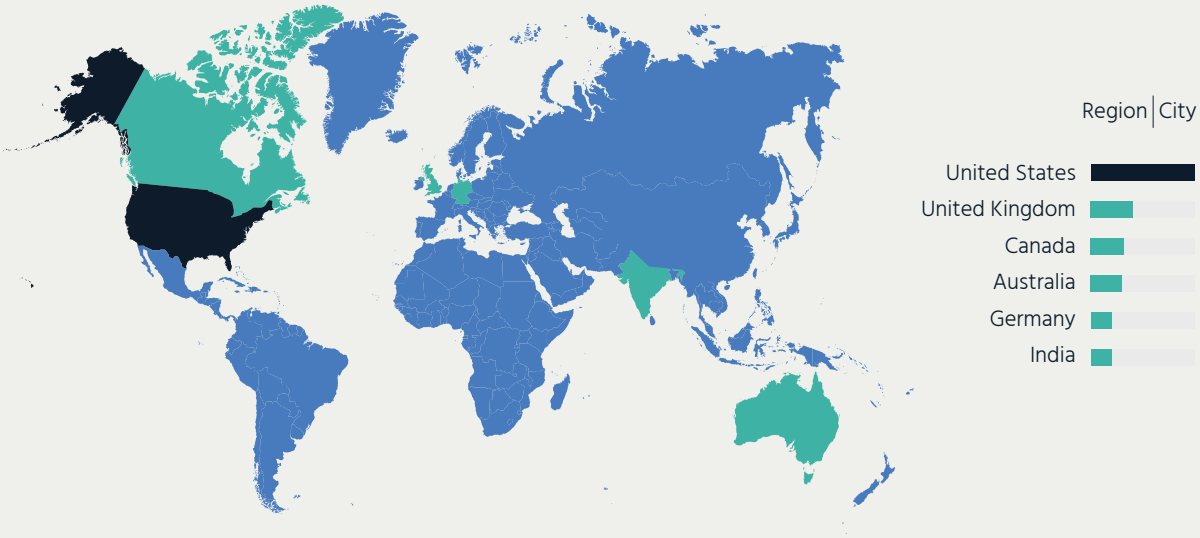
There are some surveys focusing specifically on the impact of data breaches on consumers, although with a narrow focus on how a data breach would impact their loyalty towards that company, rather than more broad impacts on users' trust. Nonetheless, they show the impact on trust is significant and represents a business risk companies should take into account.

The repeated news about significant data breaches appears to have raised awareness and interest. For instance, the graph below shows interest in 'Data Breach' as a topic in Google Trends, which is based on web searches. The trends show both a rising interest, along with distinct spikes that likely correspond to news of large breaches as users search for more information, or check if they might be victims.

The graph shows search volume by country, compared to the country with the maximum search volume, which is always 100 in Google Trend reports. For the topic 'Data Breach', the US dominates. This is likely because of the higher rate of disclosures there. However, these trends are confined to searches in English, and thus do not necessarily represent global interest in the topic.



Source: Google Trend: 24 May 2016



The UK Google Trends chart shows spikes corresponding to large local breaches, most notably peaking with the TalkTalk breach in October 2015

Source: Google Trends, 24 May 2016

The Centre for International Governance Innovation (CIGI) commissioned Ipsos to conduct the Global Survey on Internet Security and Trust that reached over 24,000 users in 24 countries in late 2015.[10] The results confirmed a greater awareness of privacy issues and corresponding changes in reported behaviour.

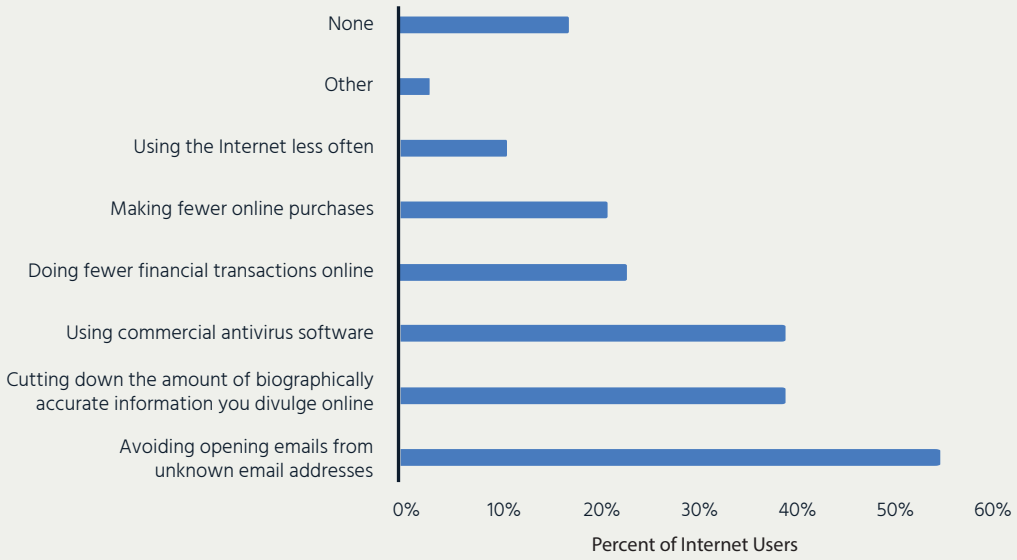
57% of the respondents are more concerned about their online privacy compared to the year before; in 2014, 64% reported more concern compared to the year before that. Thus, privacy concerns are definitely on an upward trajectory.

These concerns may only be partially related to data breaches. Some users may be concerned by other factors, including pervasive surveillance or how their data is collected and used by businesses. Nonetheless, data breaches are among those factors that impact users' decisions about how they use the Internet.

When asked how they changed their online behaviour, only 17% of users said they had not changed their behaviour at all. The rest expressed a variety of changes as shown. While only 11% said they were using the Internet less often, more were changing their online behaviour including providing less biographically accurate information online.

Some users indicated they were taking sensible defensive measures including using commercial antivirus software and not opening emails from unknown sources. This shows a growing awareness among users that they have a role to play in protecting the security of their devices and their personal information.

Changed behaviour to control personal information



Source: 2016 CIGI-Ipsos Global Survey on Internet Security and Trust

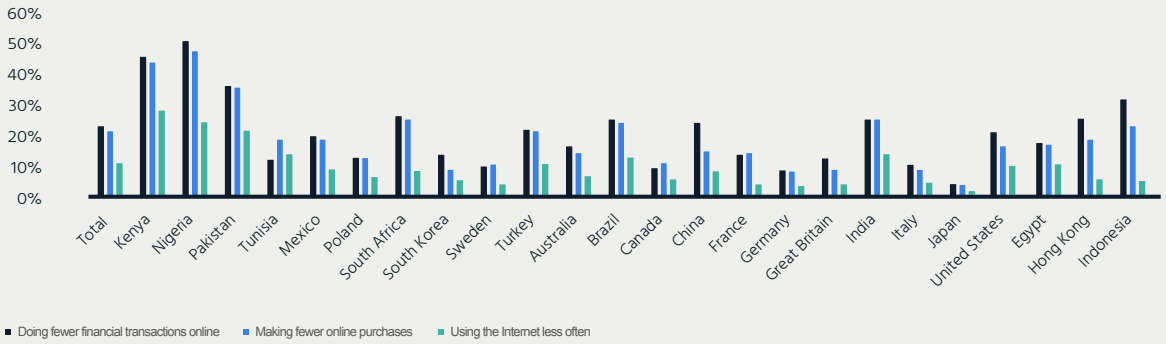
The following graph shows the responses in each of the 24 individual countries covered by the CIGI-Ipsos survey, to show variations across countries in three key questions of how users are changing their online behavior: using the Internet less often; doing fewer financial transactions online; and making fewer online purchases. In most of these cases, negative responses in emerging countries tended to be higher than the total average, notably in Kenya, Nigeria, Pakistan, and India, while in developed countries, the negative responses tended to be lower than the total average, notably in Germany and Japan.

This lack of trust can have a significant impact on the ability to do business. For instance, the lack of trust in online payments, and fear of online fraud contribute to the high prevalence of cash on delivery (COD) usage for e-commerce in India. This payment mechanism requires the recipient to pay the deliverer for the products, which requires the buyer to be present, marks the deliverers for robbery,

and results in many returns, where the buyer simply does not accept the package at delivery.[11] Similar issues are arising in other countries where online trust is low, such as Nigeria.[12]

This lack of trust in online payments, along with other changes such as fewer financial transactions online, challenges both the full potential of the Internet economy as well as the impact it can have on the broader economy.

How have you changed your behaviour as a result of online privacy concerns?



Source: 2016 CIGI-Ipsos Global Survey on Internet Security and Trust

United States

The US data demonstrates a difference in how trust issues impact the attitudes and behaviour of those already online compared with those not yet online.

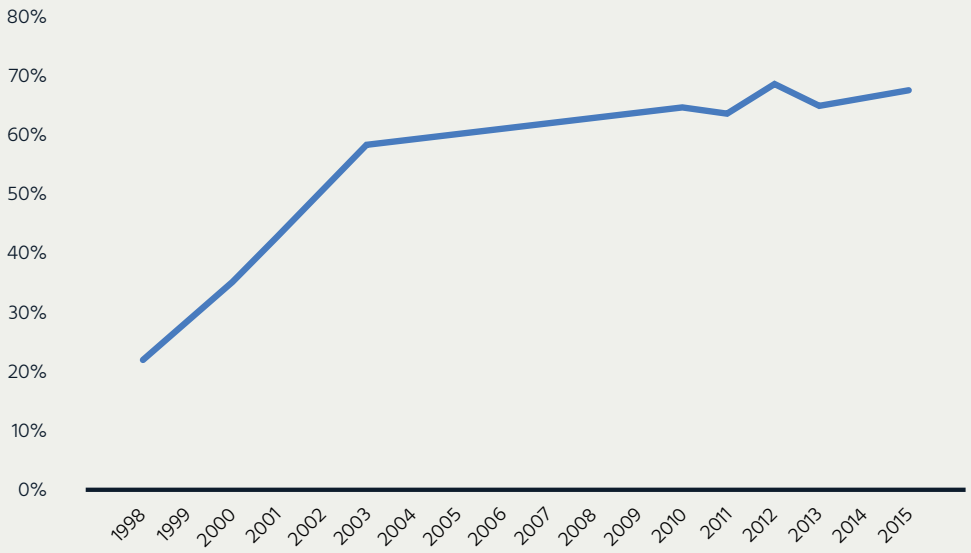
The chart shows how US Internet use at home has grown since 1998, from just over 20% to almost 70%. Internet use among individuals is now even higher, near 75%, but not everyone accesses the Internet from home.

Among the declining number of households who do not access the Internet from home, the percentage who cite privacy and security as the main reason for not going online is very low, given by 1.4% of households not online in 2015. This was the least cited reason for households not to go online in 2015.

In 2015, the majority of households not online stated it was because of a lack of need or interest in the Internet, followed far behind by cost concerns, then even further behind by the lack of a computer to use. A small percentage stated it was because the Internet was not available in their area. Another small group said they were not interested in using it at home because they could use it elsewhere.

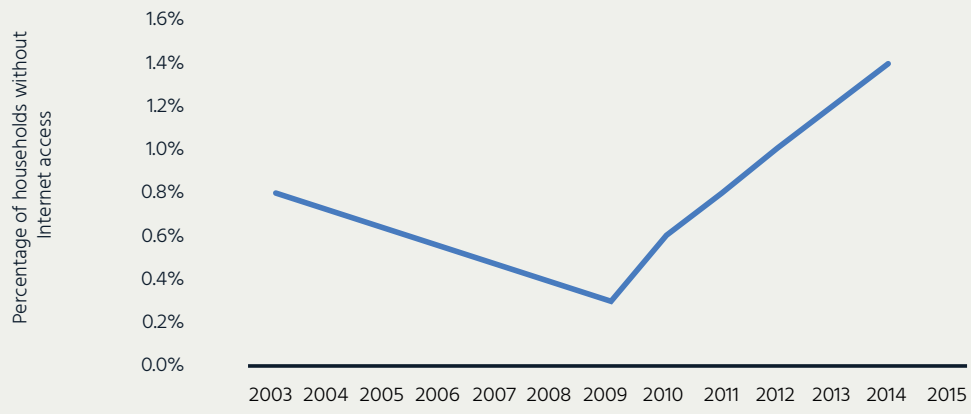
Instead, privacy and security concerns weighed more heavily on those already online, particularly for those who had already had their online security violated.

Uses the Internet at Home



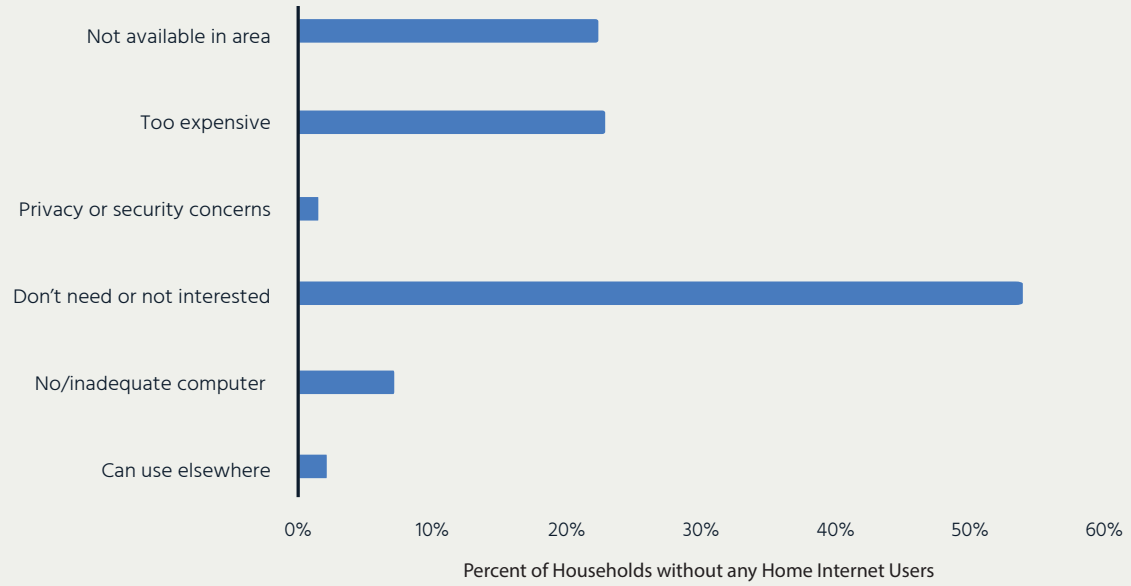
Source: NTIA Digital Nation Data Explorer, 2016

Main reason for household not online: Privacy or security concerns



Source: NTIA Digital Nation Data Explorer, 2016

Main reason for household not online at home



Source: NTIA Digital Nation Data Explorer, 2016

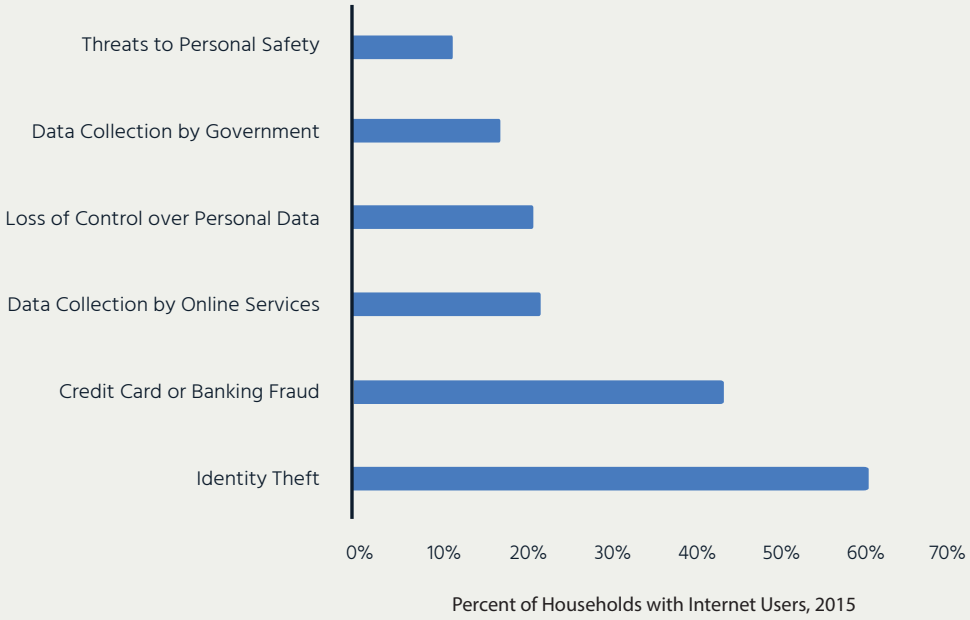
Households with Internet users are concerned about online trust, according to a recent survey conducted for the National Telecommunications & Information Administration (NTIA) by the US Census Bureau.[13]

As shown in the graph, online households had significant privacy and security concerns, particularly about identity theft and credit card or banking fraud. Many had direct experience with such events.

The study revealed an average of 19% of Internet-using households had been impacted by a security breach, identity theft, or other malicious activity in the 12 months before. Further, the more online devices in the household, the more likely a breach, ranging from 9% for those with one device, to 31% for those with five or more devices.[14]

Those households who had recently been affected by a breach were, not surprisingly, even more concerned about privacy and security risks. While the average concern about identity theft was 63% of households, for those who recently experienced a breach, 70% were concerned about another one occurring.

Major concerns related to online privacy and security risks



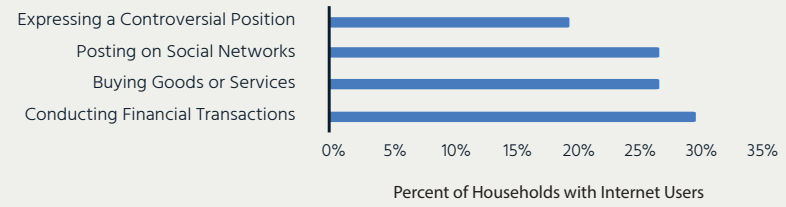
Source: NTIA Digital Nation Data Explorer, 2016

According to the survey, these concerns about privacy and security lead users to avoid certain online activities. In particular, as shown in the graph, some users expressed a reluctance to make a controversial position online, post on social networks, buy goods or services, or conduct financial transactions. For instance, up to 30% of users reported avoiding conducting financial transactions online. Among those reporting a prior security breach, the percentage avoiding online financial transactions was even higher at 40%.

However, online use of services requiring personal information, notably online shopping and financial services, continues to climb, to almost 70% of those online in 2015. While it is possible, and even probable, that online use of these services would have increased further but for the security concerns, the number of users is still climbing regardless.[15]

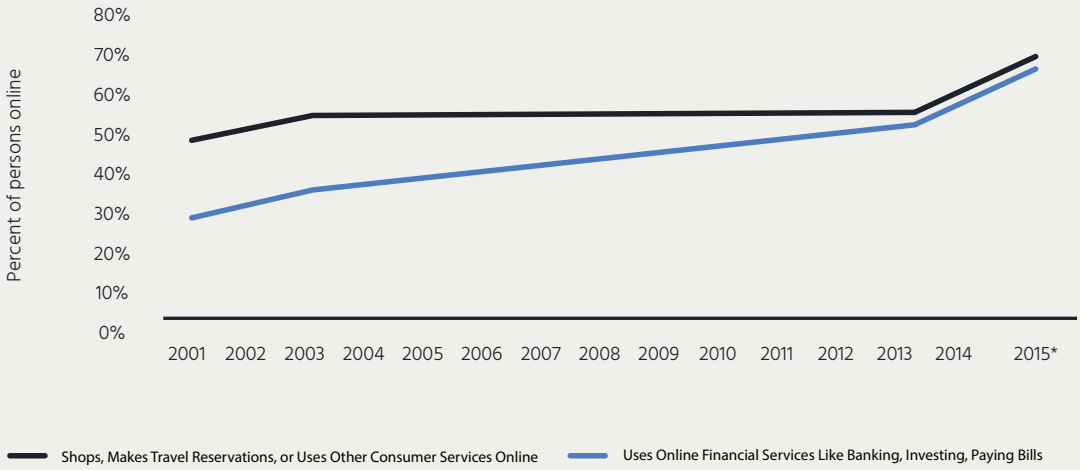
This increase in the number of users should not make organisations complacent about user trust. Prior experience (or even knowledge) of an online security breach impacts user trust. Further, more and more breaches are taking place. It is important to listen to what users are saying, and not dismiss their concerns simply because online transactions are increasing. Users are less trustful, and as the pace of data breaches increases, their concerns should be front and centre for those working to promote and restore trust in the Internet.

Online activities avoided due to privacy or security concerns



Source: NTIA Digital Nation Data Explorer, 2016

Online use



European Union

In the European Union, the story is quite similar to the US. Online households across the current 28 countries of the EU climbed to a level now over 80%.

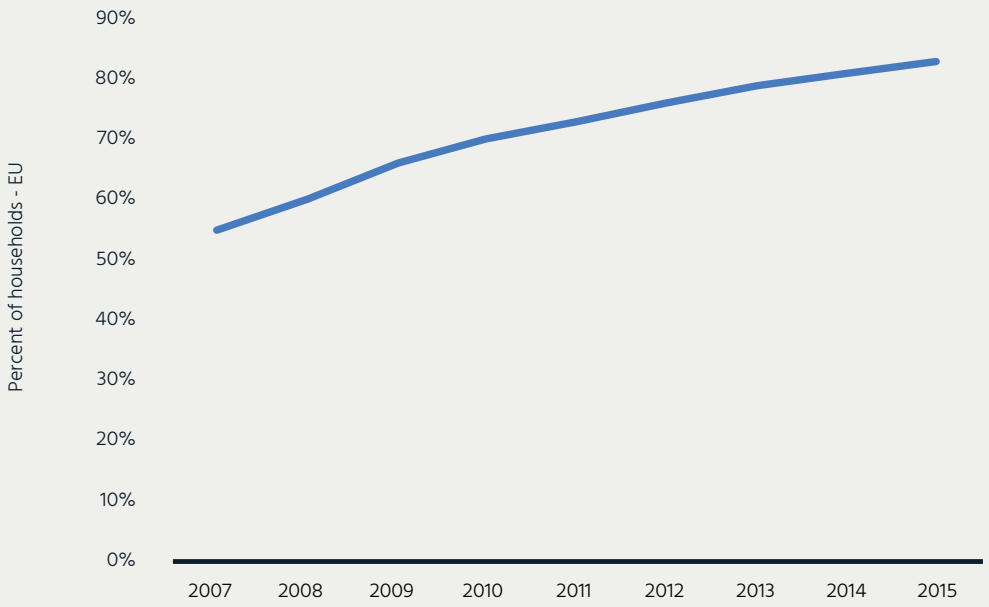
The concerns of the households not yet online are examined below.

Concerns about privacy and security have been climbing over the past years. But, still only 9% of households that are not online cite privacy and security as a concern.

Instead, the top reason cited for not being online is a lack of perceived need, followed by a lack of skills, and then by concerns with the cost of access or equipment. As in the US, privacy and security is the lowest ranked reason for not going online, although at a higher level than in the US.

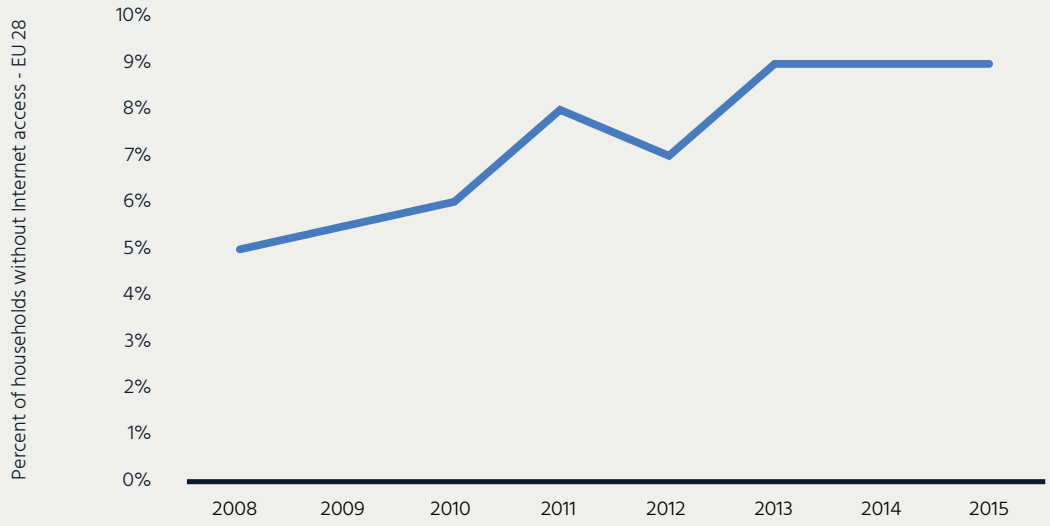
Like in the US, security concerns in the EU weigh more heavily on those already using the Internet.

Level of Internet access - households



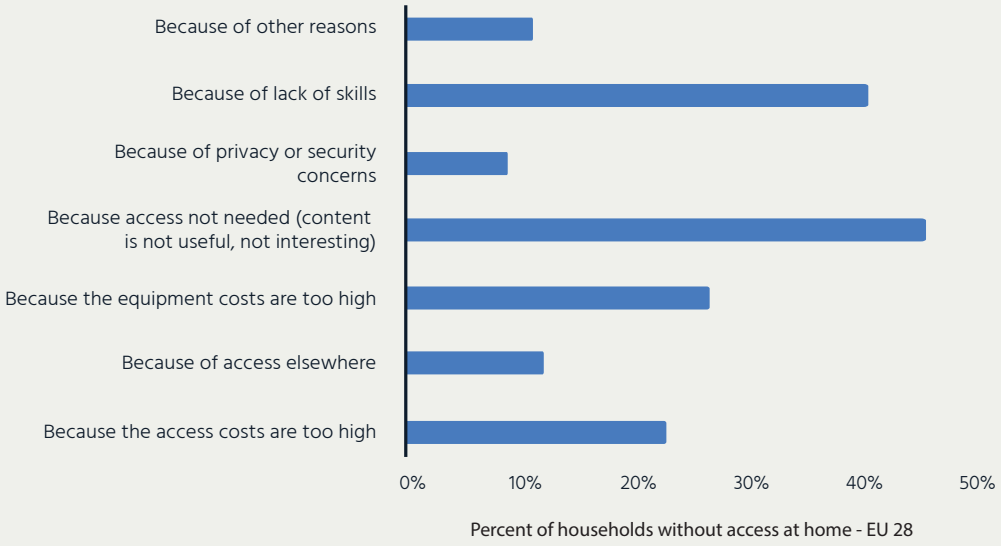
Source: Eurostat, 2016

Households without access to Internet at home, because of privacy or security concerns



Source: Eurostat, 2016

Reason for not having Internet access at home



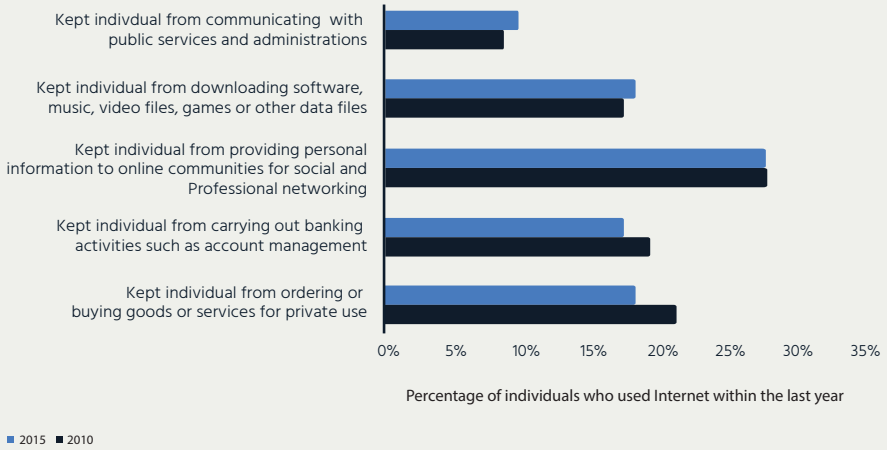
Source: Eurostat, 2016

According to Eurostat, 25% of European Internet users experienced general security issues on the Internet, including viruses, abuse of personal information, financial losses, or children accessing inappropriate websites.[16] With regard to the issues relevant to this report, 3% experienced abuse of personal information, and 3% experienced financial loss.

Some Internet users in the EU cited Internet activities they were not willing to engage in as a result of security concerns, including online banking, e-commerce, social networking, and interacting with public authorities. The greatest level of concern was just under 30%. Further, there was relatively little variation between 2010 and 2015, the two years in which these questions were asked.

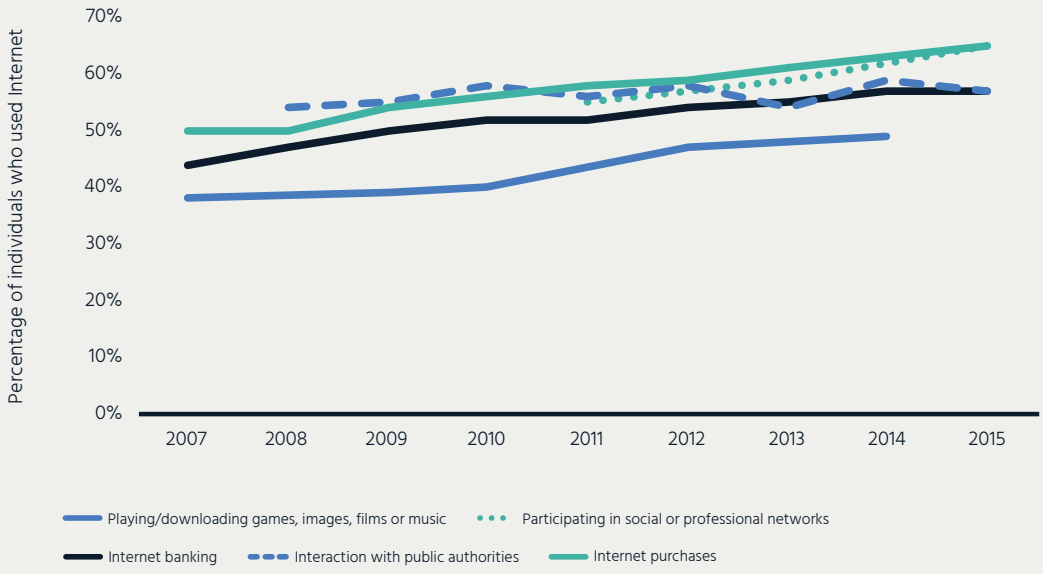
As in the US, growth of use of the corresponding services has nonetheless been steady over the years. It is not possible to gauge the impact of the expressed security concerns on use. But up to 65% of Internet users in the EU are now engaging in services that require personal information such as online banking. Of course, that means a significant minority of Internet users are still not using such online services.

Activities via Internet not done because of security concerns



Source: Eurostat, 2016

Internet activities



Source: Eurostat, 2016

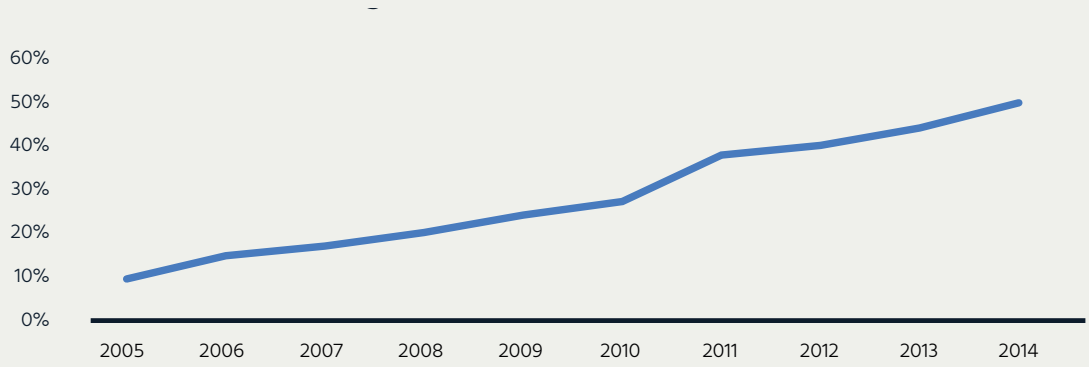
Brazil

The Regional Center for Studies on the Development of the Information Society – known as Cetic.br – has been gathering survey data in Brazil over the past ten years. The data provides evidence of the value of detailed long-term surveys in assessing Internet issues in general, and for us in assessing the impact of security concerns on users in markets less developed than the US or the EU.

Over the past decade Brazil made impressive strides, during a period in which household and individual Internet adoption began under 10%, and ended at 50% for households, and over 60% for individuals (who may not always access from home).

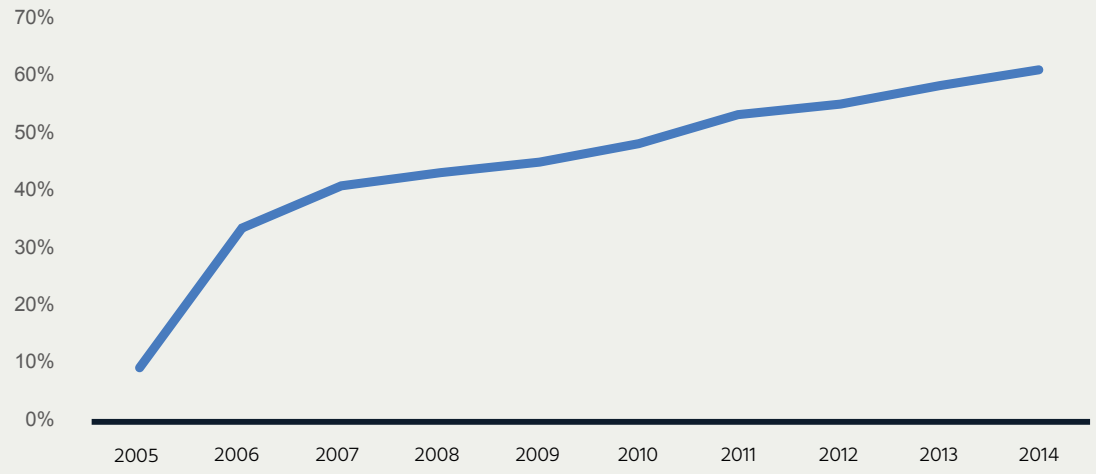
Households without Internet access citing security and privacy concerns as a reason for not going online have been climbing relatively steadily over the past ten years, reaching 12% in 2014. However, as in the US and the EU, this was the least cited reason for that year (along with concerns about dangerous content). Instead, households cited a lack of need or interest quite highly, as in the US and the EU, with more emphasis on cost and availability of a computer, as would be expected in an emerging market.[17]

Percentage of households with Internet



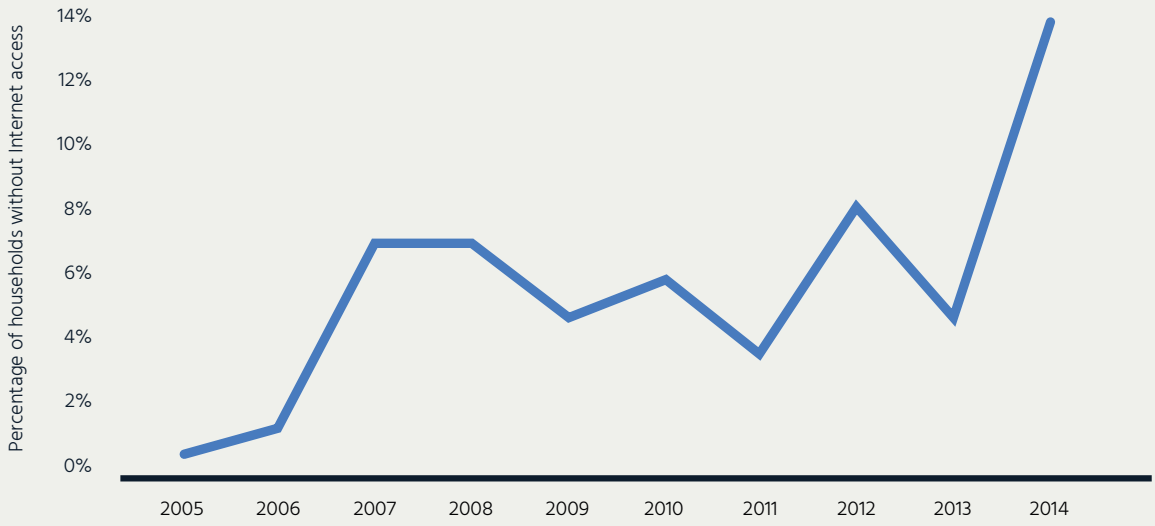
Source: Cetic.br

Percentage of individuals with Internet



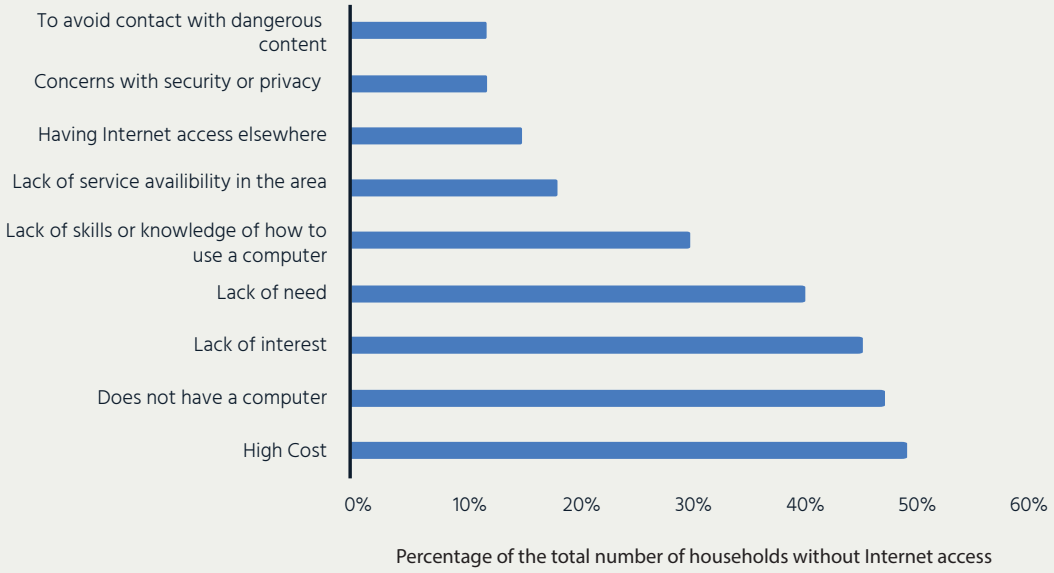
Source: Cetic.br

Non-users citing privacy and security reasons



Source: Cetic.br

Proportion of households without Internet access by reason for not having Internet

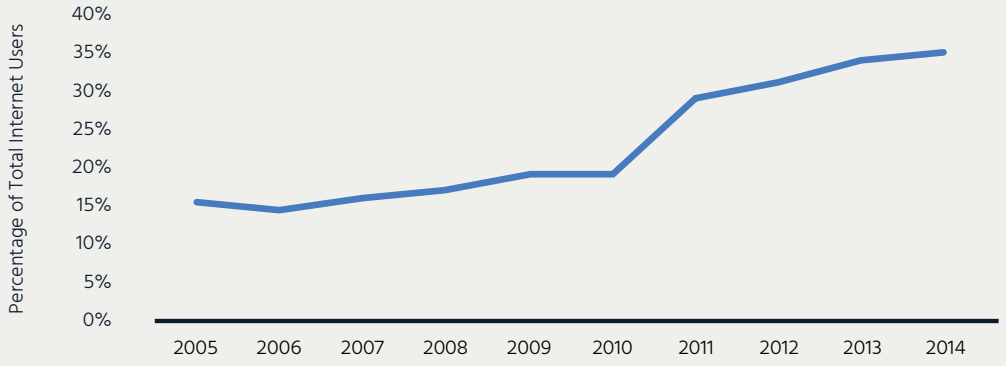


Source: Cetic.br

Key online activities, namely e-government and e-commerce, have been growing steadily among Internet users, albeit to relatively low levels, with only 35% using these services, as shown in the top graphs below.

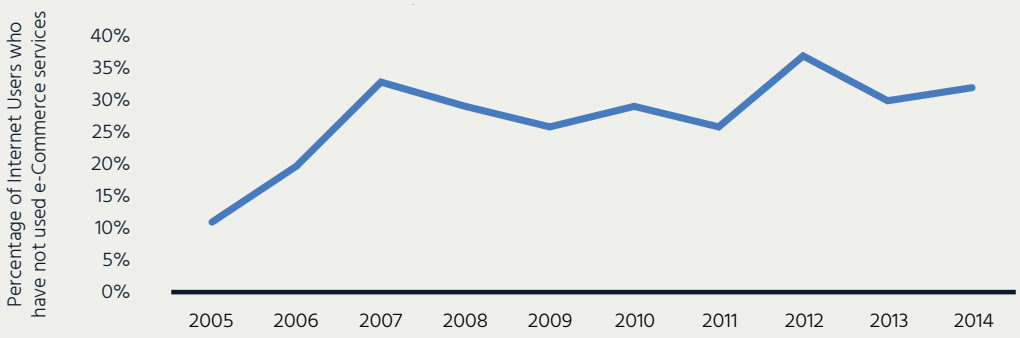
With respect to e-commerce, the most cited reasons for not transacting online were related to demand, while the same is basically true for e-government services. Nonetheless, as shown in the bottom graphs, security and privacy are factors in decisions not to engage in these online activities and could be holding back the growth of Internet use in Brazil.

E-commerce users



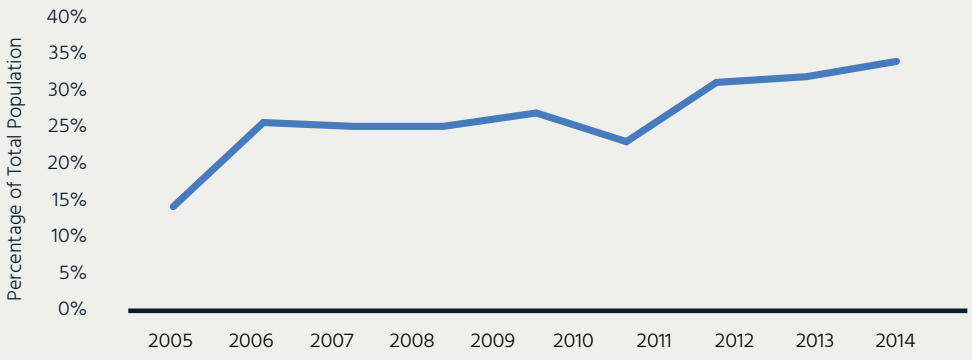
Source: Cetic.br

Non e-commerce users citing security and privacy concerns



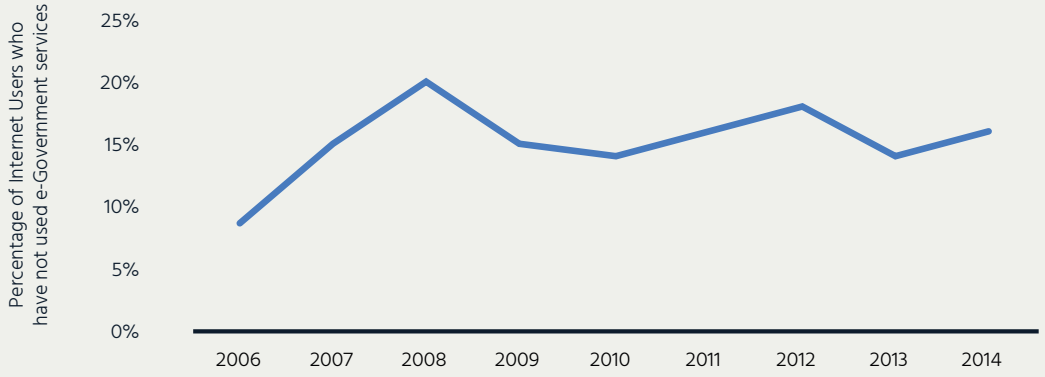
Source: Cetic.br

E-government users



Source: Cetic.br

Non e-government users citing data security concerns



Source: Cetic.br

Consumer loyalty

While these surveys cover the broad impact of privacy and security issues on users' trust, they do not focus exclusively on the impact of data breaches. There are other surveys that focus on this topic, from the narrower lens of impact on users as consumers of the companies who were breached. The results show that consumer loyalty would be shaken by a data breach, representing a significant cost to companies who experience one.

One survey of five countries (US, UK, Germany, Australia and Japan) asked how likely a customer would be to do business with a company that had experienced a data breach in general, involving personally identifiable information, or involving financial and sensitive information.[18] The willingness to do business with such a company decreased as the information breached became more sensitive, as one would expect. With respect to financial and sensitive information, the global results are below.

Globally, 40% of respondents said they would never again do business with such a company. Within countries, this ranged from 25% in the US to 55% in Japan. The results are not surprising, yet still sobering.

When asked, a global average of 49% of consumers felt companies are not taking the protection and security of customer data seriously enough.

These results suggest companies have their work cut out for them. Should they fail to justify trust, they will face significant customer loyalty challenges, particularly for losing the most sensitive of personal information.

Willingness to do business with a company where financial and sensitive information was stolen

Source: SafeNet

Summary

People in a wide range of countries indicate a concern People in a wide range of countries indicate a concern with online privacy and security issues. For non-users, there is a small impact on their willingness to go online. For those already online, the concern is stronger and impacts the willingness to use services requiring personal information.

While privacy and security concerns are not yet an epidemic, as more and more users are affected by data breaches, they will become more sensitive to the risks and may reduce their use of the Internet accordingly. This is generally true, but also specifically true with respect to using the services of the companies that were breached.

There is also financial cost associated with these breaches, in addition to the impact on customer loyalty. While the overall costs are significant, organisations may not fully account for the impact of breaches on users, and their trust and use of the Internet. This reduces the incentive for organisations to prevent them.

Data breaches have a significant impact on the organisations breached, as well as their users.

For a breached organisation, there are significant costs, both direct and indirect. The direct costs include investigation and compensation to those whose records were breached as well as the cost of recovery. Indirect costs include reputational costs, loss of customers, and negative stock price impact.

Given the increased amount of data organisations are gathering, and the increased risk of breaches, they are spending a significant amount of money on cybersecurity, to prevent, detect and mitigate breaches, and on cyber insurance, for help in the aftermath of a breach.

Connecting the unconnected

These surveys shed important light on the Internet Society's objective of promoting and restoring trust in the Internet. They are equally relevant for the Internet Society's other main goal – connecting the unconnected.

In the US and the EU, the main reason for households not going online is a lack of need or interest in the Internet. This is an accurate reflection that availability and affordability are no longer issues for most of these populations.

Even in emerging Brazil, however, where cost and ownership are primary concerns for households not going online, a lack of need or interest in the Internet is almost as important.

Addressing the lack of need or interest in the Internet has been the subject of a number of recent Internet Society papers focusing on the value of increasing local content to bring people online.[19]

However, many of the costs of a breach fall on other third parties. For instance, when Target stores were breached for credit card data, the financial institutions bore the cost of replacing the credit cards, and followed with lawsuits to recover losses from Target. Indeed, Target itself was breached through a connected contractor, whose defences were weaker but it may not have borne any of the direct cost of the breach. Even Target customers, whose credit card details were the target of the breach, had to sue for compensation, finally reaching a legal settlement.[20]

Users do not seem to be fully in the equation in calculating the cost of data breaches, which is of particular concern to the Internet Society. Specifically, users are typically considered in terms of the cost to the organization following a breach, relating to the cost of notification, identity protection, lost business, and discounts to keep customers. However, few studies show the full cost of the breach for users separate from the cost to organizations, in terms of any user liability for fraud, time spent on trying to be compensated for fraud and restore their identity and credit, not to mention the non-financial cost in terms of anxiety and uncertainty.[21]

In addition to the financial and non-financial costs, another cost not generally considered is the broader impact on the Internet economy resulting from users choosing to limit their online engagement because of concerns about data breaches.

The lack of organisational liability for all the costs of a breach may limit the incentive to stop them.

Cost of data breaches

An accurate estimate of the total global cost of breaches is impossible to calculate. As discussed above, not all breaches have been discovered, and not all breaches discovered are disclosed, in part or whole. Further, even for the disclosed breaches, it is hard to calculate the full costs borne by the affected organisations, the individuals whose data was breached and the cost to society.

Still, Juniper Research estimated in 2015 that the cost of data breaches was around USD 500 billion, and would quadruple to USD 2.1 trillion by 2019, representing 2.2% of global GDP.[22]

In a recent CIGI publication, *Look Who's Watching, Surveillance, Treachery and Trust Online*, the authors estimated the accumulated costs of data breaches in the countries they surveyed to be between USD 5.3 trillion and USD 15.7 trillion.[23]

Another study by the Ponemon Institute took a more detailed approach. It focused on calculating the cost of data breaches among a sample of 383 companies in 12 countries who had experienced a data breach.[24]

It looked at breaches that included personal information, including at least a name as well as medical and financial records.

It also included both direct and indirect costs. The former included experts to help with internal forensics, as well as external help for those whose data were breached, such as credit monitoring. Indirect costs included customer loss in the wake of the breach.

This study had the following results for 2016:

- Average total cost of a data breach: USD 4 million (up 29% since 2013)

- Average cost per lost record: USD 158 (up 15% since 2013).

The cost per lost record is quite high already – USD 158 – and is an average. In the US it is USD 221 compared with USD 61 in India; while in the health sector the average overall is USD 355 per record compared with USD 80 per record in the public sector.

The greatest cost component for organisations, on average, is lost business. This confirms the impact of a data breach on consumer loyalty. The second highest is the cost of working with customers and remediation, closely followed by the cost of detection.

These breaches can threaten to overwhelm an organisation. One health clinic breached for personal information, including medical histories and social security numbers, publicly announced they could not survive if they had to pay the 200,000 affected patients for credit monitoring services. This leaves the patients with little alternative other than a law suit (which could, of course, have the same impact on the clinic's finances).[25]

Given these high costs of data breaches and the costs of other cyber attacks, it is not surprising spending on cybersecurity is high and increasing. The result is a healthy market for those in the cybersecurity business:[26]

- Annual spending USD 75 billion in 2015, growing to USD 170 billion by 2020 (Bank of America Merrill Lynch)
- ISE Cyber Security Index of stocks beat the S&P 500 by 120% between 2010 and 2015.
- 1 million cybersecurity job openings globally (Cisco) in spite of a salary premium of 9% over other IT jobs (Burning Glass Technologies)

In light of the high and increasing level of losses through security breaches, not surprisingly the cyber insurance market is growing rapidly.

One study has insurance spending at an annual level of USD 2.5 billion, set to triple by the end of the decade (PwC). Within that spending, however, 90% is focused on the US market, leaving significant room to grow in other countries.

Furthermore, the market is quite immature, because of a lack of data on disclosures, and the impact of human behaviour that is difficult to predict.[27]

Finally, and somewhat disappointingly, there are few studies of the cost of data breaches on the customers themselves. One such study showed a significant proportion of victims of stolen US social security numbers were the subject of identity theft. Each incident resulted in USD 3,300 in losses along with 20 hours of time and USD 770 spent on lawyers.[28] It is not clear if these costs were covered in the aftermath of that breach – in general though, users have to fight for compensation.

Conclusion

All data with respect to data breaches are trending upwards:

- Reported breaches are increasing, with an increasing number of known records breached and more that are unknown in number, meaning an increasing number of people are directly and indirectly impacted.

- Surveys do not yet indicate a significant impact of reported data breaches on non-users willingness to go online. However, as more users are impacted by data breaches, such as having their identity stolen for profit, more users will hesitate to use online services requiring personal information in general, and specifically stop doing business with a company that has been breached.

- Finally, organisations are spending more on prevention, but this has not yet noticeably lowered the number of breaches, or the impact and cost of breaches when they do occur. In turn, the cost of breaches, when calculated, typically focus on the cost to the organisation, and not the full cost for the users who were the ultimate victims of the breaches.

These trends cannot be allowed to continue, or accelerate, without significant harm to individuals' privacy and users' trust in the Internet, resulting in lower and more selective use of the Internet. This, in turn, has the potential to negatively influence the economic and social impact of the Internet on the broader economy and society.

A number of key issues and recommendations follow in the next sections that could slow or reverse this negative cycle of data breaches and distrust.

Footnotes

[1] See, for example, discussions in the previous two Global Internet Reports about connecting the unconnected at http://www.internetsociety.org.

[2] A McKinsey study of the Internet economy in 13 countries, representing 70% of the global economy, showed that the Internet contributes 3.4% of GDP, but 21% of the growth in GDP, most of it across traditional sectors. Thus, decreased trust and a corresponding decrease in usage of the Internet could slow growth worldwide. See http://www.mckinsey.com/industries/high-tech/our-insights/Internet-matters.

[3] See http://breachlevelindex.com for more details.

[4] See https://www.riskbasedsecurity.com/2016/02/2015-reported-data-breaches-surpasses-all-previous-years/

[5] See https://www.symantec.com/security-centre/threat-report

[6] "Global Cyberspace is Safer than You Think: Real Trends in Cybercrime", by Eric Jardine, Global Commission on Internet Governance Paper Series No. 16, July 2015. See https://www.cigionline.org/publications/global-cyberspace-safer-you-think-real-trends-cybercrime

[7] Data Breach QuickView, Risk Based Security, 2016

[8] See, for instance, Gemalto 2015 Breach Level Index Annual Report, p. 12, at http://www.gemalto.com/brochures-site/download-site/Documents/ent-Breach_Level_Index_Annual_Report_2015.pdf

[9] In addition to Gemalto data, presented here, that is also true for the Risk Based Security reports as well as those of Symantec.

[10] See https://www.cigionline.org/internet-survey-2016

[11] See for example http://indianonlineseller.com/2016/01/cash-on-delivery-cod-slowing-down-indian-ecommerce/

[12] For a description of the cost of cash on delivery by one e-commerce provider in Nigeria, who decided to stop offering it as an option, read https://techpoint.ng/2015/07/13/cash-on-delivery-free-delivery-are-2-worst-things-to-happen-to-ecommerce-in-nigeria-drinks-ng-founder-lanre-akinlagun/.

[13] "Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities", blog by Rafi Goldberg, May 2013 at https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other- online-activities

[14] This may not be because the devices themselves are breached, but because the number of online devices is an indicator of the owner's level of online engagement; the more online engagement, the greater the risk of being victim of a data breach.

[15] "No, the NTIA's Survey Data Do Not Show a "Tipping Point" in Behavior Due to Privacy Concerns", Scott J. Wallsten, May 15, 2016. https://techpolicyinstitute.org/2016/05/15/no-the-ntias-survey-data-do-not-show-a-tipping-point-in-behavior-due- to-privacy-concerns/

[16] See http://ec.europa.eu/eurostat/documents/2995521/7151118/4-08022016-AP-EN.pdf/902a4c42-eec6-48ca-97c3-c32d8a6131ef

[17] When the question of why not go online is posed to individual non-users, instead of households, the top reasons for not going online are lack of skills (68%), lack of interest (63%), and lack of need (48%), with cost trailing at 33%. Concerns about security and privacy are slightly higher than for households, at 16%, and avoiding contact with dangerous content, at 14%, but still are the least cited issues.

[18] For the survey, personal identifiable data was defined as 'name, email address, mailing address', while financial and sensitive information was defined as 'card details, bank account, social security number, password'. See http://www2.gemalto.com/email/2014/dp/GlobalCustomerSentiment/index.html#631 for full results.

[19] This has been discussed in the two previous Global Internet Reports, as well as a recent report on increasing content in Africa, which can be found at http://www.internetsociety.org/doc/promoting-content-africa.

[20] Target first argued that customers had no standing to sue because they had no costs (because customers are protected by their credit card companies), and then settled for USD 10 million to cover the costs to users of late payments and other issues resulting from fraud. The settlement also included an agreement to hire a Chief Information Security Officer and increase employee training and risk assessment – all steps that one would have expected to take place anyway after a breach of that magnitude. See http://www.bloomberg.com/news/articles/2015-03-19/target-agrees-to-settle-customers-lawsuit-over-breach-of-data.

[21] And, at least in the US, customers have had to sue to recover their costs, often unsuccessfully. When customers file suits in data breach cases, the companies fight back and judges often dismiss the case, because of the difficulty of proving any harm from the breach. However, there is some evidence that this is shifting as judges let lawsuits proceed. See http://www.wsj.com/articles/for-consumers-injury-is-hard-to-prove-in-data-breach-cases-1466985988.

[22] http://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion and Juniper Research Whitepaper "Cybercrime and the Internet of Threats", May 2015. While the report covers Cybercrime, they note that the primary unit of cost measured is for data breaches.

[23] https://www.cigionline.org/sites/default/files/look_whose_watching_09.16.pdf

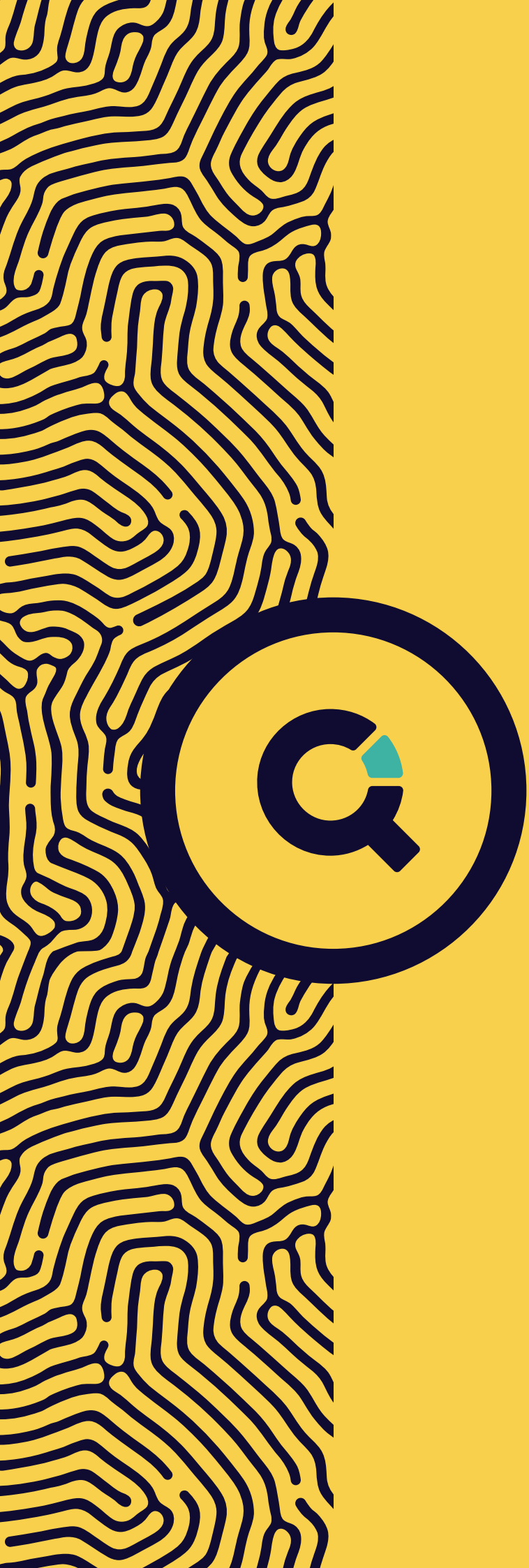
[24] "2016 Cost of Data Breach Study: Global Analysis", sponsored by IBM, conducted by Ponemon Institute, June 2016. See http://www-03.ibm.com/security/infographics/data-breach/. The report states specifically that they would not use these data to calculate the cost of mega breaches, involving millions of records, because they limited their research to the types of breaches that are in the most typical range of 100,000 or less, rather than the outliers.

[25] See http://www.zdnet.com/article/clinic-wont-pay-breach-protection-for-victims-ceo-says-it-would-be-death-of-company/.

[26] For more numbers, see http://www.forbes.com/sites/stevemorgan/2015/10/16/the-business-of-cybersecurity-2015-market-size-cyber-crime-employment-and-industry-statistics/#30d61fcd10b2 and http://www.forbes.com/sites/stevemorgan/2015/12/20/cybersecurity%E2%80%8B-%E2%80%8Bmarket-reaches-75-billion-in-2015%E2%80%8B%E2%80%8B-%E2%80%8Bexpected-to-reach-170-billion-by-2020/#7f24be0d2191

[27] A recent report noted the lack of 'reliable actuarial data' and lack of ways to measure risk, mostly 'because of the unpredictable human behaviors associated with cyber attacks.' See http://www.businessinsurance.com/article/20150610/NEWS06/150619981/1251. As discussed in the recommendation section, a startup called UpGuard is undertaking risk assessments to help insurance companies underwriting cybersecurity insurance. See http://www.forbes.com/sites/brucerogers/2016/02/11/upguard-out-to-disrupt-7-5-billion-global-cybersecurity-insurance-market/#6b7370112dda.

[28] See http://bucks.blogs.nytimes.com/2013/04/30/the-cost-to-consumers-of-a-data-breach/?_r=0



CHAPTER 3

Case Studies

Introduction

The data presented in the previous section paint a broad picture of the extent and impact of data breaches around the world. This section highlights case studies that shine a light on key issues and gives examples of the leading causes of data breaches, and their impact.

As seen in the previous section, the leading trend in data breaches is outside attacks, mostly by hackers for financial gain, but also some state-sponsored attacks, and some by hacktivists for political or moral reasons. These outside attacks can exploit a known vulnerability or use a zero-day exploit. They can directly attack the organisation, indirectly attack it through a connected third party, or via an employee using social engineering.

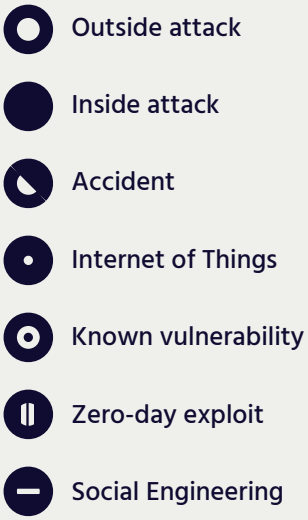
Other, less prevalent causes of data breaches are inside attacks and accidents (such as employee error). Inside attacks, by employees, may be easier to achieve than an outside attack, given the access required by, or afforded to, employees in the course of their job. The prototypical example of this is the undetected access that Edward Snowden had, as a contractor, to the secrets of the US National Security Agency (NSA). Accidents can include anything from human mistakes in developing a system that unwittingly allows access to simply losing a drive or computer with personal or confidential data.

The case studies also highlight the impact of data breaches on users, third parties, and the organisations. They show how easy some attacks are, but also how difficult it is for organisations to protect against all threats. They also show how large the impact of a data breach can be – both financially and otherwise – extending well beyond the organisation breached.

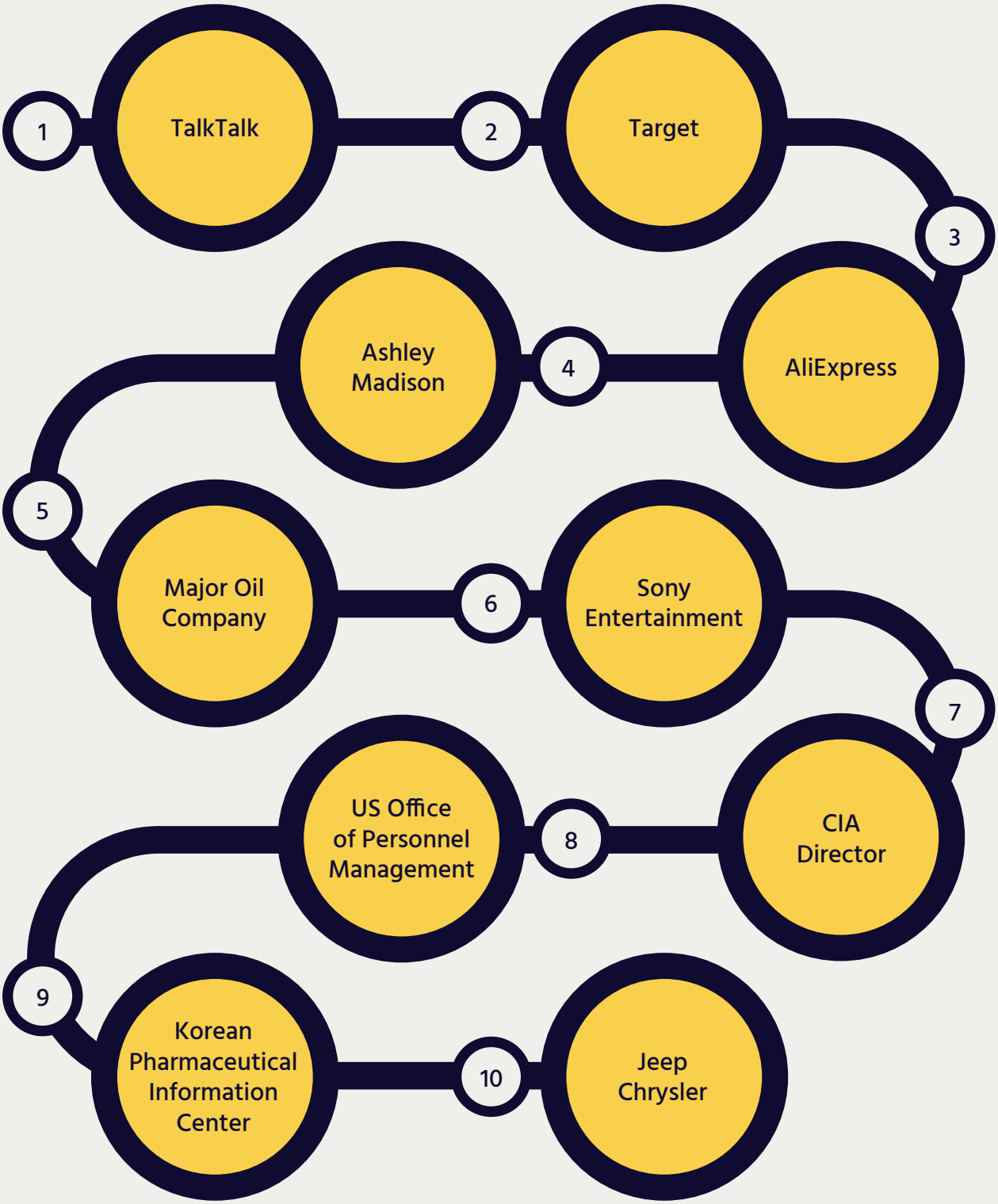
For users, the case studies highlight the increasing sense of insecurity we feel when going online, as we put trust in organisations whose security we could not possibly assess. An ever increasing number of us have been directly impacted by a data breach, or indirectly via a family member or friend.

Finally, as the world of ubiquitous Internet of Things (IoT) grows, vulnerabilities that lead to data breaches of organisations' systems can also apply to IoT, with perhaps even greater impact on users. First, of course, connected devices, such as baby monitors, can contain sensors, including for video and audio, that can yield personal information about the users. Beyond data breaches, we may also put our safety in the control of Internet connected devices, such as medical devices or connected cars, which may be susceptible to attack. While this is a broader issue than data breaches, the causes may be the same and should be considered in addressing the general security of these devices as a matter of priority.

Highlight:



Organisations:



TalkTalk

Description
TalkTalk, a UK broadband provider, was hacked in October 2015. The first indication came when the CEO received a ransom note asking GBP 80,000 for the stolen data. The hack was originally feared to cover significant data for all four million TalkTalk subscribers but was later downgraded.[1]
Please see timeline.

Leak
Eventually, it was shown 157,000 customer records were breached, including bank account and credit card details; 2,500 of these were later found for sale online for GBP 0.20 per record. While the data was not encrypted, TalkTalk had redacted six digits of the credit card numbers to make them useless. The bank details apparently only contained information that would be required to make a payment.

Cause
An initial distributed denial of service (DDoS) attack crashed its servers and may have been a distraction for the attack. The hack was achieved with a SQL Injection, and it was revealed the data was not encrypted. The UK Information Commissioner's Office (ICO) found that the SQL injection was made possible because TalkTalk had not fixed a known vulnerability. The information commissioner noted that this was a failure "to implement the most basic cyber security measures [which] allowed hackers to penetrate TalkTalk's systems with ease".[2]

Cost
The breach cost TalkTalk GBP 60 million, including GBP 15 million in lost revenue from 125,000 departing customers, and the rest in 'exceptional costs', which are not specified but likely include credit monitoring services.[3] The stock price took a dive of over 30%, which has still not recovered.

Customer impact
The breach caused customers significant uncertainty and anxiety, particularly in the early days before all the details were announced. To date, no evidence of direct financial harm has been uncovered. However, customers are more vulnerable to phishing attacks using their breached data – see timeline for further details.

Aftermath
Subsequent to the attack, five young people were arrested. Customers were provided with free credit monitoring to help prevent identity theft, and were advised to change all their passwords. TalkTalk itself replaced the need for passwords in favour of a voice biometric system to authenticate customers accessing their account information. TalkTalk was assessed a record GBP 400,000 fine by the ICO following their investigation.[4]

Lessons learned

Several young people were able to inflict tens of millions of GBP worth of costs on TalkTalk, whose CEO was first unaware of whether encryption was used, and later justified the minimal protection afforded (at least with respect to encryption). Meanwhile, customers were subject to uncertainty and stress. They still face the risk of identity theft based on the information that was hacked and sold on the dark web.

Timeline

October 21, 2015

The TalkTalk website was taken down due to unspecified 'technical issues.'[5]

October 22, 2015

TalkTalk disclosed the website was taken down to protect data from an attack.

October 23, 2015

TalkTalk provided further details, noting the possibility some sensitive data on all 4 million subscribers may have been breached, including "names, addresses, date of birth, phone numbers, email addresses, TalkTalk account information, credit card details and/or bank details."

When asked by the BBC that day if customer data was encrypted, CEO Dido Harding said: "The awful truth is, I don't know. But it would be wrong of me to give you that today, when the amount of data that these criminals have had access to is very large."[6]

October 25, 2015

October 25, 2015; CEO states "[Customer data] wasn't encrypted, nor are you legally required to encrypt it…We have complied with all of our legal obligations in terms of storing of financial information."

In terms of legal obligations, UK Data Protection Act (1998) Principle 7 states that: "Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."[7]

October 27, 2015

TalkTalk announces "[i]n the unlikely event that money is stolen from a customer's bank account as a direct result of the cyber-attack (rather than as a result of any other information given out by a customer) then as a gesture of goodwill, on a case by case basis, we will waive termination fees [for customer's wishing to leave TalkTalk]."[8] Further, TalkTalk refused to pay charges for new credit cards, unless money was taken.' The data taken, even if it could not be directly used to take money from a customers' account, could help in a spear-phishing attack to get further details from a customer. It appears TalkTalk would not waive fees if that happened, since it would involve " . . . other information given out by a customer."

November 3, 2015

When TalkTalk customer data was found being sold on the dark web, one of the customers was contacted by a journalist, and stated "I'm quite angry. It feels like your details are never safe." She stated she was particularly frustrated because TalkTalk had told her that her details were safe.[9]

November 16, 2015

Professor John Naughton states: "Companies like TalkTalk are up against professional criminals. They, therefore, need to up their amateurish game. If a company's business requires it to store customers sensitive information, then data security has to be a board-level responsibility, up there with health and safety and regulatory compliance. It is not just a matter for techies and boffins."[10]

December 12, 2015

CEO Harding seems to agree with the Professor. "It really does come back to the CEO and board. Was there sufficient oversight in terms of the security policies, the resourcing of the technology team to implement those policies, and the knowledge and understanding of best practice? It is a board level issue, not an individual issue below."[11] At this writing, she remains CEO of TalkTalk.

This author was visiting his mother-in-law in England, who was a TalkTalk customer, during the attack, and saw directly the frustration and uncertainty in the immediate aftermath of the attack when little information was available, and the website was not operating. Later, it was revealed the police advised the company not to inform their customers what had happened for a period of time. Without questioning the decisions taken in the immediate aftermath of the attack, this highlights that the bits and bytes are connected to people. Non-financial impacts of data breaches, such as loss of privacy, emotional distress, humiliation, and damage to reputation should be accounted for in all responses to data breaches, by all involved parties.

Target

Description

The Target data breach was discovered in December 2013. This was a massive loss of credit card data, with a black market value of over USD 50 million and larger cost to Target and the banks.[12] It was first reported by a security blogger, Brian Krebs.[13]

Leak

Forty million credit and debit card records were stolen between 27 November and 15 December, 2013. An additional 70 million records including personal information on shoppers, but without credit card information, were also stolen.[14]

Cause

Attackers entered Target's systems through the computer system of a Target refrigeration contractor. They installed software on Target's point-of-sale terminals, collected customer information on an internal host, and then forwarded it back to themselves (see next figure). The initial attack used known malware that may not have been found because the refrigeration contractor only used free anti-malware software that did not offer real-time protection. It also appears Target itself was vulnerable, in part, because of weak or default passwords.[15]

Cost

The cost of replacing the credit cards was at least USD 240 million. It was covered, at least initially, by the credit card companies.[16] The total cost of the fraudulent use of the cards is unknown. The cost to Target so far is at least USD 235 million, with USD 90 million covered by insurance.[17]

Customer impact

Customers are generally protected from the cost of the fraud and replacement of their credit cards. In this case, they received free credit monitoring services, and also won USD 10 million from Target in a class action lawsuit to cover costs.[18]

Aftermath

Target's CEO resigned in the wake of the theft, albeit with a reportedly large severance payment. Target committed to spending USD 100 million on chip and pin terminals. However, data is still vulnerable as long as it is not encrypted, and all other Target data, such as for online purchases, are not protected by chip and pin technology.[19]

Lessons learned

Attackers will put in significant effort to penetrate a system where valuable credit card data is available, however, Target – and its refrigeration contractor – made it easier by having known vulnerabilities to exploit. The result was a cost of hundreds of millions for Target; at least as much for the banks (subject to pending suits against Target), and unknown, and perhaps unreimbursed, costs to Target customers. It is worth pointing out the Target customers were shopping in stores, and not online, and thus unaware of the online vulnerability of their data.

Copy of Letter to Target Customers

Dear Target Guest,

As you may have heard or read, Target learned in mid-December that criminals forced their way into our systems and took guest information, including debit and credit card data. Late last week, as part of our ongoing investigation, we learned that additional information, including name, mailing address, phone number or email address, was also taken. I am writing to make you aware that your name, mailing address, phone number or email address may have been taken during the intrusion.

I am truly sorry this incident occurred and sincerely regret any inconvenience it may cause you. Because we value you as a guest and your trust is important to us, Target is offering one year of free credit monitoring to all Target guests who shopped in U.S. stores, through Experian's® ProtectMyID® product which includes identity theft insurance where available. To receive your unique activation code for this service, please go to creditmonitoring.target.com and register before April 23, 2014. Activation codes must be redeemed by April 30, 2014.

In addition, to guard against possible scams, always be cautious about sharing personal information, such as Social Security numbers, passwords, user IDs and financial account information. Here are some tips that will help protect you:

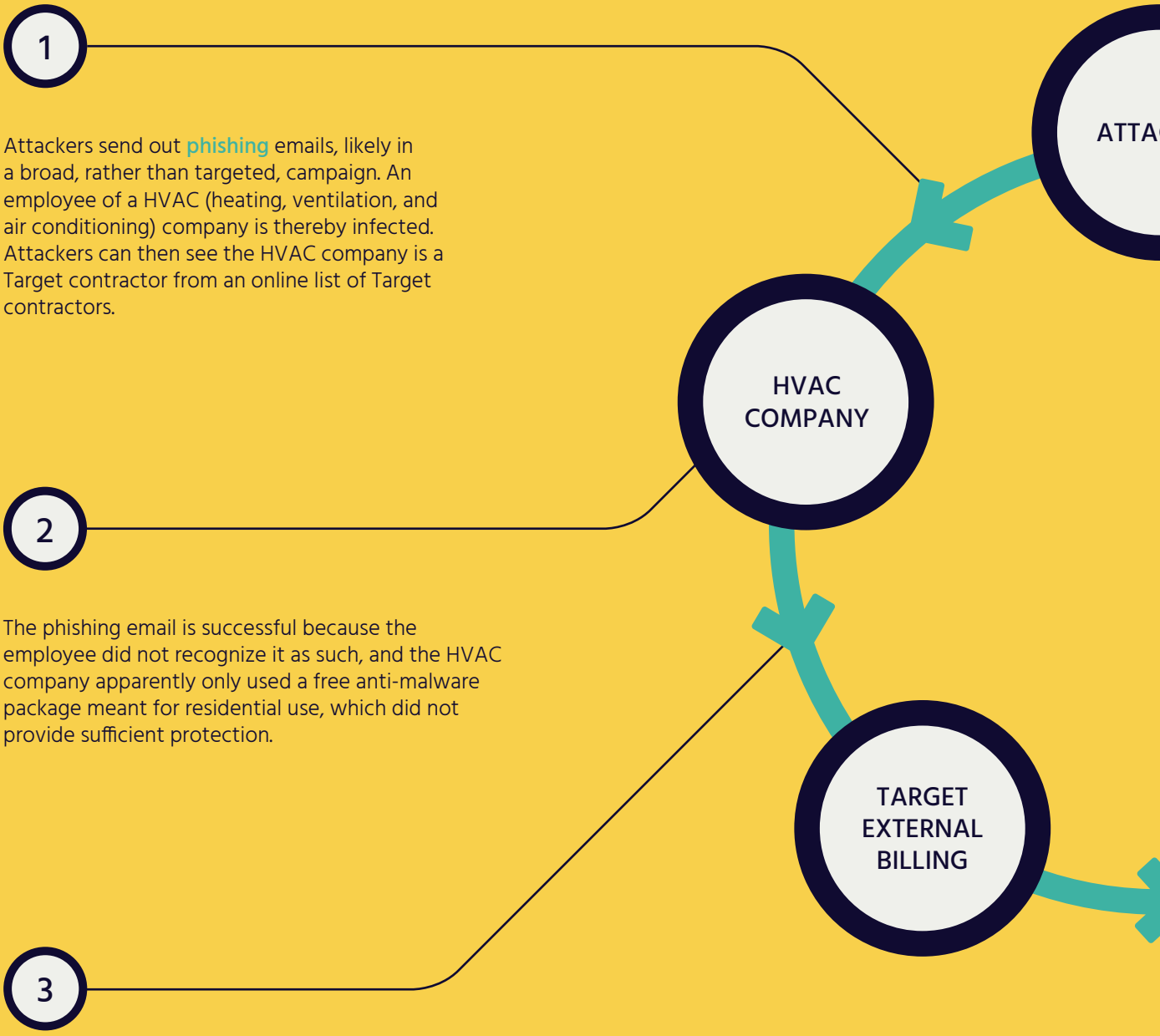
- Never share information with anyone over the phone, email or text, even if they claim to be someone you know or do business with. Instead, ask for a call-back number.
- Delete texts immediately from numbers or names you don't recognize.
- Be wary of emails that ask for money or send you to suspicious websites. Don't click links within emails you don't recognize.

Target's email communication regarding this incident will never ask you to provide personal or sensitive information.

Thank you for your patience and loyalty to Target. You can find additional information and FAQs about this incident at our Target.com/databreach website. If you have further questions, you may call us at 866-852-8680.

Gregg Steinhafel
Chairman, President and CEO

⁎ In 2015 Experian itself was breached, compromising 15 million T-Mobile subscribers' personal data, possibly including encrypted information, resulting in its own set of customer letters from Experian and T-Mobile[20]



Attackers send out phishing emails, likely in a broad, rather than targeted, campaign. An employee of a HVAC (heating, ventilation, and air conditioning) company is thereby infected. Attackers can then see the HVAC company is a Target contractor from an online list of Target contractors.

The phishing email is successful because the employee did not recognize it as such, and the HVAC company apparently only used a free anti-malware package meant for residential use, which did not provide sufficient protection.

Attackers were able to get a password to Target's billing system using Citadel password stealing software installed on the HVAC company system. It appears most contractors did not need to use two-factor authentication.

* This diagram is based on the reporting of Brian Krebs, who was the first to report on this data breach, in his blog KrebsonSecurity. All the points are not definitively known about this (or most) data breaches, because the companies do not disclose all details, possibly to prevent future breaches based on the same weaknesses, or they may not fully know themselves.

7

A new variant of the BlackPOS software used in the Target breach was used a few months later for a similar large breach at Home Depot, where the stolen cards details also showed up on the Rescator website. A budget version of BlackPOS can be purchased for USD 1800 online..

6

The card details were sold in large batches on recscator.cc. The first batch, sold prior to the acknowledgement of the breach by Target, sold for up to USD 44.80 apiece. After disclosure, when the 'valid rate' of the cards began to fall, the online price fell accordingly.

5

The data was collected on a server within Target's own system, before being sent to external servers controlled by the attackers.

4

Attackers were then able to install memory-scraping software on point of sale (POS) terminals in Target stores to collect card details. Apparently Target did not follow a strict password policy, making it easier to move between internal systems.

AliExpress

Description
In December 2014, two security flaws were found on AliExpress, an online marketplace owned by Alibaba, exposing consumers' and merchants' data to potential attackers.

Leak
An Israeli security researcher, shopping for lights, noticed users could access the personal information of any of AliExpress' 300 million subscribers by simply changing the user ID, which is '123456' in the following illustrative URL: http://trade.aliexpress.com/mailingaddress/mailingAddress.htm?mailingAdressID=123456

Another security researcher noticed it was also possible to change the price of a product before buying it. Both security researchers informed AliExpress about the flaws.[21]

Cause
These flaws appeared to be accidental mistakes in the development of the website.

Cost
According to Alibaba, with the information from the security researchers, the flaws were fixed before any costs were inflicted on consumers or merchants.

Customer impact
There were no reports of consumers impacted by the security flaws, but there is no way to know for sure whether or not they were exploited before being patched.

Aftermath
There do not appear to be any after effects of these vulnerabilities, which could have been exploited to expose the personal information of millions of users if it had not been discovered and patched quickly.

Lessons learned
This case study demonstrates how a mistake and possible lack of testing can have significant repercussions for users, and merchants, although, in this case, there is no evidence the vulnerability was exploited. While the vulnerability was discovered by a user who happened to be a security researcher, the average user or vendor would not be likely to identify this vulnerability before shopping or selling on this site, and could not reasonably judge whether the site would sufficiently safeguard their own personal information or not.

Ashley Madison

Description

The entire database of Ashley Madison, an online service dedicated to enabling extramarital affairs, was stolen and released by a group calling themselves "The Impact Team" in the summer of 2015, along with a trove of employee emails and internal documents.[22] The hackers claimed to be upset about the purpose and purported deceit of Ashley Madison, and tried to convince the company to take down the site before releasing all the data.[23]

Leak

The user data of all 37 million users, including names, hashed passwords, addresses, phone numbers, and information on millions of transactions were all leaked, along with many gigabytes of internal documentation and emails.

Cause

It is not clear how the hackers were able to access the data. Eleven million of the hashed passwords were compromised because the hackers had access to the source code used to protect the passwords. Worse, it appears the Ashley Madison developers knew the approach was not sufficient, and strengthened the protection going forward, but did not go back and protect the earlier 11 million passwords.

Cost

The cost to Ashley Madison to date is not yet known, and will ultimately depend on the result of lawsuits that have, or will be, filed. Two Canadian law firms have already filed a USD 578 million class-action lawsuit, while others are being filed in the US. Whether users of Ashley Madison are willing to publicise their membership in the course of these lawsuits remains to be seen.

Customer impact

Given the intended use of the website, the customer impact is significant and will never be fully known. Several suicides have been linked to the disclosures, many customers have been blackmailed, and the impact on customers' marriages and family life are likely to be severe. Although Ashley Madison offered a full profile deletion option for USD 19, they did not delete the data in question – this apparently contributed to the attackers' motivation.

Aftermath

The full impact on Ashley Madison depends on the lawsuits. The CEO, whose own alleged adulterous affairs were also exposed, has resigned. In August 2016, an official report was released on the breach, which noted the lack of an adequate information security framework and included an enforceable undertaking. This could serve as a guide for future data breach situations.[24]

Lessons learned

To paraphrase, Hell hath no fury like a hacktivist scorned. Users put their trust in this service, which, by definition, carried data whose release would be, at the very least, personally embarrassing. The cost to users in their marriages, from blackmail, or identity theft, may never be fully known. The success of the lawsuits seeking retribution from Ashley Madison may yet bankrupt the company.

Major Oil Company

Description

A major oil company was breached by attackers through malware embedded in a Chinese restaurant website.[25]

Leak

The attackers found a Chinese restaurant popular with employees of the oil company, and infected the online menu with malware, which downloaded the infection to the company's network. It is not known how the online menu was infected.

Cause

This is known as a 'watering hole' attack, in which the attackers infect a website used by the target rather than infecting the target directly, in the same way that a predator waits by a watering hole for its prey rather than hunting the prey directly.

Cost
As is often the case, much about this case is unknown, including the identity of the oil company, and the cost and impact of the attack.

Customer impact
Unknown, as the target chose to remain anonymous and did not provide details on what was breached.

Aftermath
The particular aftermath of this attack is unknown.

Lessons learned
As companies themselves begin to tighten cybersecurity, the attackers can go after contracted vendors (as in the case of Target), or unaffiliated companies such as the Chinese restaurant, whose security standards were presumably much lower. It also highlights that organisations are loath to provide more information than is required, which increases the challenges of understanding and addressing such data breaches.

Sony Entertainment

Description
In late 2014 a group calling itself "Guardians of Peace" hacked Sony Pictures Entertainment, demanding Sony not release the movie The Interview, a comedy featuring the assassination of the North Korean leader, and threatened cinemas that showed the movie.

Leak
The leak was comprehensive and included embarrassing emails between Sony executives, copies of unreleased movies, salaries of executives and movie stars, and personal information, including Social Security numbers, of Sony employees and their dependents.

Cause

The hackers wiped out many of the Sony computers, thereby removing evidence of the means of attack. After Sony initially cancelled the release of The Interview, in response to cinemas cancelling screenings, the US, alarmed about the attack on freedom of expression, broke with tradition by naming North Korea specifically as responsible for the attack.[26] Outside cybersecurity experts expressed some doubts North Korea was responsible, arguing it was more likely to be well-placed insiders. The FBI rejected this theory after a meeting with the cyber security company Norse.[27]

Cost

The cost of the hack to Sony was expected to be USD 35 million, covering investigation, and restoring the damaged systems.[28] At least part of this was covered by insurance.[29]

Customer impact

The leaked emails and salary details generated damaging gossip and led to the resignation of a Sony co-chairperson. Further, former employees filed four lawsuits as a result of their personal data being stolen and disclosed.

Aftermath

The hack raised significant questions about state-sponsored hacking, attacks on freedom of expression, and had wide-ranging impacts on Sony employees and their dependents.

Lessons learned

While the means of this attack is still unknown (at least outside Sony) it clearly raised the stakes in terms of demonstrating the broad impact a comprehensive cyber-attack can have on a company. The breach of privacy for employees, including the executives whose emails were leaked, as well as the employees and their dependents whose personal information was breached, is also significant. It shows how vulnerable people are even if they are not consumers, or even direct employees, of an organisation breached.

CIA Director

Description
In October 2015 a group of hackers revealed they had accessed the private AOL account of the United States Central Intelligence Agency (CIA) Director, John Brennan, and began to leak data from this account.

Leak
The hackers had access to his private email and released some of the emails publicly, which included some sensitive emails and documents from 2009.

Cause
One of the hackers called Verizon, which had recently purchased AOL, and claiming to be a Verizon employee was able to acquire the CIA Director's AOL PIN and the last four digits of his bank card. The hackers then called AOL and reset the password.

Cost
There was no apparent financial cost.

Customer impact
After learning of the breach, the CIA Director tried to reset the password several times, but the account was taken back by the hackers, so he disabled the account.

Aftermath
While some sensitive documents were apparently leaked, none were classified. Others were personal. It is not clear what actions Verizon/AOL took to remedy the breach, but after the breach, additional two-step authentication was added to AOL access. The CIA Director was quoted as concluding: "There are ways that individuals can get into the personal emails of anybody."[30]

Lessons learned
This lesson shows the perils of social engineering attacks, and why employees should be better trained as to how to handle sensitive customer information. Further, it shows how difficult it is for users to understand the security levels of an online provider such as AOL. Better tools are required to address known vulnerabilities such as the use of simple passwords by customers.

US Office of Personnel Management

Description

The United States Office of Personnel Management (OPM) announced a breach in June 2015. OPM gathers information on US federal government employees, including security clearance background information.

Leak

Personally identifiable information on 21.5 million people was taken, including Social Security numbers, names, addresses, and for some, the detailed financial and personal information needed to provide a security clearance, including fingerprints for 5.6 million employees, presumably in the most sensitive positions.

Cause

The breach was active for more than a year and appears to have been discovered when a cyber security company demonstrated its forensic products on the OPM system, and then helped with the incidence response.[31] It is not clear how the system was infiltrated, but it is clear OPM knew of security vulnerabilities, and key data was not encrypted, possibly because of the age of OPM's computer systems.[32] The breach was assumed to originate from China. The Chinese government denied it was state-sponsored, and later arrested individuals who they said were responsible.[33]

Cost

OPM awarded a contract for USD 133 million to a company to provide three years of credit monitoring for all employees and former employees whose data was taken. It is not clear if or what the OPM is doing to update their system and cybersecurity.

Customer impact

In addition to the financial risk of identity theft, employees are subject to potential blackmail attempts based on the information in their background checks, particularly those who had very detailed and personal investigations before being granted access to classified information, while agents outside the US can be definitively identified based on their stolen fingerprints.[34]

Aftermath

The director of OPM resigned after the full extent of the breach was revealed, and then the Chief Information Officer resigned two days before she was scheduled to testify before a US House of Representatives panel. A Congressional report on the attack showed the vulnerabilities were known and the attack was preventable.[35]

Lessons learned

This case is a lesson in false economies, as it appears the old systems were vulnerable to attack, OPM did not have the capabilities to detect an attack, and had not encrypted the data to mitigate the impact. As a result, those employees entrusted to safeguard government secrets were themselves at risk.

Korean Pharmaceutical Information Center

Description

Medical information on most of the population of South Korea was sold without consent, to a processing company for profit.[36]

Leak

KPIC and another company in Korea sold data on 43 million Koreans (almost 90% of the population), to a multinational called IMS Health Korea, which processed it in the US and sold it back to companies in Korea for usage.

Cause

This is generally considered an insider breach although it is not clear whether the company itself participated in the sale, which generated a profit of USD 8.59 million in revenue for the company that bought and resold the data.

Cost
The financial cost of the breach is unknown as yet; the cost in privacy to the patients whose data was sold and processed is unmeasurable.

Customer impact
The sale and use of the data are clear violations of the individuals privacy, and gives the pharmaceutical companies who purchased the data personal information on individuals, including their health records.

Aftermath
The breach seems to have violated two laws – first, for unauthorised usage of personal and medical information in the initial sale, and second, for unencrypted transfer of the medical information to the US by the buyer of the data.[37] Twenty-four people were criminally indicted – the outcome of those cases, as well as any penalties imposed on the companies, is not yet known.

Lessons learned
It is not clear whether it would be worse if the company knowingly sold the health information, or if it was the action of rogue employees. Either way, the personal information was sold without the knowledge, much less consent, of the patients, and represents a breach of individuals' privacy. Their most sensitive personal information was processed and will be used in ways that the patients could not have foreseen, would not want, and may never know.

Jeep Chrysler

Description
Two security researchers demonstrated the ability to control a Jeep's steering, brakes, and transmission, via its connected entertainment system from a remote computer over a wireless connection.[38]

Leak

This was an outside attack conducted by the two security researchers, which was shared with Chrysler before the researchers presenting and demonstrating their results.

Cause

The security researchers were able to find a vulnerability in the Uconnect entertainment system that enabled them to rewrite the firmware in a key chip used to control the vehicle.

Cost

In response to the information provided by the researchers, Chrysler issued a recall for 1.4 million vehicles, and also blocked the attack passing through the Sprint network used to communicate with the vehicles. However, the update to the system needs to have a USB drive plugged into the vehicle, by the owner or the dealer, which will likely result in not all the cars being patched.

Customer impact

In the case of the Jeep exploit, the researchers demonstrated they could take over the Jeep by cutting the transmission and the brakes, causing the (terrified) Wired reporter to drive into a ditch on a busy highway. While this is more of a security breach, the researchers could also use the vulnerability to track Jeeps, demonstrating the Internet of Things can generate sensitive data, which can be breached.

Aftermath

While Chrysler argued the vulnerability was not a defect, but rather the result of a hacker, similar to a vandal slashing a tire, the US Congress deliberated on (but did not pass) an Act to help protect connected cars from hackers.[39] In the meantime, the two security researchers were hired by Uber, to help protect planned autonomous cars.

Lessons learned

As Internet access is added to existing devices – be they cars, medical devices, or baby monitors – it subjects them to the same vulnerabilities as online services. The data gathered can be monitored, such as the location of the Jeeps, or the devices themselves can be taken over, with potentially lethal consequences. It seems clear, at least in this case, that Jeep did not assume much, if any, liability for the flaws that had been demonstrated.

Conclusion

In practice, data breaches have a range of causes and impacts. Some of the breaches highlighted here are hard to understand because a known piece of malware, some of which can be purchased online such as the BlackPOS, leads to breach after breach without prevention. Others are puzzling because no one knows, or reveals, how they were accomplished, leading to little learning and no prevention.

All breaches can have an impact on the organisation, its employees, customers, and even third parties. In some cases, the organisations face a steep financial and reputational cost and the CEO resigns. In some cases, employees, and even their families, have their personal details and emails leaked. And in most, cases, the users who put their trust in an organisation for professional financial, health, or even amorous services, bear the brunt of the breach.

Looking forward, the known data breaches may be the tip of the iceberg for users. It is incredibly distressing to have one's health records stolen and sold. It is potentially fatal to have one's health devices hacked and overridden. As the Internet of Things is taking hold, people are increasingly putting their lives in the control of devices provided by companies whose core focus is on manufacturing or service provision, rather than data security, and may not understand the vulnerabilities and what attackers are capable of doing to their newly connected devices, or how to prevent it.

The next section raises the known issues contributing to data breaches. If these breaches cannot be addressed, it is hard to see how the next generation of devices and systems will be adequately protected.

Footnotes

[1] See http://www.theregister.co.uk/2015/10/27/talktalk_incident_management_review/ and http://www.itpro.co.uk/security/24136/talktalk-hack-what-to-do-if-hackers-have-your-data-20 for more details.

[2] See https://www.ft.com/content/15ea6930-8b07-11e6-8aa5-f79f5696c731.

[3] The ICO said TalkTalk "should and could have done more to safeguard its customer information". See https://www.ft.com/content/15ea6930-8b07-11e6-8aa5-f79f5696c731.

[4] See http://www.m2computing.co.uk/hack-cost-talktalk-60-million-and-101000-customers/.

[5] Unless indicated otherwise, this timeline is based on the article "TalkTalk incident management: A timeline, The Register, 27 October, 2015. See http://www.theregister.co.uk/2015/10/27/talktalk_incident_management_review/.

[6] See http://www.bbc.com/news/business-34618187.

[7] See http://www.legislation.gov.uk/ukpga/1998/29/schedule/1/part/I/paragraph/7, see also http://www.theregister.co.uk/2015/10/26/talktalk_encryption_dpa/ for interpretation. A more recent recommendation by the UK Information Commissioner's Office (ICO), suggests that a lack of encryption of the data following a breach may result in a fine, but there is no set rule, see http://www.welivesecurity.com/2016/04/21/encrypt-or-face-a-huge-fine/. For the ICO discussion on encryption see https://ico.org.uk/media/for-organizations/encryption-1-0.pdf.

[8] See also http://www.contextis.com/resources/blog/communicating-cyber-attack-retrospective-look-talktalk-incident/.

[9] See http://www.lbc.co.uk/exclusive-lbc-tracks-down-talk-talk-hacking-victims--119043

[10] See http://www.itpro.co.uk/security/24136/talktalk-hack-what-to-do-if-hackers-have-your-data-20

[11] Id.

[12] See http://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers/

[13] Brian Krebs apparently discovered that Target had been breached by identifying the banks that had issued a batch of cards that had gone for sale on a black market site, and learning that all had been used at a Target outlet recently. See http://ajr.org/2014/06/16/reporter-mingles-criminals-cover-cybersecurity/.

[14] See tp://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers/

[15] See http://krebsonsecurity.com/2015/09/inside-target-corp-days-after-2013-breach/

[16] The cost to replace 21.8 million of the 40 million cards was USD 240 million, covered by the banks, and not Target – Target is only liable to cover the cost of any fraud taking place on the cards. See http://blog.credit.com/2014/02/target-data-breach-cost-banks-240-million-76636/. Target made a deal with Visa to pay USD 67 million related to the fraud, and now faces a class action suit by the other financial institutions that issued cards that were subject to the Target data breach. See https://consumerist.com/2015/09/16/target-to-face-class-action-lawsuit-from-banks-over-data-breach/.

[17] See http://www.businessinsurance.com/article/20140806/NEWS07/140809889

[18] These costs could include the time to deal with fraudulent claims. See http://money.cnn.com/2015/03/19/technology/security/target-data-hack-settlement/

[19] Chip and pin cards make it difficult to create counterfeit cards, but do not prevent their use online, and without end-to-end encryption, do not prevent the numbers being taken at the point of sale. See https://www.theguardian.com/commentisfree/2014/may/06/target-credit-card-data-hackers-retail-industry.

[20] See http://http://www.t-mobile.com/landing/experian-data-breach.html

[21] See http://www.latimes.com/business/technology/la-fi-tn-alibaba-security-breach-20141210-story.html.

[22] See https://securityintelligence.com/two-important-lessons-from-the-ashley-madison-breach/ and http://www.tripwire.com/state-of-security/security-data-protection/cyber-security/the-ashley-madison-hack-a-timeline/ for more details.

[23] See http://www.ibtimes.co.uk/ashley-madison-hack-who-are-impact-team-why-did-they-leak-website-data-will-they-be-caught-1516328.

[24] See http://www.dataguidance.com/international-ashley-madison-report-likely-to-serve-as-benchmark/

[25] "Hackers Lurking in Vents and Soda Machines", by Nicole Perloth, 7 April 2014, New York Times. See http://www.nytimes.com/2014/04/08/technology/the-spy-in-the-soda-machine.html.

[26] Typically, the US does not specify the country responsible for a cyberattack, but in this case broke with precedent to stress the importance of freedom of expression. See https://www.washingtonpost.com/world/national-security/why-the-sony-hack-drew-an-unprecedented-us-response-against-north-korea/2015/01/14/679185d4-9a63-11e4-96cc-e858eba91ced_story.html

[27] See http://www.politico.com/story/2014/12/fbi-rejects-alternate-sony-hack-theory-113893

[28] See http://www.networkworld.com/article/2879814/data-center/sony-hack-cost-15-million-but-earnings-unaffected.html. Other estimates put the cost higher than that, at closer to USD 100 million. In addition, the cost of lost revenues for The Interview and the other unreleased movies that were leaked is not known.

[29] See http://www.cnet.com/news/sony-pictures-hack-to-cost-the-company-only-15-million/

[30] See http://motherboard.vice.com/read/john-brennan-aol-email-hack-60-minutes-no-ones-emails-are-safe

[31] See http://arstechnica.com/security/2015/06/report-hack-of-government-employee-records-discovered-by-product-demo/

[32] As noted in this article, a number of government agencies signaled the significant unresolved deficiencies in data security at OPM prior to the data breach. See http://www.slate.com/articles/technology/future_tense/2015/06/opm_hack_it_s_a_catastrophe_here_s_how_the_government_can_stop_the_next.html.

[33] See https://www.washingtonpost.com/world/national-security/chinese-government-has-arrested-hackers-suspected-of-breaching-opm-database/2015/12/02/0295b918-990c-11e5-8917-653b65c809eb_story.html

[34] See also https://www.lawfareblog.com/why-opm-hack-far-worse-you-imagine.

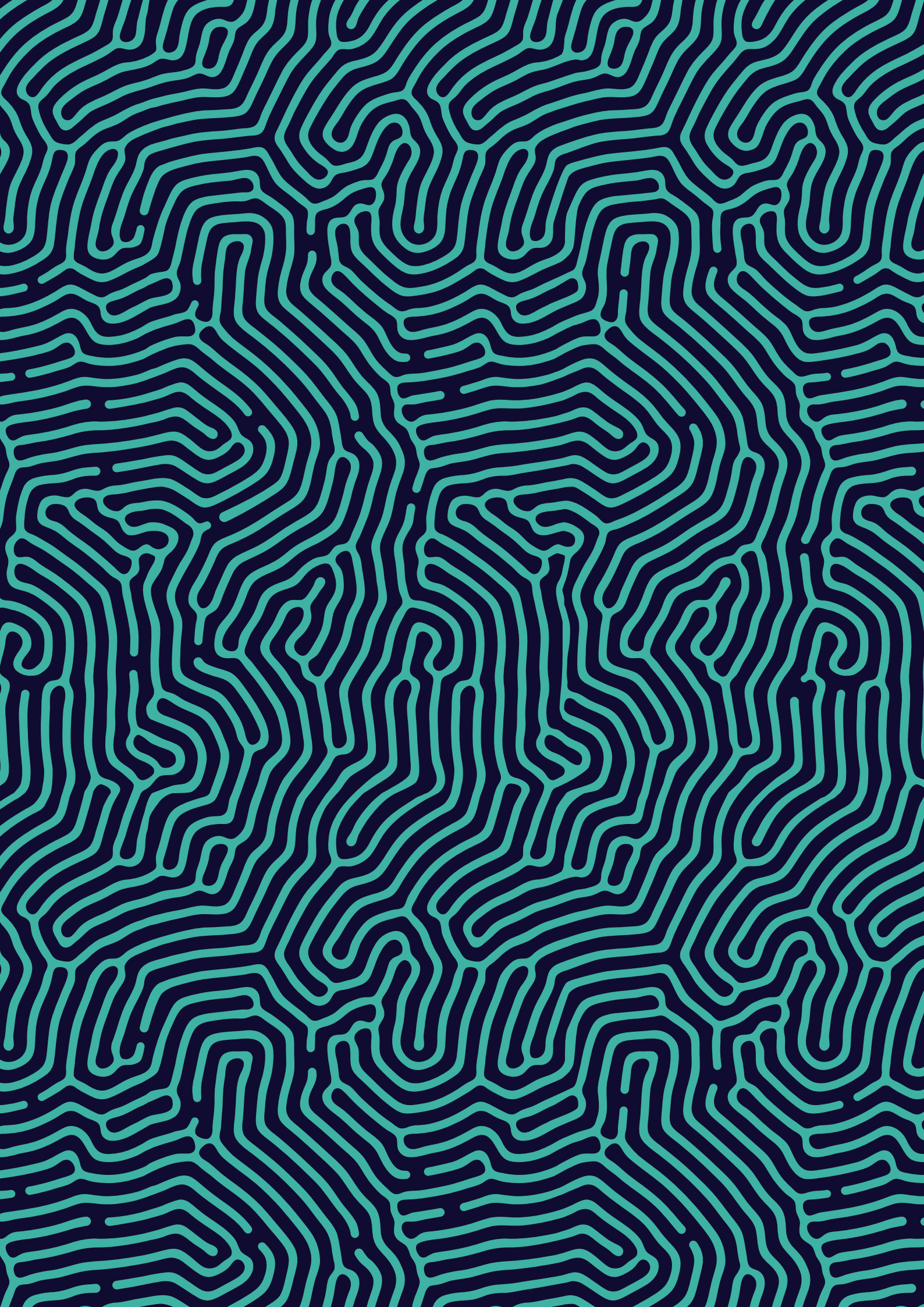
[35] See http://www.infoworld.com/article/3117353/hacking/opm-hack-was-avoidable-says-congressional-report.html

[36] See https://www.databreaches.net/43-million-south-koreans-had-their-medical-information-leaked/

[37] IMS Health claims to have encrypted patient registration numbers that would be used to identify them, but according to one source, the encryption involved simply replacing numbers with letters. See https://www.databreaches.net/south-korea-major-health-data-breach-hits-sector-weak-in-compliance/.

[38] See https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

[39] See http://www.wsj.com/articles/is-a-hacked-vehicle-also-defective-1440457334



CHAPTER 4

Issues

Introduction

The issues related to data breaches – their causes, impacts, and solutions – are vast. The data breach trends section shows that the source of data breaches can be from outside attacks, whether initiated by hacktivists, state-sponsored hackers, or attackers motivated by financial gain. They can be inside attacks with their own set of motivations; or they can result from accidental loss. The case study section highlights the reasons for and ways to a system, and the resulting impacts on the organisation, its customers, and others. We now focus on a set of issues that emerge repeatedly, and point the way toward recommendations.

First, the impact of data breaches can be extensive, and broad-ranging. In the case of the Target breach, there were significant financial costs imposed on Target, on the banks forced to replace compromised credit cards, and on customers having to address the resulting fraud. In the case of Ashley Madison, the costs extend far beyond the financial as users' personal affairs were exposed. In the case of the Office of Personnel Management, not only were employees' and others' private data exposed, but the breach made it possible to establish the identity of certain employees by using stolen biometric information, with unknowable consequences.

In the face of these financial and non-financial costs, it is puzzling to learn many of these breaches exploited known vulnerabilities, and were preventable. For some of these, there were patches available, but they were not used. Some involved social engineering attacks on employees, again using known approaches, which are possible to guard against.

Of course, not all breaches result from attacks, and not all attacks are preventable. Some are the result of attacks using zero-day exploits that were not known before they were employed. Others result from an accidental disclosure of data, sometimes through the loss of a device containing sensitive data. While not preventable, given how common they are, such breaches are at least foreseeable. Therefore, it is possible to mitigate the impact.

The question here is 'why?' Why, given the cost of a breach, more is not done to address the preventable ones, and to lower the cost and impact of foreseeable ones? This is where the economics of trust becomes relevant.

This section is organised as follows. First, it outlines the actions that could be taken prevent the preventable attacks, and to mitigate the non-preventable attacks. It is followed by the economics of why such actions are not uniformly taken.

Security gaps

Many attacks are preventable

It is striking to learn many, if not most, attacks, could be prevented with up-to-date systems and employees trained in data security and how to avoid social engineering attacks. One recent study of reported data breaches stated 93% were avoidable.[1]

Known vulnerabilities

According to a Verizon report, 70% of outside attacks rely on known vulnerabilities, some of which date as far back as 1999.[2] Further, the report shows ten known vulnerabilities accounted for almost 97% of the security exploits for 2014, and 85% in 2015.[3] While these must be patched, that still leaves a long tail of known vulnerabilities to address.

Another report raised a specific angle of the same problem. Symantec showed 78% of websites they had scanned had known vulnerabilities. Further, 15% of these were critical, allowing malicious code that could result in a data breach, and compromise visitors to the websites.[4]

As one prominent example of security challenges, many web attacks focus on third-party plugins. These include web browser plugins such as the Adobe Flash Player, which has been a significant source of attacks over the years, including a large proportion of zero-day exploits.[5]

Plugin issues are not restricted to browsers, but also impact websites. WordPress is the basis of 25% of global websites and allows anyone to write a plugin. These plugins increase the functionality of websites, for instance enabling easy entry of contact details, but may also be vulnerable to attacks such as SQL Injections.

Software providers can enable third-party developers to add features to their software through plugins. For instance, web browsers enable plugins to be developed and installed by users to run audio, video, or offer other features such as changing the look and feel of the original software.

A common example of a plugin is Adobe Flash, which enables audio or video playback on web browsers. Developers of video content can make it available in Adobe Flash, and users will be prompted to download the Player plugin to view such content if they do not already have it.

The features that make plugins valuable also make them vulnerable. The ability to use plugins allows third-party developers to add functionality to the underlying software platform. Ready-made solutions such as Adobe Flash can help simplify the way that content is served, making it easier for providers to deliver content.

This helps to promote content availability. However, it also creates more targets for attacks because the user base is larger, and the plugins can be developed and installed separately from the underlying platform, which reduces the ability to screen the software and prevent attacks.[6]

While not all attacks on websites focus on plugins, they offer a good illustration of the challenges resulting from opening a platform to third-party software that may have security vulnerabilities.

Social engineering

Social engineering is a common technique hackers use to gain entry to a closed system. Employees are tricked into giving up their passwords or directly introducing the infection themselves.

One popular practice is called phishing. An official-looking email directs users to login to a fake site or includes a malware attachment. Spear-phishing is a more targeted, and lucrative, approach than simple phishing.

There is evidence these phishing campaigns are quite effective, even against security companies. This technique was used to attack Target, via their refrigeration contractor.

According to Verizon, in one test 150,000 emails were sent out and within the first hour, 50% of users had opened them and clicked on phishing links, with the first click coming within 82 seconds.[7]

A more recent trend is known as spear-phishing, which is more targeted than a general phishing campaign. In this case, the emails target employees of a particular company, and often specific employees, providing more details than a typical phishing email, to increase the chances the attack is successful.

The attackers may even use social media to learn about the target employee or company to make the email look like it comes from someone who knows the target.

These campaigns can get even more targeted, using specific information about a company to deliver instructions, typically from a travelling CEO. Using a fake email address, the attackers request to transfer money as part of a transaction. As improbable as it sounds, in one case such a campaign led a company to transfer USD 46.7 million to overseas accounts.[8]

Phishing is not the only means of social engineering an attack. Some experiments have been conducted in which USB memory sticks were dropped in areas such as employee parking lots. Up to half were plugged in, the first in as little as six minutes.[9] In these cases, the USB stick relayed back to the researchers that it was opened, but a malicious person could have infected the computer with malware.

The problem of social engineering is magnified by common work trends. With the increase in homework, along with 'bring your own device' (BYOD) policies enabling employees to use their PCs or mobile devices, which may not be sufficiently protected, a social engineering attack on an individual through his or her personal device could also compromise the employer's system.

The human tendency to re-use passwords does not help. If someone uses the same password in their private and professional lives, a phishing attempt could compromise their corporate network, leading to a data breach.

A number of password shortcomings, including re-use, were recently revealed by the full release in 2016 of 167 million user accounts from LinkedIn that were hacked 4 years earlier in a massive data breach. This leak had significant implications.

First, Mark Zuckerberg illustrated how it is common to re-use passwords. His password on LinkedIn was apparently 'dadada' and hackers used that to take over his Twitter and Pinterest accounts, mainly, it appears, to brag they had done so.[10]

Second, it may not always be necessary to use social engineering to learn a password, as the most common password turned out to be '123456' followed by 'linkedin', and then, of course, 'password'.[11]

Not all attacks are preventable

It is not possible to protect against all cyber vulnerabilities. Some are unknown, or difficult to fix. Other breaches result from accidental loss or release of data. In all cases, however, actions can be taken to mitigate the impact of the outcome.[12]

Unknown vulnerabilities

While it is possible to protect against known security vulnerabilities, at some point each known vulnerability was unknown, and so there would be no way to prevent such attacks.[13] These are called zero-day exploits.

According to Symantec, the number of zero-day exploits has been increasing in recent years, to 54 in 2015; versus 24 in 2014, and 14 in 2013. Of course, by definition, not all zero-day exploits are known today, some may be waiting for the right target or the right price.

There is a sophisticated black market for zero-day exploits, which can be sold to hackers, governments, and the companies who produced the software. Once the zero-day is used, it may become a 'half-day' exploit used on targets that have not yet patched the vulnerability.[14]

Market prices for a zero-day exploit depend on the target of the vulnerability but may be as high as USD 250,000, for example, for a recent Apple iOS vulnerability. There is also a 'white market' for the exploits, which may be offered by the original software developer, but typically the price is USD 10,000 or lower.[15]

Finally, some zero-day exploits are used by those developing them. The Hacking Team, a company selling commercial surveillance software to governments and other buyers, develops such exploits to use in their software. However, many of their zero-day exploits were released in a breach of the Hacking Team and were quickly included in exploit kits such as Angler, for broader usage.[16]

Insider actions

In addition to outside attacks, which according to most studies represent the largest group of attacks, employees also play a role in data breaches. Sometimes this is with malicious intent, in other cases it results from accidental disclosures or loss of devices with valuable data. Symantec provides a breakdown for 2015 in the following graph.

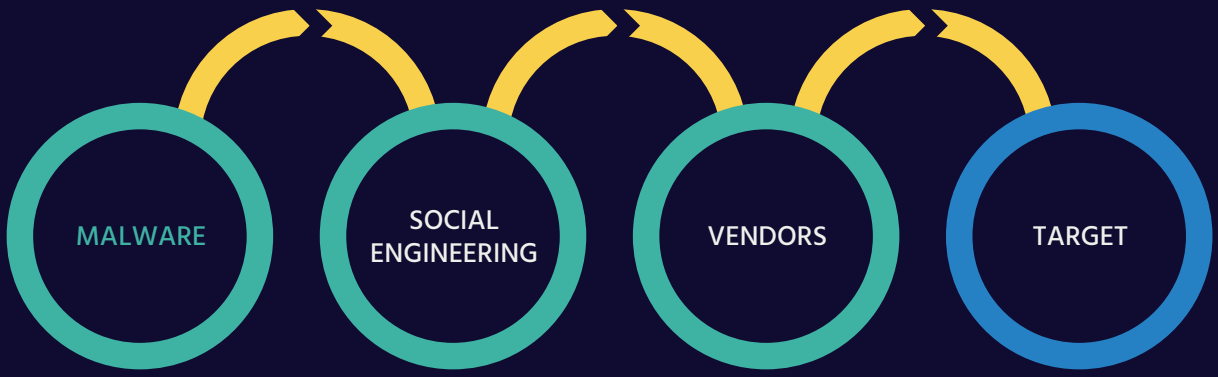
Everyone makes mistakes, and that can include coding a new website with bugs, losing a USB key, or hiring the wrong person, and some of these mistakes lead to data breaches. As discussed in the recommendations section, it seems safer to design technology around humans than to expect humans to design their actions around technology.

In some cases, even trying to do the right thing may not be enough. In one study, a security firm bought 200 second-hand hard drives off eBay and Craigslist and found in spite of attempts to delete data, 67% contained personal information that could be recovered, including social security numbers, and 11% had sensitive corporate data, including emails and sales projection data.[17]

In most cases, the data had been deleted, but in ways that could be recovered, such as putting it in the trash or recycle bin. In only 10% of the cases was the data permanently erased. While part of the issue is understanding the difference between 'delete' and 'erase', the tools need to make this simple for all users.

Asymmetric warfare

Organisations are engaged in a form of asymmetric warfare, in which they have to defend against a mind-boggling number and forms of attack, whereas an attacker only has to get lucky once to get into the system. And, as in any arms race, any advantage the defence gets is quickly matched by new offensive weapons.

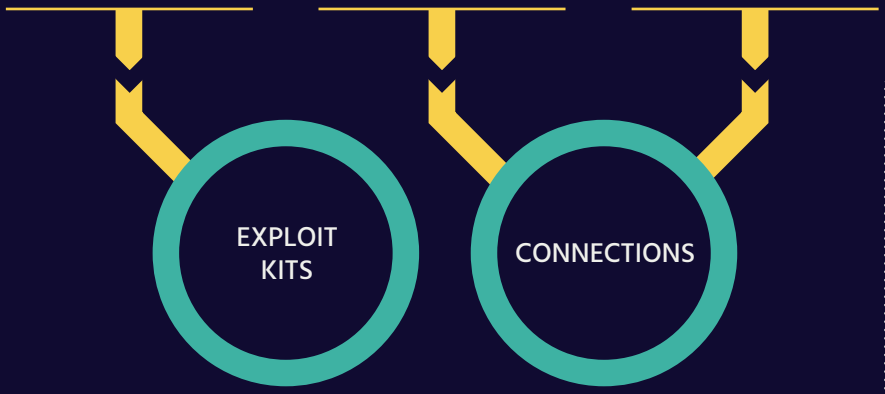


According to Symantec, 430 million unique forms of malware were discovered in 2015, more than 1 million per day.[18]

Large organisations may have hundreds of thousands of employees susceptible to phishing attacks.

Organisations are also vulnerable to large and small vendors whose systems are connected for business purposes.

A target, such as Target, may have thousands of computers, running new and old systems, whose interdependencies make it difficult to defend.

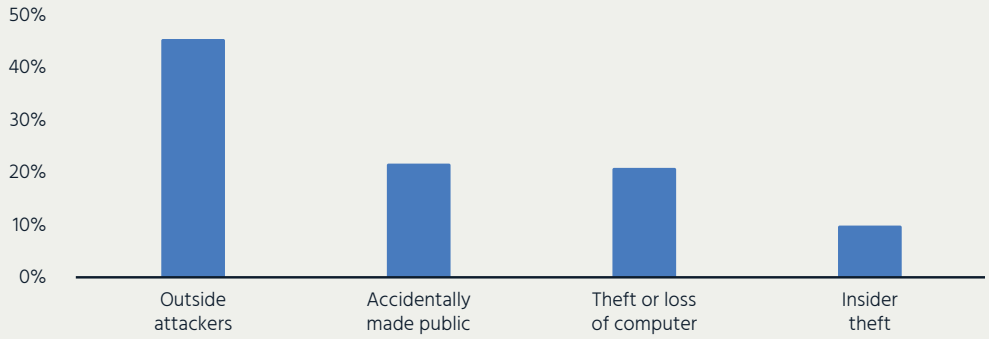


To make it easier for attackers, malware is incorporated into exploit kits such as **Angler**, which effectively make hacking more accessible to those without skills.

According to Verizon, 70% of attacks where the motive is known involve a secondary target; 70% of attacks spread from one victim to the next within 24 hours.[19]

A popular exploit kit in 2015 is called **Angler**. According to one source, it might cost up to USD 30,000 to buy, but could return millions in revenues just from imposing ransoms on users to get their data back. Other uses include accessing login details for a further attack. The kit is 'user-friendly' from the attacker perspective, and continuously updated to evade attacks and find new vulnerabilities.[20]

Individuals using the Internet



Source: Symantec Internet Security Threats Report, 2016

It happens to the best of them.

Further proving that breaches will happen even when security is a core business, a number of recent targets have been in the cyber security business themselves, but they still could not avoid a targeted attack.

RSA Security: In 2011, An employee of RSA's parent company EMC clicked on a file entitled '2011 Recruitment plan.xls' attached to a spear-phishing email, which used a zero-day exploit to install an infection through Adobe Flash. This enabled the hackers to gather information about the SecurID two-factor authentication product of RSA, presumably to be used on other targets.[21]

Hacking Team: Hacking Team is an Italian IT company that develops commercial surveillance – e.g. hacking – tools for governments, law enforcement, and commercial companies. It was the subject of a data breach in 2015 using a zero-day exploit, which leaked 400 gigabytes of data, including emails, a few zero-day exploits which Hacking Team had found for its own uses, and a list of clients. The clients included some repressive governments, leading the Italian government to revoke its license to sell outside of Europe without permission.[22]

Kaspersky Lab: The Russian Internet security company was hacked in 2015, using what the company called a sophisticated attack involving three zero-day exploits. The company claims that some data was taken, but nothing critical to its operations.[23]

The list goes on. Security and surveillance companies appear to present an attractive target for attackers. Some, seemingly for bragging rights, to prove they can break the most secure of systems, and others, to use the security information gathered to attack their true target.

For our purposes, this reinforces the idea that full prevention is not possible, and there is no such thing as absolute security – a determined and skilled attacker, focused on a particular company, seems to be unstoppable. However, there are steps that can be taken to increase the cost and difficulty of successfully executing an attack, to increase the possibility of detecting an intrusion, to mitigate data breaches, and to recover faster.

Organisations can mitigate the impact of an attack

Prevention is important, to protect against opportunistic attacks like phishing exercises, and even against more targeted attacks, like spear-phishing. However, prevention cannot be the only plan, because it seems a determined attacker will likely succeed.

Accepting a breach is possible under the best of circumstances, and probable under the worst, steps can be taken to minimise the damage. The full playbook is lengthy and requires a broad and deep strategy including various technical tools, such as early detection tools, training, and a legal and communications plan.[24]

Here are two straightforward ways to mitigate the impact of a breach.

- First, attackers cannot take data that does not exist.
- Second, any data that is taken has no value if it cannot be read.

More detail on these principles can be found in the recommendations section.

The increasing number of devices and sensors gathering data, online activity generating input, and venture capital seeking the next big thing, are all matched in pace by the falling cost of data storage, creating a perfect storm of big data.

However, as cybersecurity expert Bruce Schneier has pointed out, such data can be a 'toxic asset'.[25] The cost of the data, in a breach, can far outweigh any benefits it may have reaped otherwise.

Of course, data gathering for use can be minimised, but may nonetheless still be essential. Companies should reduce the impact of any data that is lost, through appropriate encryption – if it cannot be read, it cannot be used.

Many organisations are not routinely minimising the data they collect and encrypting what they have. These are such obvious protective measures that, without looking at the economic factors, it is hard to understand why they are not used more extensively. More detail on these principles can be found in the recommendation section.

Economics of data breaches

Why are organisations not taking more steps to prevent breaches and mitigate costs?

The economics of data breaches and their impact on trust is at the heart of this report. This report highlights some of the costs of breach, which can be quite high, and some of the causes. While not all breaches are preventable, many of them are, as discussed in the case studies section.

For instance, Target was hacked through a connection to a refrigeration contractor. One of the contractor's employees fell prey to a phishing attack, which succeeded due to inappropriate anti-virus software. The malware was used to access Target's point of sale terminals to gather data, likely because of the use of weak or default passwords in one or more systems. Was the employee trained in the risk and dangers of phishing attacks? Why was a home version of an anti-virus program considered sufficient? Did Target have any way to vet the security of the refrigeration contractor's system before connecting? Why were default passwords still in use?

Likewise, after a breach, could the impact be lowered? In the case of TalkTalk, at first, the CEO said she did not know if the customer data stolen had been encrypted. Then, admitting it was not encrypted, she argued TalkTalk had met all of their regulatory requirements. Why would the CEO of a major broadband provider, experiencing its third security event in succession, not know if its customer data was encrypted?

In the case of Ashley Madison, some members whose personal information was exposed had paid the company USD 19 to delete their records, which was either not done, or not done correctly. Charging to delete customer records is not a common practice, but perhaps understandable given the nature of Ashley Madison's core service. But having offered the paid service of deleting records, why take the risk of not fully deleting them?

In the Target case, did the refrigeration contractor, having provided the initial breach point, bear any of the cost of the breach? Target itself did not bear all the costs. The banks spent at least USD 240 million replacing compromised credit cards, although they were able to recover some through lawsuits.[26] The aftermath of data breaches also reveals some clues. Ashley Madison customers had no way to know that their records were not safe – could another service have competed by claiming they could have offered better data security?

Why, given the potential costs, were more efforts not taken to prevent or mitigate the risks of a data breach? In economic terms, we can

explain this with two concepts that can be boiled down simply to costs and benefits. The cost of a breach is not entirely borne by the organisation breached, and the benefit of offering better data security is not high enough.

Externalities

In all likelihood, the data collector who is breached does not bear all of the costs of the breach – the cost borne by others is an externality.

- While the CEO of Ashley Madison had his own alleged extramarital affairs exposed from the breach, he might not account for the full impact of potential disclosure on others when he decides how much to spend on security.

- While Target bore a significant cost after their breach, they did not bear the cost of replacing all of their customer's credit cards, an externality borne by the banks.

- An employee provided the information used to hack the AOL account of the CIA Director, whose emails were exposed and had to take the time to deal with the breach.

In countries where disclosure is not even required, the externalities are yet greater, as the companies may not even bear any reputational cost from the breach, further lowering the incentive to invest in cybersecurity.

Further, the weight of data breaches impacts future trust, both for those who were directly affected, but also among those who learn about them indirectly. This can lead to a reluctance to go online, and once online, a reluctance to use services requiring personal information, which in turn can limit the growth of the Internet economy. This impact on trust is an externality, and from an economic perspective, there is no reason for organisations to account for their impact on trust in the entire Internet when they take their decisions on data breach prevention and mitigation. However, this is an impact which society cannot neglect.

Asymmetric information

Stakeholders have asymmetric information about the risks they may face, making it difficult to take rational decisions. In particular, it makes it difficult for organisations to benefit from taking the right steps to avoid data breaches. Target cannot check the anti-malware software of every one of its contractors; the CIA Director cannot know how well Verizon employees are trained to resist social engineering attacks. The issue is deeper than this. Ashley Madison cannot credibly signal they have done the utmost to protect the data of their current customers, and that they have truly deleted the data of the former users who paid to have it deleted.

Issues of adverse selection and moral hazard arise from the asymmetric information. Consider the example of an online retailer, who is worried about being hacked, and wants to take actions to protect the company from a data breach.

Assume the retailer decided to invest a significant amount to protect their users' information from hackers, as a means to compete with other online retailers who might be more vulnerable. How would they signal this credibly to users? They could point out they have not been hacked, but that does not mean they could not be hacked. If there is no way to signal it, there is no way to win more customers, and thus by adverse selection, the market would consist of retailers who have underinvested in security.

If the retailer is still worried about the risks of a data breach – not having invested in the optimal amount of cybersecurity, the company might instead choose protection through cybersecurity insurance (this would be an example of adverse selection – those most at risk are most likely to take insurance). Now moral hazard can kick in – having the insurance means potentially investing even less in cybersecurity, because there is even lower cost from a breach, which of course becomes more likely.

Of course, this is a stylized example, and there are no doubt many companies that recognize the full costs of a data breach, and invest wisely to prevent them. Regardless, this example raises some significant issues that must be addressed to increase security. In particular, the ways to credibly signal different attributes of security.

Economics 101

Externalities and asymmetric information are examples of market failure

Positive or negative externalities arise when a decision taken by one party provides a benefit or harm, to other parties, who have no voice in the decision. For instance, when a homeowner paints their house, they do it because it pleases them, even though it may make the neighbourhood more pleasant for other neighbours, and possibly even raise the value of their houses. On the other hand, if they paint their house in garish colours, it may have the opposite effect. Either way, the homeowner has no reason to take those effects into account – unless, of course, there are historical regulations or homeowner agreements governing the upkeep and colour of houses in the neighbourhood, to promote positive externalities and avoid negative ones.

Asymmetric information arises when one party to an agreement or exchange has more information than the other about the object of the exchange. The classic example is the used car market. The seller of the car knows more about its quality, and how it has been treated, than the buyer. It is difficult, however, for the owners of high-quality cars to convince buyers that they are high quality, so cars that are the same on paper (model, year, mileage driven), will sell for the same average price. As a result, high-quality cars are less likely to be sold, and the market is full of low quality 'lemons'.[27] While a used car dealer may be able to create a reputation for selling high-quality cars or provide a warranty to protect buyers, the individual seller of the used car may not have any reputation to uphold, and cannot credibly offer a personal warranty.

There are two particular outcomes of asymmetric information of interest here.

- **Adverse selection.** Those with better information will be selective in how they participate in a market. In the used car market, without a means to signal if a used car is high-quality, only those with lower quality cars will sell, resulting in a market of lemons. In insurance markets, people understand their own risk better than the insurance company, which can also result in adverse selection, as those with higher risk may be more likely to take out insurance (and then, with a riskier pool of insured, premiums will rise accordingly).[28]

- **Moral hazard.** Insurance may lead those with coverage to take less care because they do not bear the full cost of their actions. For instance, if one had a car insurance with no deductible, and no increase in premiums, then people would have less incentive to park their cars securely, or may even take more risk driving. This is known as moral hazard.

Car insurance has deductibles to address asymmetric information. First, with a deductible, owners bear some of the cost of their actions so there is less moral hazard. Second, some insurance companies offer different levels of premium and deductible to address adverse selection. Owners who know they have low risk will choose a low premium and a high deductible that they expect not to have to pay. Those with high risk will choose a higher premium and a lower deductible, that they know they may be likely to pay.

While adverse selection can be addressed privately, such as offering deductibles, in other cases the government may need to intervene. For instance, in healthcare, individuals know more about their own health history, genetic makeup, and daily activities, than any insurance company could hope to find out (although, with cheap DNA tests, online histories, and fitness trackers, that could change). As a result of adverse selection, those of us with more risks would be more likely to take health insurance, raising the premiums. One of the many reasons for governments to provide healthcare (as in the United Kingdom) or to require everyone to have private insurance (as in Switzerland) is to make a broader and healthier pool to spread the risks and lower the premiums.

Similar issues arise with cybersecurity – the private market can help to find solutions to address asymmetric information, but governments may need to intervene in certain cases to help convey certain attributes of security.

The Attributes of asymmetric information

While we have already seen the challenges on assessing the quality of a used car, even for a new car there is a lot of asymmetric information involved in the purchase decision. While the challenges in assessing the quality of a used car are easy to understand, even for a new car there is a lot of uncertainty. There are many attributes involving different degrees of asymmetric information, and several ways to make sure the car meets those attributes. Buyers first need to decide the type of car to purchase. Even for a new car there are concerns about the quality; its fuel efficiency; and then what safety features it has. While some of these attributes are clear, others may never be.

So how do we decide?

The first thing many people choose is the type of car; some want a two-seat sports car, others a seven seat sport utility vehicle, and it is easy to identify which cars to consider based on those attributes. Other details are harder to find out – how the car drives, and how well it holds up over time. People can test drive the car to see how it handles, and the reputation of the car manufacturer may signal the quality. Finally, however, people cannot test the airbags, fuel efficiency, pollution levels, or the resistance of the car body in an accident. Here, people may need to rely on a third party, such as the government, to test and certify the car meets minimum standards.

In economic terms, there are three specific attributes of products or services, with respect to asymmetric information:

Attributes one can identify in advance, such as the type of car.

Attributes that only become apparent over time, such as the quality of the car.

Attributes one may never learn about, such as the quality of the airbag.

A number of models have emerged to assist us in assessing these attributes, which typically involve a third-party to help test, certify, or mandate one or more attributes.

Ratings

Trusted third-party agents can test products and services against a number of attributes, and provide ratings for consumers before they purchase. For instance, Consumer Reports is a publication that rates a wide variety of products on a wide variety of attributes. For cars, it rates safety, reliability, and general consumer satisfaction with each model rated.[29]

Certification

For some attributes, it may not be necessary to provide a rating, but simply determine the product meets a certain baseline standard. For instance, UL (formerly Underwriters Laboratories) is a private company that can certify safety standards of products such as electrical products, often against their own benchmark.[30] In automobiles, car manufacturers are allowed to self-certify certain attributes such as fuel economy and emissions in some countries, which has recently highlighted the need for third parties.[31]

Mandates

For credence attributes, such as safety, a consumer or private third party agent may never be able to assess them. Governments may need to mandate safety standards. For instance, governments may be best placed to test-crash automobiles and ensure that they meet safety standards.

Because of asymmetric information, it is difficult for customers to assess the data security of organisations along various attributes. Ways for organisations to send credible signals of their security levels involving third-parties are discussed in the recommendations section.

In economics, we say there is a market failure when a market outcome is not efficient. A market outcome is efficient when no one could be made better off without harming someone else. One example of a market failure is monopoly power – when one company controls the market and can set prices higher than in competitive markets, then there will be potential customers who are willing to pay the cost, but not the inflated monopoly price. This excess demand is inefficient. In the case of a market failure, there is an argument that a third party could intervene. This is the role, for instance, of competition or antitrust authorities in governing market power.

When it is difficult for customers to distinguish the quality level between goods or services, asymmetric information poses a problem. In particular, the seller with high-quality items wants to distinguish themselves from the lower-quality sellers. One solution is to send a desirable signal to potential customers – to be credible, the signal must be one that only high quality sellers can make. Branding is one type of signal – a company that invests in advertising its brand sends a signal it knows it is high quality and will be able to recoup its investment. Banks attempt to send a similar signal by investing in expensive buildings. However, given the importance of banks in the economy, governments may support deposit insurance as the ultimate credible signal to customers that their deposits are secure.

Conclusion

The economics of data breaches highlights some key solutions.

First, organisations must be induced to internalise the negative externalities they cause other organisations and users, and society at large, to reduce the incentive to create them. In many cases, this can be monetary – just as taxes can reduce certain types of pollution, increasing the liability or penalty faced by the organisation responsible for allowing a breach to occur will no doubt lower the probability of one occurring. Just as some types of pollution are too toxic and must be outlawed, such as lead in paint or gasoline, there may be a need to impose certain data security practices outright.

Second, the way to address the problems of asymmetric information is to make information more symmetric. If organisations can credibly signal their cybersecurity levels to customers, then they will be more likely to invest in it as their investment will be rewarded. This will also lead to a more vibrant cybersecurity insurance market, and reduce the extent of moral hazard as companies with better practices will be rewarded with more favourable policies. In the end, customers will benefit because the organisations they interact with online will have the right incentives to increase data security.

These recommendations are addressed more fully in the next section.

Internet of Things

Looking forward, we can see similar economics issues playing out in the emerging Internet of Things devices.

For instance, software companies typically avoid liability through their license conditions.[32] As devices become more connected, they contain more software, and could seek similar licenses. In the case of the connected Jeep hack, the company was arguing for the minimum level of liability, stating the hack was the cause of a vandal, rather than a product defect that would raise its liability levels. This lack of liability could lead to significant externalities imposed by a broader range of devices including health devices, baby monitors, and a wide variety of sensors.

Likewise, someone shopping for a baby monitor, WiFi router, or connected car, has no way to learn how well it has been protected from attackers. There is less incentive to invest in safety, and instead, rush the device out to compete with others. Addressing any security issues through patches is problematic when the patches themselves may be difficult to apply, as in the case of the Jeep, leading again to suboptimal security levels.

The potential issues go beyond data breaches. While a connected car may be hacked to give its location, the hack can also extend to personal safety, potentially at the cost of life and limb. We note the lessons of this report may extend forward to the Internet of Things, as well as more broadly to general security breaches.

Footnotes

[1] See the Online Trust Alliance 2016 Data Protection and Breach Readiness Guide, Updated May 16, 2016 (OTA 2016 report) at https://otalliance.org/resources/data-breach-protection.

[2] Verizon publishes a yearly Data Breach Investigations Report. The 2015 edition contains a section on the use of Known Vulnerabilities, which we cite here. See http://www.verizonenterprise.com/verizon-insights-lab/dbir/ at pages 15-17. For its analysis of known vulnerabilities, Verizon used a database of "Common Vulnerabilities and Exposures (CVE)" which is defined as "a list of information security vulnerabilities and exposures that aims to provide common names for publicly known cyber security issues. The goal of the CVE is to make it easier to share data across separate vulnerability capabilities (tools, repositories, and services) with this 'common enumeration.'" The CVE is sponsored by US-CERT at the US Department of Homeland Security, and managed by MITRE. See cve.mitre.org for more details.

[3] See http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/. We note that there was some controversy about the top ten list, with another put together here http://www.theregister.co.uk/2016/05/12/verizon_dbir_criticised/. In response, the author of the section in the Verizon report, Michael Roytman, wrote a blog responding to the points. http://blog.kennasecurity.com/2016/05/collaborative-data-science-inside-the-2016-verizon-dbir-vulnerability-section/. While questioning the methodology for putting together the top ten list, no one questioned the basic underlying premise that known vulnerabilities are a significant target for attacks.

[4] Symantec 2016 Internet Security Threat Report, at https://www.symantec.com/security-center/threat-report, Web Threats section.

[5] According to Symantec, Adobe Flash constituted 10 zero-day vulnerabilities in 2015, which was 17% of the total that year; 12 in 2014 (50%), and 5 in 2013 (22%). Id.

[6] Browsers and websites are beginning to stop to support Adobe Flash, at least in part because of security vulnerabilities, in favor of HTML5 support, which does not require plugins and is more secure. See http://www.dailymail.co.uk/sciencetech/article-3160644/Google-Mozilla-pull-plug-Adobe-Flash-Tech-giants-disable-program-browsers-following-critical-security-flaw.html.

[7] Verizon DBIR 2015, page 13.

[8] See https://next.ft.com/content/19ade924-d0a5-11e5-831d-09f7778e7377.

[9] See https://nakedsecurity.sophos.com/2016/04/08/almost-half-of-dropped-usb-sticks-will-get-plugged-in/.

[10] See http://uk.businessinsider.com/mark-zuckerberg-twitter-pinterest-accounts-hacked-linkedin-hack-facebook-passwords-2016-6

[11] See http://uk.businessinsider.com/linkedin-hack-data-shows-people-pick-awful-common-passwords-2016-5

[12] As noted in the OTA 2016 Report, "…we have learned that no organisation is immune. As larger quantities of diversified data are amassed and the reliance on third party service providers increases, every business must be prepared for an inevitable loss of data. The facts highlight the need for startup and global enterprises to shift attitudes and make data security and privacy part of every employee's responsibility." https://otalliance.org/resources/data-breach-protection at p. 8

[13] As noted in the Recommendations section, even known vulnerabilities may not be easy for some organisations to patch, and the patching process itself may introduce further vulnerabilities.

[14] https://en.wikipedia.org/wiki/Market_for_zero-day_exploits

[15] http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/#7d4865bf6033. Apple recently joined the group of companies paying a so-called 'bug bounty' for new vulnerabilities, with payments up to USD 200,000, which it notes will still not top those paid on the black market. See https://techcrunch.com/2016/08/04/apple-announces-long-awaited-bug-bounty-program/.

[16] http://krebsonsecurity.com/tag/angler-exploit-kit/

[17] See http://www.infosecurity-magazine.com/news/data-left-behind-two-thirds-drives/ and http://www2.blancco. com/en-rs-leftovers-a-data-recovery-study for the original study.

[18] Symantec 2016 Internet Security Threat Report.

[19] Verizon Data Breach Investigations Report 2015.

[20] See https://heimdalsecurity.com/blog/exploit-kits-service-automation-changing-face-cyber-crime/.

[21] See https://www.wired.com/2015/04/hacker-lexicon-spear-phishing/.

[22] See https://en.wikipedia.org/wiki/Hacking_Team

[23] See http://www.bbc.com/news/technology-33083050.

[24] For one view of the range of issues involved, see the OTA Report 2016 at https://otalliance.org/resources/data-breach-protection.

[25] See https://www.schneier.com/blog/archives/2016/03/data_is_a_toxic.html. As discussed in the introduction, the analogy of data with oil as the fuel for digital and industrial revolution, respectively, is also apt for the downsides of each as a fuel, as noted by the Internet Society's Robin Wilton at https://www.internetsociety.org/blog/tech-matters/2014/10/they-say-"personal-data-new-oil"-thats-good-thing. One downside of both is the risk of data breach or oil spill.

[26] See http://www.reuters.com/article/us-target-breach-settlement-idUSKBN0TL20Y20151203.

[27] This example is commonly referred to as the lemons problem (in English, a lemon is the popular term for a low-quality car). The theory was described by George Akerlof, in a 1970 paper titled "The Market for Lemons: Quality Uncertainty and the Market Mechanism." Professor Akerlof shared the 2001 Nobel Memorial Prize in Economic Sciences with Michael Spence and Joseph Stiglitz, for their work in asymmetric information.

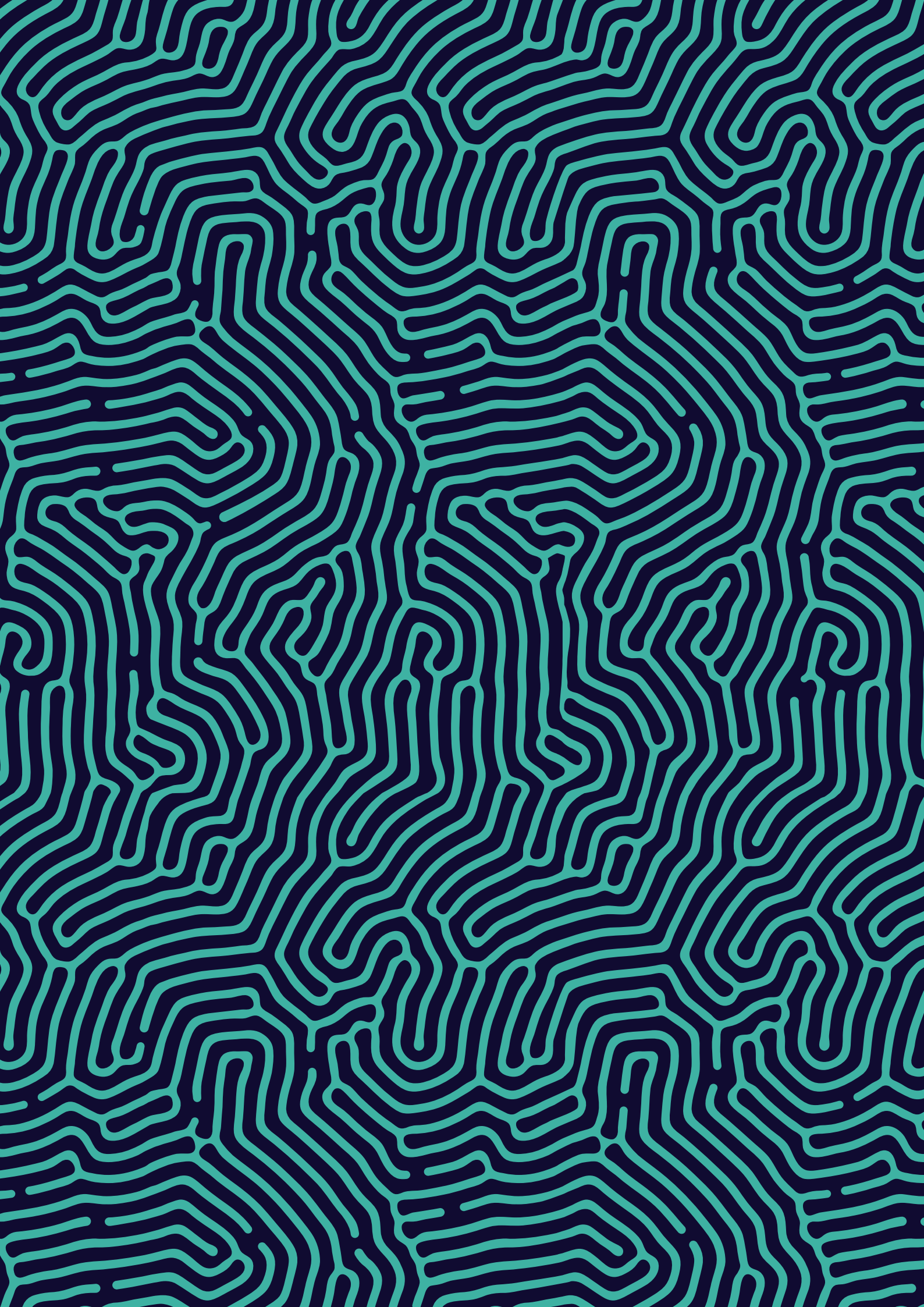
[28] Of course, typically insurance is mandatory, in part at least because of externalities – to ensure that there is adequate coverage for those not responsible for an accident.

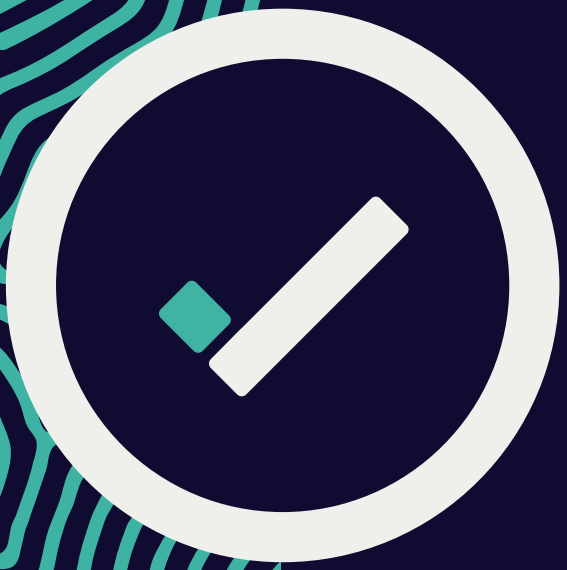
[29] See www.consumerreports.org for more details and examples. On their website, they note that "Formed as an independent, nonprofit organisation in 1936, Consumer Reports serves consumers through unbiased product testing and ratings, research, journalism, public education, and advocacy. We stand firmly behind the principle that consumer products and services must be safe, effective, reliable, and fairly priced. We insist that manufacturers, retailers, government agencies, and others be clear and honest. We advocate for truth and transparency wherever information is hidden or unclear. We push companies to quickly address and remedy issues with their products and services."

[30] See www.ul.com for more details and examples. For instance, in relation to small home appliances, UL states the following " UL has been working with small appliance manufacturers, retailers and related parties for over 100 years. We fully understand the market drivers, pain points and business necessities of small appliance manufacturers, and we offer a comprehensive portfolio of services and certifications to meet all of the industry's needs, including safety certifications, energy efficiency testing, performance testing, reliability testing, EMC testing, claims validation, environmental sustainability validation and product benchmarking. The UL Mark is one of the most widely recognized and trusted symbols of safety among consumers globally, giving UL certified products the surest path to market acceptance. Consumer research shows the UL Mark is valued by consumers and is looked for on the products they buy."

[31] See http://www.autonews.com/article/20150922/BLOG06/150929959/in-wake-of-vw-scandal-its-time-to-scrap-self-certify-era.

[32] https://techcrunch.com/2015/08/06/should-software-companies-be-legally-liable-for-security-breaches/





CHAPTER 5

Recommendations

Introduction

Principles

Recommendations

Summary

Introduction

The Data and Case Studies sections show that data breaches are a significant issue worldwide. Yet, despite growing awareness of the risk, they still happen, with a negative impact on user trust in the Internet. In seeking to understand the problem, the report highlights the underlying economic issues that may be hindering proper investment in, and adoption of, adequate data security measures.

This report highlights five recommendations for addressing the issues we have raised regarding the economics of data breaches. Each one helps to reinforce the others as part of a virtuous data security circle, as shown below.

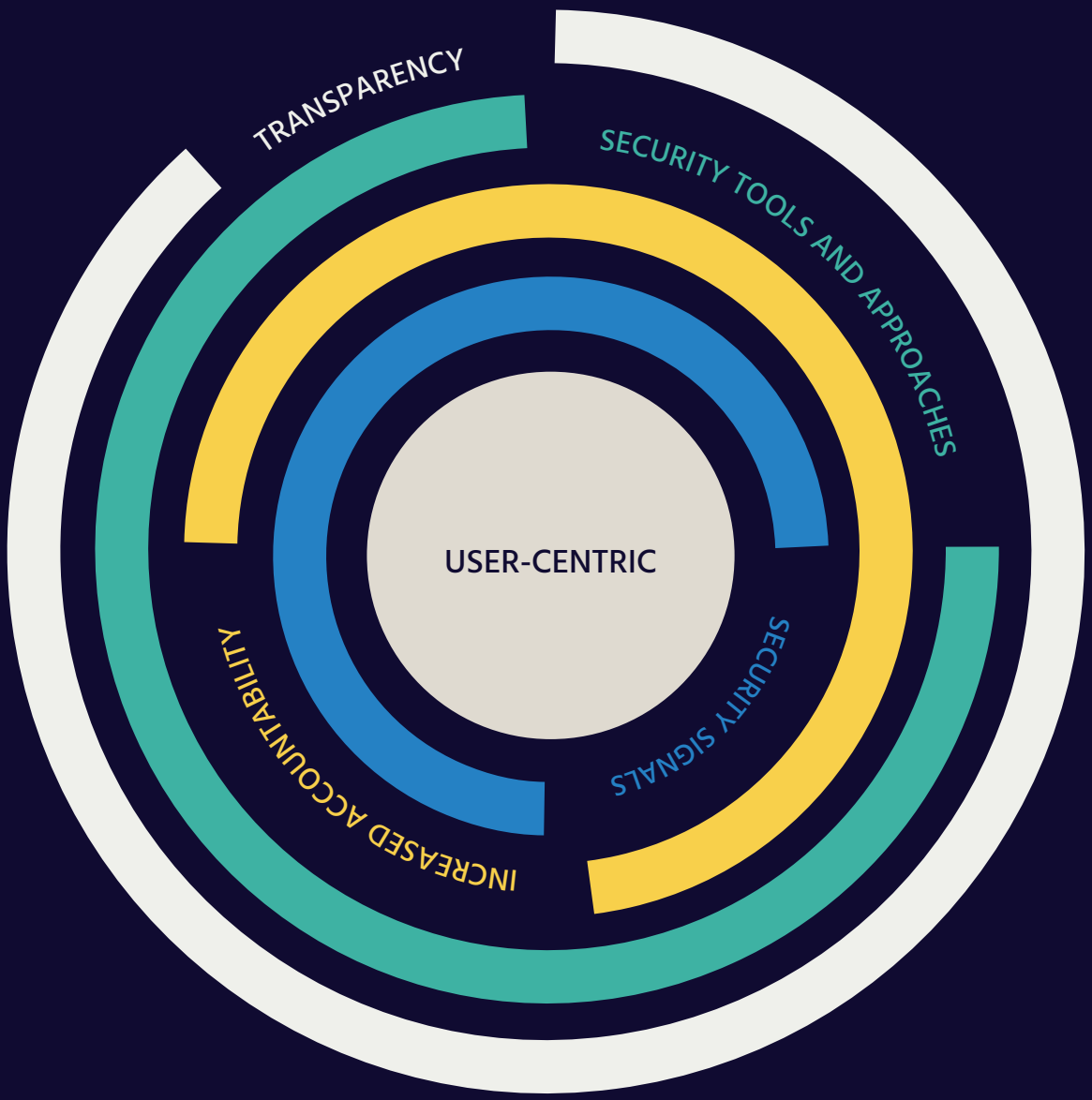
The first recommendation is to put users, who are the ultimate victims of data breaches, at the centre of the solutions. As a way to kick-start this approach, our second recommendation is to increase transparency about the risk, incidence and impact of data breaches globally. This will help make data security a priority and create demand for better security tools and approaches to prevent and mitigate the problem.

To help increase the economic incentives for organisations to implement these tools, they should have increased accountability and bear more of the cost when a data breach occurs. At the same time, those organisations that have invested in better protection against data breaches should be able to provide credible security signals to the market, so that they can benefit from their increased security investments.

Underpinning these five recommendations are two important principles: data stewardship and collective responsibility.

We recognise these are medium and long term recommendations and that input from all relevant stakeholders is needed. As a starting point, we provide some suggestions on key points to begin the process of implementing them. We wish to start the dialogue and point the way, and not attempt to impose our own solutions.

The five core recommendations



Principles

The high-level principles underpinning the five recommendations are:

Data stewardship

Organisations should regard themselves as custodians of their users' data, protecting their data not only as a business necessity but also on behalf of the individuals themselves. This is consistent with the user-centric recommendation discussed below. Users would like organisations to view their personal information as more than a revenue source. Organisations should apply an ethical approach to data handling, and understand that they can do well by doing good – protecting users' data should be a goal in its own right, which also protects the organisation.

Collective responsibility

On the Internet, everyone is connected. One breach could lead to another – "your breach could be my breach". Organisations share a collective responsibility with other stakeholders to secure the data ecosystem as a whole.[1] For example: Vendors can help provide security solutions that make it easier to prevent breaches; Employees should generally protect their activities against hackers and accidental disclosure; Governments can help by creating an enabling environment for better security solutions; and other parties can play a critical role in providing independent standards and reviews at every stage of data security. Should one of these links not function, it could break the entire trust chain.

Recommendations

R1

USER-CENTRIC

Put users at the centre of solutions; and include the costs to both users and organisations when assessing the costs of data breaches.

The Internet Society has long advocated for a user-centric approach to Internet issues.[2] A user-centric approach focuses on users and their needs.

In our work on this topic, we view users as the often overlooked subject of data breaches, even though they are ultimately the biggest victims.

Specifically, when there is a breach:

- Users may not even be aware of a data breach, as many organisations do not notify them, in part because there are no disclosure requirements in many countries;

- Even if they are aware, their options may be limited – Once disclosed, the data cannot be recovered. Users may have trouble obtaining financial compensation or damages, especially if they cannot show direct harm. They may also be exposed to an extended risk of identity theft and other harm. And, non-financial issues are difficult to remedy;

- The impact of a breach on users is typically only studied as one of the costs to the organisation, in terms of compensating direct harms, credit protection, and impact on consumer loyalty, rather than in terms of the cost to users, and in turn to society.

This must change. The consideration of user impact should also extend to: time and costs spent on addressing fraud enabled by the data breach; non-financial harms; and future damage. Greater awareness of the full impact on users will help generate more user-focused approaches to data breaches.

More broadly, every breach has a ripple effect that spreads distrust from impacted users to all users. Less trust in the Internet results in less benefits for all of us.

The primary goal of data breach solutions should be to protect users and their data. Data breach risk assessments must include risks to the users whose personal data is at stake. Economic incentives should enable users to choose services that have better data security.

R2 TRANSPARENCY

Increase transparency through data breach notifications and disclosure.

We advocate for increased study of the evolving risk of data breaches, starting with more transparency about the incidence, causes and impact of data breaches worldwide. Our goal is for this increased awareness to create demand for the kind of solutions we highlight in the subsequent recommendations.

Data breach notification requirements increase transparency about data breaches – what are likely targets, what security works and what does not, what data is taken, how the breaches are carried out. Indeed, much of this report itself is based on existing data breach disclosures.

Sharing information responsibly has a number of benefits – it could help organisations globally improve their data security, help policymakers improve policies and regulators pursue attackers, and help the data security industry produce better solutions. All this can help protect the data ecosystem as a whole.

Transforming transparency to the level of action is part of the responsibility we must collectively take on, so that everyone can make informed choices, help prevent data breaches, and mitigate the impact when they do occur.

If the market does not provide organisations with incentives to take action to voluntarily disclose data breaches, leading to a situation of information asymmetry, government intervention may be needed.

Organisations should warn users when a breach has occurred so that they can also take action to protect themselves. Data breach notification requirements help increase awareness and should be the norm, and are consistent with the user-centric approach this report advocates.

R3 PRIORITISE SECURITY

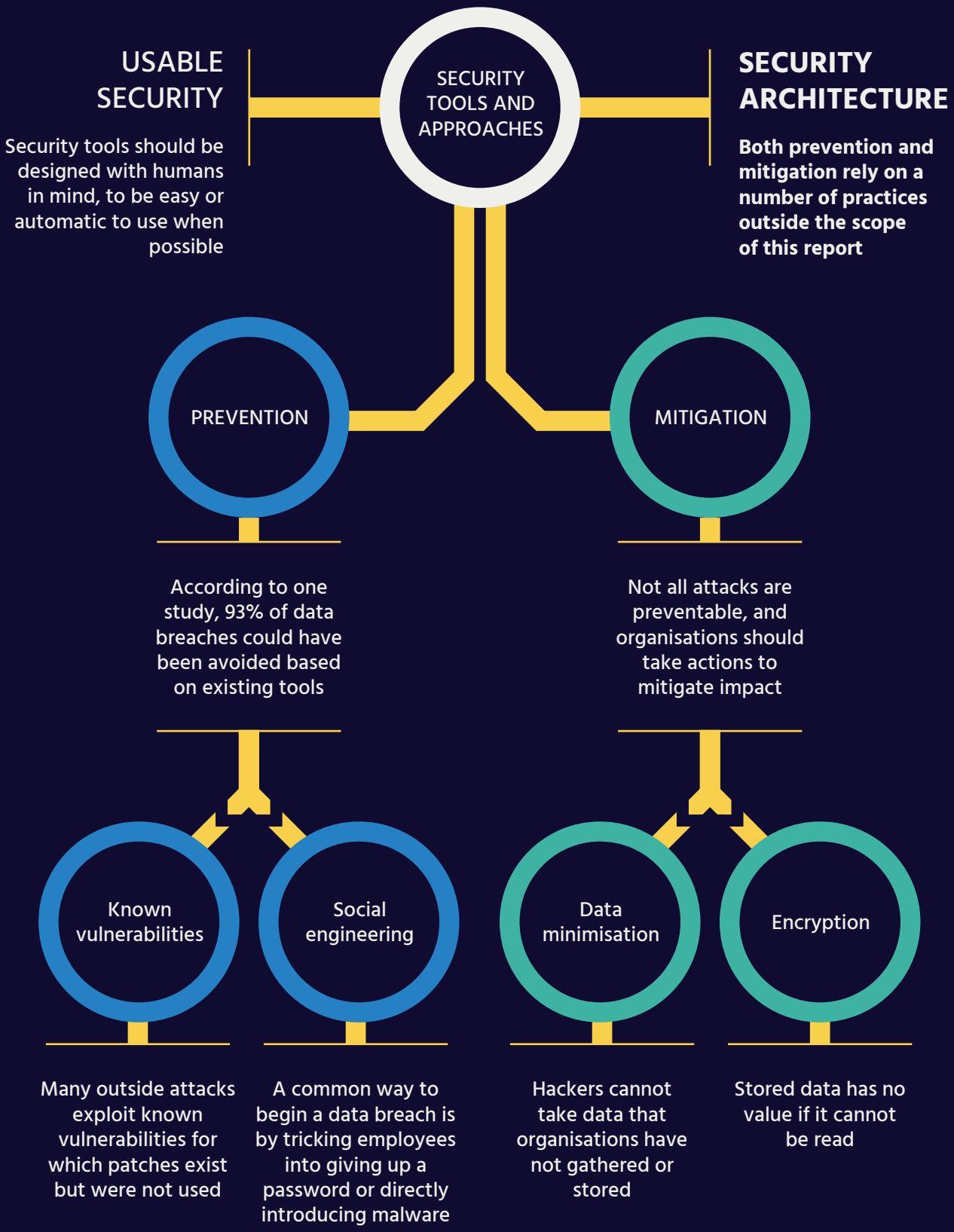
Data security must be a priority. Better tools and approaches should be made available. Organisations should be held to best practice standards when it comes to data security.

As seen in the Issues section, many of the tools to prevent data breaches and to mitigate their impact already exist. However, these tools are not always used by organisations responsible for handling user data. Given the cost of data breaches, why are some organisations not using the tools? In part it may be a lack of awareness, or in part a lack of economic incentives. However, even with the best of intentions, these tools are not always easy to use. Progress must be made on usable security – how to make it easier, or automatic, to use the tools that can prevent or mitigate data breaches.

Here is a roadmap of the tools and approaches we advocate in this section.

A breach of just one organisation could expose users' data held by multiple organisations – "your breach could be my breach" – we must share the responsibility to secure users' data.

Roadmap of data security tools and approaches



Usable Security

Data security has a human element. For instance, employee password use is always a security issue: Is the password strong enough? Is it changed periodically? Is it unique? Is it memorised? Is the password requirement robust? Is the password safe from social engineering? Personal experience tells us the answer to at least one of these questions is often no. That may be enough to enable a breach.

This is why security practices, tools and approaches should be designed with humans in mind, resulting in usable security. Security should be built into the design of data-handling tools from the bottom-up, rather than adding it as an afterthought. This is the concept of security by design. And, to account for our human nature, we should be nudged, where possible, into implementing security tools.

It is not the goal of this report to provide a playbook for how to prevent data breaches – that requires a multi-faceted and deep approach far beyond the scope of this report. Data security is a field of its own and implementing a security architecture takes significant resources and training. Instead, this report identifies certain improvements that can prevent data breaches regardless of the overall security architecture.

Many of these concepts are easy to understand, regardless of a user's experience level – for instance upgrading our software and setting passwords. While these are practices organisations should use and support for employees, as part of our collective responsibility for security these are also practices that individuals can use on our personal devices and systems.

We will draw upon these principles throughout – to encourage organisations to take the more secure path, including providing tools for individuals – as employees, but also as users – to defend ourselves from breaches.

- Data security is a necessity, not a luxury.
- Data security should be a priority for everyone - from users to business to government.
- Data security needs to be usable if organisations are going to use it.
- Data security needs to be part of the design of systems (security-by-design) and business practices.

Security by Design

Many of the tools to help prevent and mitigate data breaches already exist and the barriers to adoption are largely economic. The reasons they are not widely used is likely because the tools are not optimal and may be hard to implement.

In particular, as users, we are all aware that human nature usually prevails– thus, it is much better to adapt technology to our needs than to expect us to adapt ourselves to technology.

Security by design generally means baking security into the technology from the beginning rather than trying to strap it on at the end after the shortcomings become clear.

We must recognise people do not always act in their own self-interest, as users or in organisations, and they may need to be 'nudged' to take a different approach.

Nudge Theory

Nudge theory draws on behavioural science and economics to influence decision-making among groups or individuals, in ways seen to be positive by the designers. The theory starts from the observation that humans do not always make rational decisions, and seeks to influence those decisions without making them obligatory.

The authors of the book that popularised the theory offered the following definition.Fn

...To count as a mere nudge, the intervention must be easy and cheap to avoid. Nudges are not mandates. Putting fruit at eye level counts as a nudge. Banning junk food does not.

In our domain, with respect to password security, for instance, nudge theory might suggest the answer is to provide users with the option to change their password periodically together with a reminder; going further would require people to change their password periodically.

Security Architecture

We recognise security-by-design should start with a tailored security architecture. Making decisions about data security requires specialist expertise that organisations (especially smaller ones or start-ups) may not have, and the tools available may not always be simple to implement. Designing and maintaining such a security architecture entails up-front costs and may potentially delay speed to market.

A tailored security architecture should include security that is usable. In any well-designed security architecture there are users (employees in this case) that have to interact with the system. This is particularly relevant in smaller organisations without in-house IT security specialists: products and services that provide data solutions will need to take into account their non-specialists users might need to be nudged or forced towards certain behaviour.

Unfortunately, economic drivers work against implementing such a security architecture. While these are similar to the economic drivers we discuss in the rest of this paper, the entire security architecture is more complex, making the analysis more complicated, and outside the scope of this report.

Prevention of data breaches

Known vulnerabilities

As noted earlier, many data breaches could have been prevented if known security vulnerabilities had been patched. It is, therefore, important to address this issue to help prevent future data breaches.

The global accessibility of the Internet makes it vulnerable to attacks, but also helps to provide access to the tools, such as software patches, to prevent breaches and other security problems.

For example, to increase software updating, particularly for critical security patches, first Microsoft and then Apple began enabling business and private consumers to choose automatic updates, or to make the updates automatic by default.[3] Many software vendors have also started to schedule their updates at specific times so organisations can prepare their own update schedules around them (such as Microsoft Patch Tuesday). Here, at least at the individual device level, the theory of nudge seems to be working well.

However, at the organisation system level, software updating is more complex – it may require pre-testing, internal scheduling, steps to address legacy hardware that may not support the updated software, as well as potentially incorporating employee-owned devices. The

software patch itself may introduce new vulnerabilities while repairing old ones, and may have unintended consequences across different hardware and software systems that need to be considered.

There is no magic bullet to address known vulnerabilities – existing IT systems cannot be replaced overnight, and introducing new systems will continue to introduce new challenges. Going forward, increased awareness of the risks of data breaches should result in the application of security by design principles from the ground up, both by vendors as well as the organisations implementing the vendors' solutions.

Organisations should secure data against known security vulnerabilities and be prepared to react against new threats. To improve data security, the marketplace needs incentives to produce usable data security tools.

Social Engineering

As seen in the Case Studies section, many successful data breaches are initiated through social engineering, such as phishing attacks. Addressing these threats requires instilling an awareness of the risks and employees' collective responsibility to help protect their organisation, while also providing them with suitable technology and training.

Employees should be taught how to avoid a phishing attack by understanding threats, including how to recognise a fraudulent email, not to click on unknown attachments, and how to report something that seems suspicious.

More deeply, employees should understand the risks of such attacks for their organisation. The case studies provided here are a good a starting place, showing how an ISP employee can accidentally compromise the CIA Director's email, and that social engineering and default passwords contributed to the Target breach.

Employees should understand the results of a data breach can be devastating, compromising users' personal affairs (Ashley Madison), employee data (Office of Personnel Management) as well as salaries and embarrassing emails (Sony).[4] Not to mention impacting the bottom line, with risks for compensation or further employment.

Technology (such as email spam filters and web filters) can help reduce the risk of social engineering attacks used to enable a data breach. Technology can also help protect systems from attacks using information obtained via a social engineering attack. For example,

more advanced forms of authentication (e.g. two-factor) instead of simple passwords may prevent unauthorised access. These measures should be extended to employees who use their own smartphones or computers, also known as "bring your own devices". Likewise, while it is important to train everyone not to plug-in unknown devices that may transfer an infection, such as USB sticks, one technical solution could be to prevent them from running automatically when they are plugged in.[5]

Our view on one important issue is that passwords (both those used by employees and those that are stored by organisations) have demonstrated security challenges. We support the principle that the tools for authentication should be improved, to address the known human and technical deficiencies that have been shown time and again. Further, any stored passwords should be encrypted securely.

For a lighthearted view of a serious topic, see this clip from a TV show asking passersby about their passwords. https://www.youtube.com/watch?v=opRMrEfAIiI

Clearly password security still has a few hurdles to clear!

One common way to strengthen authentication is using strong, unique passwords stored in a trusted password manager; another is two-factor authentication.[6] While they are common methods, as the case studies show, they are still underutilised. Neither is 100% secure, and organisations and users need to assess the pros and cons of these and other various ways to improve authentication and authorisation.

We discuss these as examples of the challenges of increasing security, not as the only, or best, solutions, for addressing social engineering attacks.

Organisations should apply trusted tools and best practices to prevent phishing and block embedded malware. They should also train employees to help avoid social engineering attacks. Vendors should develop security features that nudge people to choose the more secure option.[7]

Password Manager

Many of us have tens, if not hundreds, of online accounts including social networks, email, shopping, and work. Each account requires its own password for authentication along with a user name, and no one can remember hundreds of passwords and user names. One human response is to re-use passwords. This raises the impact of a data breach of stored passwords or a successful phishing attack leading to a data breach, because with just one password and user-id, the attackers may be able to get into many of the users' accounts, including those of their employers'.

One commonly discussed solution to this is a password manager, which creates and stores unique strong passwords, and then uses them to log into online services. However, the decision to use a password manager is not so simple.

While many experts argue in favour, others note that a single master password is still required to use the password manager, and if that is cracked then everything is exposed.[8]

Second, if one decides to use a password manager, one must decide which one to use. Some are built into web browsers, others are standalone; some use cloud storage, others local. Some may be more secure than others. The choice is not necessarily an easy one.[9]

Anyone who has read this far in the report will not be surprised to learn that password manager services are themselves a target of hackers. At least one was recently hacked - although the encryption of the passwords apparently was not violated, all users had to change their master passwords.[10]

Here, in a microcosm, we see the two main economic challenges we have been discussing.

Cracking a password manager could expose a user's entire online life – including professional, health, financial and sexual – and inflict untold damages on the user. However, the terms and conditions of one representative password manager seeks to limit the developer's liability to USD 100 per user. As a result, the significant potential costs for the users of a password manager are externalities for the developer.[11]

Further, there is asymmetric information - a user would have no way of knowing what security tools are used for the password manager, and how well they are implemented, making it difficult to choose the safest one.[12]

Mitigation in the event of a breach

Even if some data breaches can be prevented, there is no such thing as 100% security or a risk free environment. A zero-day exploit can be used to access a system, a mistake can disclose data, or a computer can be stolen or lost by an employee.

However, a breach can only take data that is stored, and if the stored data cannot be read, it cannot be used.

The approaches we discuss here to help mitigate data breaches are known as data minimisation, to not gather or keep more data than needed, and second, encryption, to make the data that are stored unreadable. These approaches should be part of broader business and technical practices respectively.[13]

The OECD Privacy Guidelines[14] state

7. There should be limits to the collection of personal data ...

8. Personal data should be relevant to the purposes for which they are to be used ...

This is a general statement of the need for data minimisation, recognising that data may need to be collected and stored, but should not be collected or stored if it is not needed.[15]

Data Minimisation

We have seen some cases where collectors kept extraneous data that significantly increased the cost of a breach. The Office of Personnel Management held data on former employees no longer working for the government, while Ashley Madison kept data users had actually paid to have deleted.

There are a number of competing forces at work.

There is the clear commercial incentive to gather data that can be monetised, now or later, and little cost for keeping the data given the falling cost of storage. In some cases, for users as well, there can be savings in time and convenience if, for instance, the collector stores credit card details to facilitate future purchases or enable long-term subscriptions.

On the other hand, there are two downsides of casting a wide net for data: the intended uses of the data, and the unintended uses of the data.

In general, even for the intended uses of personal information, there are privacy concerns, as data sets grow and are combined with other data sets in ways that users may not be able to foresee or predict.

There are also many unintended uses of our personal data, that data minimisation would help avoid or mitigate. Aside from a data breach, our data may be subject to government surveillance or be subject to data misuse.[16] As a result, there are good reasons for organisations to limit the amount of data collected even if it is never breached. At the same time, users should question when more data is requested than is needed for the specific purpose, such as a mobile flashlight app asking for permission to access location information.[17]

Organisations should take a clear and informed view of the risk of a data breach, and then consider if the value of each element of data might outweigh the additional cost if it is breached, and the corresponding impact on their users. For instance, in the US the social security number (SSN) is a key piece of information for identity fraud.[18] If an organisation needs an identifier, the questions should include:

Is it necessary to use the SSN or other government-issued id number as an identifier?

If so, once identity has been established does the government id number need to be saved or could another identifier be used or created?

If the government id number must be used as the identifier, can it be partitioned from other personal information?

Such a review would broadly consider what data are relevant to collect and keep, how long such relevant data are to be stored, and when they are to be erased. It would also recognise the value of the data not just to the organisation, but also to the customer or employee, taking into account not just what benefit such data might provide from an intended use, but also what harm may come from an unintended disclosure or unintended use. This approach is part of data stewardship.

Where market forces for increased data gathering and retention are difficult to overcome, the principle of data minimisation may need to be incorporated in national privacy laws, together with guidance as to what practices are important.

Organisations should minimise the personal data they collect and store. Governments should encourage voluntary codes of conduct and other outcomes that favour data minimisation.

Encryption

The Internet Society believes encryption should be the norm for Internet communications and data.[19] More specifically, organisations should use a level of encryption whose time and cost to crack, if at all possible, outweighs any possible benefits of an attacker potentially gaining access.

Many of the case studies highlight the cost of a lack of encryption – Target, the Office of Personnel Management, and others had no encryption, while TalkTalk, Korea Pharmaceutical Information Center, and others used insufficient encryption. Further, encryption is not a static prospect – the Ashley Madison hack highlighted that, if encryption is improved, it must be applied retroactively to existing accounts, and not just to new accounts going forward.[20]

The economic reasons for limited or no encryption are two-fold – the cost of properly implementing strong encryption is perceived to be high, while the benefits are not perceived to be high enough. However, the calculation seems to be changing in recent years.

Encryption

Encryption involves encoding data so that only the intended parties can read them. The idea of protecting information is as old as the need to keep secrets, and has always generated a race between those generating the secrets, and those trying to steal them. This has continued in the computing age, where computing power has increased the power of encryption, but also the power of those trying to break encryption.

The general challenges of encryption are: to ensure the encrypted data cannot be cracked; the keys are only accessible to the right user(s); establishing the authenticity of end-points (for encryption of network transactions); proper bug free implementation of encryption technology; and to accomplish this without adding a level of cost, difficulty (remember usable security), or computing power that renders the encryption unusable or useless.

In the past several years there has been a marked increase in the use of encryption, such as WhatsApp for messages, and Apple for data stored on devices and their cloud service.[21] Partly, this has been in response to reports of pervasive government surveillance of data, and partly in response to the risks of data and other security breaches. Regardless of the motivation for the encryption, the benefit in terms of mitigating the impact of the data breach is the same.

The particulars of encryption are of a technical nature, and certainly beyond the scope of this report. Our principles, however, are clear – implement security-by-design that nudges, or defaults, users towards

adopting sufficient encryption in the most transparent way possible. Encryption must be designed around the users rather than expecting users to work around encryption. It must be easily available, affordable and easy to apply to Internet communications as well as Web browsing, and for all devices and cloud services.

Given the increase in employees working from home and while travelling, along with using one's own devices at work, organisations have a strong interest in ensuring employees use trusted encryption technologies. Employees in turn must understand the potential risk to their employer and to their customers from a lack of use of encryption, to make sure they are not the weak link that is breached.

- Organisations should encrypt the data they hold.
- Encryption needs to be strong, easy to use and implement.

Economic Incentives

Of course, as user-friendly as tools might become, they still cost time and money to implement, which not all organisations are willing to spend.

There is a market failure that governs investment in cybersecurity. First, data breaches have externalities not accounted for by organisations, limiting the incentive to invest. Second, even where investments are made, as a result of asymmetric information, it is difficult to convey the resulting level of cybersecurity to the rest of the ecosystem.

Here we focus on how these market failures can be addressed through economic incentives, with respect to both costs and benefits.

By imposing more of the externalities of the data breach on the organisation holding the data, the costs of a data breach will go up, leading organisations to increase efforts to prevent data breaches and mitigate their impact. In economic terms, the goal is for organisations *internalise* the impact of a data breach.

By enabling organisations to signal they are less vulnerable, they will be able to better compete for business, increasing the rewards of investing in preventing a data breach. In economic terms, the goal is that organisations can credibly signal their level of cybersecurity.

Note that when a market failure exists, by definition a market solution is not available. Often government intervention is used to address the failure. However, that is not always needed as a non-government third party may also be able to help, or even self-regulation by the private players can solve some of the issues. The Internet Society supports a multi-stakeholder approach to Internet governance issues, and that holds here as well. While we will consider appropriate government interventions in our recommendations, it is neither the first place to start, nor the last resort. Rather, we will consider recommendations most likely to effectively address the issues.

Principles reinforcing economic incentives

Internalising externalities will increase the costs of a data breach to an organisation, and the corresponding incentives to avoid a breach. However, there are broader security and economic considerations that should also be considered, which we all have a collective responsibility to help to address. For instance, training employees to avoid social engineering not only helps to avoid a direct data breach, but also helps to protect against attacks on other organisations the employee may interact with, for which the employer has no direct responsibility or benefit in avoiding. This collective responsibility is a principle which is at the core of the Internet, and which should not be forgotten in the quest to prevent particular data breaches. It is the cornerstone for creating a virtuous data security circle.

While we believe diligent data stewardship is clearly in an organisation's economic self-interest, given the cost of a data breach, we also believe each organisation has a broader social responsibility to make the Internet a safer place for everyone. For a corporation, for instance, preventing a data breach should become integral to corporate governance; broader efforts to make the Internet safer against data breaches should be part of corporate social responsibility. In the end, the more trust there is in the Internet, the greater the benefits of the Internet for all.

R4

ACCOUNTABILITY

Organisations should be accountable for their breaches. General rules regarding the assignment of liability and remediation of data breaches must be established up front.

As we have seen, the cost of a data breach may be borne by a variety of stakeholders. In the Target case, the banks bore a huge cost for replacing the exposed credit cards; in the Ashley Madison case, the cost was borne by the members, as well as inevitably their families; in the Sony case, a significant cost was borne by employees and their dependents; and in the Office of Personnel Management case, not just present employees, but the data for former and prospective employees among others was also breached.

In economic terms, there is too little incentive to avoid imposing these externalities, precisely because the externalities are borne by others. Ensuring organisations account for those externalities, in turn, increases the incentive to avoid them. With increased awareness, and higher potential costs, we expect organisations will elevate data security correspondingly, to become a key element of governance.

A number of issues may arise with efforts to internalise the economic externalities surrounding data breaches.

Overall, to have the most impact on incentives, the full extent of financial and non-financial impacts of data breaches need to be better understood. General rules regarding the assignment of liability and remediation must be established up front, and understood by all stakeholders, so that they take the desired corrective action. In some cases, some minimum standards for data handling may need to be mandated if not voluntarily adopted (such as data security and data minimisation provisions in law).

There are still practical issues, as the breach may involve a third party, like the refrigeration contractor whose system was used to infect Target. Organisations may have a variety of vendors of hardware and software who could play a role in a breach. Even if blame can be determined, liability may be assessed separately, such as financial institutions bearing the cost of replacing credit cards. These rules may not always be set in stone though, as lawsuits may shift the liability from one party to the other, in ways that may not be foreseeable up front.

Increased accountability imposes more of the externalities of data breaches on the organisations, which should cause them to increase efforts to prevent data breaches and mitigate their impact.

Given the significant challenges in broader liability issues, and in light of our goals, we focus on the liability for the impact of data breaches on users.

In general, users are at the heart of our mission to increase access and trust in the Internet, goals that are even harder to reach when users are subject to the impact of data breaches, but do not have direct control over how their data is protected. More to the point, users are often the ultimate victims of data breaches, whether for identity theft, credit card details, or medical information, but are underrepresented in considerations about how to prevent and mitigate data breaches.

As discussed above, end users are the currently "the missing link". End users may not be told about breaches that impact them; may not be able to link a harm to a particular breach; and may have had to sign away their future liability claims to use the breached service. Further, where there is no direct customer relationship, they may have very limited recourse to recover money or benefit from measures such as credit monitoring services when there is a breach. Additionally, it can be very costly for users to take legal action against organisations.

We address several of these issues.

First, as discussed above, our position is that breach disclosure should generally take place. Breach notification is a step that helps establish increased accountability. It has the benefit of ensuring those whose data was involved know their data was taken, and can take action to protect themselves (and seek restitution, covered below). It also has the side benefit of causing appropriate reputational harm to the organisation breached, which should increase the incentive to prevent breaches. Given these costs, breach disclosure is most likely to occur in countries where it is required, as we have seen for the US.

We note that required breach disclosure has its limits – the organisation may not know that it was breached, or may not understand whether or what they need to disclose. The appropriate time to disclose may also be difficult to assess. The requirements to disclose are also difficult - too many notifications may lead users to feel helpless; too few and they feel left out.[22] Also, while breach disclosure may provide information that can prevent future breaches of a similar nature, the disclosure should not provide information to enable breaches, a distinct likelihood when known vulnerabilities are not always patched. As countries gain more experience with notification rules, and more countries adopt them, we expect the right balance will be found over time.

Second, the terms and conditions of many online services seek to impose severe restrictions on liability and the ability to seek restitution. For instance, this from one password manager company (their caps):[23]

OUR TOTAL LIABILITY TO YOU FOR ALL CLAIMS ARISING FROM OR RELATED TO THE SITE OR THE SERVICES IS LIMITED, IN AGGREGATE, TO ONE HUNDRED DOLLARS (U.S. $100.00)

For example, a password manager may store hundreds of passwords, whose breach could inflict costs on users far greater than the maximum USD 100 that is covered – this is a prime example of an externality a company makes their users bear.[24]

There are also sometimes restrictions on the ability to join a class action lawsuit (where users in a similar situation would join into one suit), requiring instead individual binding arbitration.[25]

In other words, users may need to undertake a difficult and costly exercise to potentially recover a small amount of money or services such as credit monitoring.

There is no simple answer here – online service providers are free to offer these terms (subject to consumer protection laws), and users are of course free not to use these services, if they actually read the terms and conditions and do not find them adequate. Fixes could result from market forces that increase demand for more user-friendly and fairer terms such as higher liability thresholds (resulting from increased awareness), or at the other end of the spectrum, laws that do not allow terms signing away users' rights, such as the ability to enter a class action suit.

In the example of a retail chain such as Target, the customers were not even using an online service. They swiped their credit card in a store, and it was only then the data was accessible to be breached. In that case, a class action suit by customers against Target was settled, but often such suits are dismissed for lack of demonstrable financial harm. This suggests the users have little rights over data about them unless they can show a direct quantifiable harm, instead of assuming the users have the intrinsic right to be protected from a breach.

It is not always clear what rights users have in the case of a data breach, and the deck today is stacked against the users. Nonetheless, some countries are already strengthening and clarifying the extent of individuals' rights in the event of a data breach in their laws. In the final point, customers may have to prove immediate and direct harm to be compensated following a breach. This does not take into account that they may be at long-term risk of identity fraud, or the cost in time and money of preventing identity fraud. Additionally, compensation may not cover non-financial harm.

This situation runs counter to a reasonable expectation that users' rights and interests will be protected if their privacy is breached. In addition to actual damages, both in terms of time and money, the increased risk of identity fraud and other potential future harms resulting from a data breach should be borne by the organisations who were breached, and not, as today, by the victims of the breach.

Users' rights and interests should come first. Organisations should make data security a key part of their governance. Stronger incentives are needed to protect personal information and to increase accountability for those who hold the data. There should be sanctions for poor practices, and remedies for affected individuals.

R5 SECURITY SIGNALS

Increase incentives to invest in security by catalysing a market for trusted, independent assessment of data security measures.

There is a fundamental informational asymmetry we all face as customers, users, employees, and even organisations, seeking to entrust our data to another party, and for the data holder seeking to be rewarded for their security levels.

In the issues section, we talked about the challenges for the seller of a used car to convey the quality of the car, and how this can result in a 'market for lemons' in cars, as the bad cars effectively drive the good cars out of that market. We also saw that even for a new car, there are a number of attributes of interest to us, and several ways we go about making sure the car meets those attributes.

How does this apply in our situation? Return to the example of the password manager. Users can search on certain attributes such as whether it is a cloud service and they can experience the service to see whether it is easy to use through a trial. But, they cannot determine in advance the security of the service. That, unfortunately, they may only learn the hard way through a breach.

Consider also the case of Target and other companies when choosing contractors. They are clearly choosing these contractors based on criteria related to the service they are offering, such as refrigeration or vending services. To the extent security is even considered before allowing the contractor to connect to, or access, their system, it is difficult to assess every contractor's systems and practices without great expense. As we have seen, many companies have difficulty keeping their own systems protected, much less assessing the security attributes of each and every contractor whose system may connect in some way.

As discussed, organisations must be able to send a credible signal enabling users, contractors, and employees, to assess their security against data breach, as well as other aspects of security, including the security of Internet of Things devices. As noted above, there are three key ways that this can be done – ratings, certification, or mandate.

In a final note on the Ashley Madison affair, in late August the privacy authorities of Canada and Australia released a report, which notes the parent company confirmed the trustmarks on the Ashley Madison website were fabricated by Ashley Madison.[27] This reinforces the idea that it is not enough to provide a signal – the signal must be credible, and that is typically provided by an independent trusted third party.

Three Key Ways to send a Credible Signal

Ratings. Consumer Reports has already begun to rate security software against a number of attributes, which can help users find the best software to protect their devices. While this is useful, it does not go directly to the question of data security. To our knowledge, no one has begun to do this yet for online services on behalf of consumers. This would be useful in deciding which online bank, medical service, or other sensitive service to entrust the custody of one's personal information. At the same time, such a service could provide a useful information by rating data security terms and conditions to help users choose the ones that provide the greatest protection in case of an attempted or actual breach. This would hopefully spur online service providers to begin to compete on providing user friendly terms and conditions regarding data security.

In another example of ratings based on security, a new independent third party company has begun to provide ratings of organisations' security, which helps insurance companies to underwrite cyber insurance policies.[28]

Certification. There is some activity towards a certification process for data security. UL, which already certifies a wide variety of electronic devices, is now certifying aspects of financial cybersecurity, such as point of sale terminals, and is beginning to develop a certification

standard for IoT devices.[29] At the same time, Peiter Zatko, a renowned cyber security specialist, is setting up a Cyber Independent Testing Laboratory, to certify the security of devices, as well as software and services. The results are meant to look something like a nutrition label, so not simply certifying, but offering details about various attributes of security.[30] Also, the APEC Cross Border Privacy Rules system requires certifying bodies (accountability agents) to certify an organisation's security safeguards against the program requirements.[31]

Certification processes are largely to help customers (whether organisations or end users) determine which services to use, which is very welcome. Additionally, they provide greater transparency across the industry.

Another approach is to encourage the implementation of industry-recognised best practice standards that can be certified or self-certified. For example, the US National Institute of Standards and Technology (NIST), working with stakeholders, developed a Cybersecurity Framework based on a Presidential Executive Order from 2013.[32] These represent industry best practices, and are voluntary, not mandatory. The process of implementation helps to increase the security of the organisations; although compliance is self-assessed, it can be used as a signal between organisations that they meet certain standards before creating a connected value chain.[33] Full compliance so far is limited, but it appears to be a promising approach.

Mandates. Finally, where outside rating or certification is not sufficient, or where adequate voluntary standards are not fully adopted, a government mandate may be needed. This is particularly true where the market failure is significant – either high externalities, or extreme asymmetric information. Privacy and data protection laws usually contain minimum data security requirements. As noted above, there are examples where mandates are most suited to resolving a market failure. In this case, our principle would be to mandate an outcome relating to data security (such as stored data should not be readable by unauthorised parties), rather than a tool or approach to achieve the outcome (such as a type of encryption), to allow organisations to innovate and find the most efficient way to meet the required outcome.

Finally, at the Internet Society we believe that 'permissionless innovation' has been a key driver of the Internet, where anyone can develop a new service or application, without prior approval from anyone. It is important to ensure any mandated requirements or certification processes do not conflict with this principle. They should only be a last resort and be designed not to create a barrier to entry.[34]

Catalyse a vibrant market for trusted independent assessment of data security measures so that organisations can credibly signal their level of data security. Credible security signals enable organisations to indicate that that they are less vulnerable than competitors, and increases the incentive to invest in better data security.

Data breaches are a growing concern worldwide. To mitigate this problem and its economic impact, we propose a shift in the approach to data breaches, involving all stakeholders.

As users increasingly move their lives online, to achieve the full benefits of the Internet worldwide there must be user trust. That trust is dependent on how users' data are protected from a breach. Each data breach creates a new group of users whose trust has been betrayed, which spreads to their acquaintances through word of mouth, and more broadly through news reports, creating doubt, which undermines user trust at large.

While users are the ultimate victims of data breaches, and their trust is affected, currently, users, and their trust, are not the main focus of approaches to data breaches. For example, organisations may gather and keep more user data than they need, and take less precautions than they could. In the aftermath of a breach, users may find their rights are limited. In the meantime, studies of the costs of data breaches tend to focus on the costs to organisations, with users mainly factored in based on the cost of lost business as a result of the breach.

The Internet Society proposes a user-focused approach to data breaches, in which organisations adopt a model of data stewardship to protect users' data, while embracing their collective responsibility to help make the Internet safer. Organisations should also be more transparent about the incidence of data breaches and their impact. This will help make data security a priority and create demand for the security tools and approaches that can help to prevent and mitigate data breaches. To provide incentives to use these tools, organisations need to be more accountable for the costs of data breaches than they are today. They should also bear more of the costs. But, organisations should also be given the ability to credibly send a security signal to the market that they have taken additional steps to prevent data breaches.

Law Enforcement

It is also important, in closing, not to put the entire focus on the potential and actual organisations being breached, but also to focus on the attackers themselves. In addition to greater efforts to prevent and mitigate data breaches, all efforts should be taken to reduce the benefits attackers are reaping and increase the risk of being caught. Law enforcement must have the proportionate means and resources to catch and penalise the attackers, while the attackers must be aware of the likelihood of being caught and the penalties, to reduce the perceived potential benefits from a data breach. Given the lack of digital borders for attackers to steal or transmit data, any such efforts must be international in nature to ensure maximum effectiveness.

Summary

An instructive parallel can be drawn with efforts to increase automobile safety over the past 50 years. As hard as it is to believe today, early cars did not have seat belts as standard, child safety seats only began to be introduced in the 1960s, and car companies fought airbag mandates. An early attempt to compete on increased safety by Ford, in the US, was perceived as a failure. These early tools provided passive safety, to protect passengers in case of a crash – in our terms, these are mitigation tools. Today these constraints are all standard, and car companies now invest and compete on safety, introducing a variety of active safety tools to avoid crashes, such as automatic braking – in our terms, these are prevention tools.

In between, a variety of familiar forces entered the market. First, increased awareness based on third parties, notably Ralph Nader's 1965 book Unsafe at any Speed, exposing the reluctance to add safety features. Then, mandates on certain features such as airbags that companies resisted; third party companies rating cars; and government agencies testing cars, including the famous Swedish 'moose test' to see if cars can safely avoid approaching obstacles. These features have all led to significant reductions in crash fatalities over time (normalised for increased number of miles driven). Looking forward, many argue that new partially or fully autonomous cars will further increase safety by automatically avoiding accidents. This comes back full circle to the topic of this report.

Autonomous cars will, of course, be controlled by a computer, and have communications built-in to communicate with the owner, and possibly with other vehicles for safety. As a result, of course, the computer can be hacked remotely, as already seen with the Chrysler Jeep. This can lead to a significant breach of data about the location and activities of drivers, not to mention the possibility of one or more cars being hacked and taken over.

More broadly, many of our recommendations are valid for preventing or mitigating breaches of the full range Internet of Things devices. Not just for the data they are gathering with their sensors, but also for a security breach leading to personal or public safety risks, with autonomous cars a leading example of the risks. As such, we encourage the application of the findings of our report to the relevant issues arising from the Internet of Things.

Recommendations:

1. Put users at the centre of solutions; and include the costs to both users and organisations when assessing the costs of data breaches.

2. Increase transparency through data breach notifications and disclosure.

3. Data security must be a priority. Better tools and approaches should be made available. Organisations should be held to best practice standards when it comes to data security.

4. Organisations should be accountable for their breaches. General rules regarding the assignment of liability and remediation of data breaches must be established up front.

5. Increase incentives to invest in security by catalysing a market for trusted, independent assessment of data security measures.

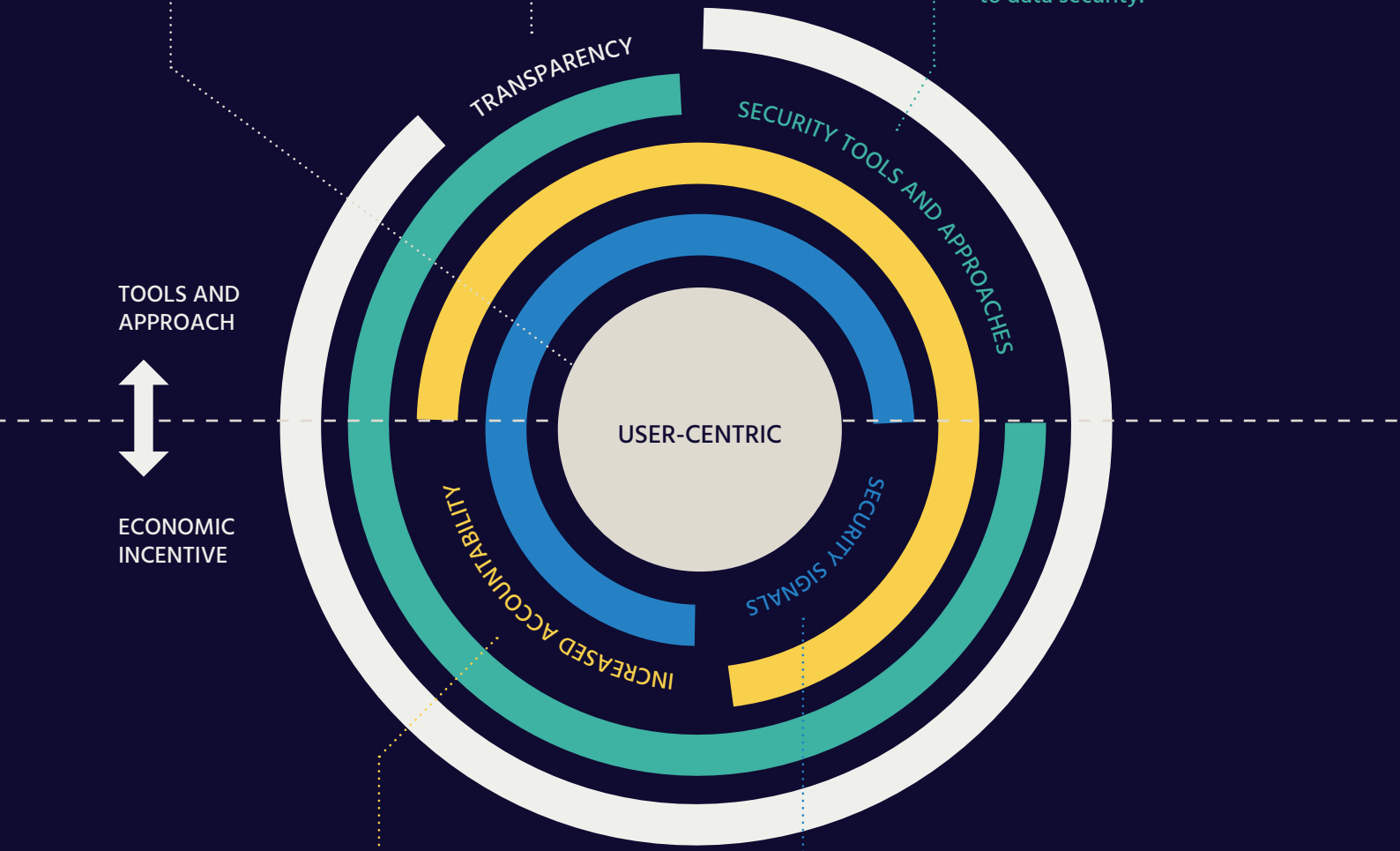
Underlying principles: data stewardship and collective responsibility

Security Circle

1. Put users at the centre of solutions; and include both users *and* organisations when assessing the costs of data breaches.

2. Increase transparency through data breach notifications and disclosure.

3. Data security must be a priority. Better tools and approaches should be made available. Organisations should be held to best practice standards when it comes to data security.



4. Organisations should be accountable for their breaches. General rules regarding the assignment of liability and remediation of data breaches must be established up front.

5. Increase incentives to invest in security by catalysing a market for trusted, independent assessment of data security measures.

1 The primary goal of data breach solutions should be to protect users and their data. Data breach risk assessments must include risks to the users whose personal data is at stake. Economic incentives should enable users to choose services that have better data security.

2 Organisations should warn users when a breach has occurred so that they can also take action to protect themselves. Data breach notification requirements help increase awareness and should be the norm, and are consistent with the user-centric approach this report advocates.

3 A breach of just one organisation could expose users' data held by multiple organisations – "your breach could be my breach" – we must share the responsibility to secure users' data.

Data security is a necessity, not a luxury. Data security should be a priority for everyone - from users to business to government.
Data security needs to be usable if organisations are going to use it.
Data security needs to be part of the design of systems (security-by-design) and business practices.

Organisations should secure data against known security vulnerabilities and be prepared to react against new threats. To improve data security, the marketplace needs incentives to produce usable data security tools.

Organisations should apply trusted tools and best practices to prevent phishing and block embedded malware. They should also train employees to help avoid social engineering attacks. Vendors should develop security features that nudge people to choose the more secure option.

Organisations should minimise the personal data they collect and store. Governments should encourage voluntary codes of conduct and other outcomes that favour data minimisation, along the lines of the OECD Privacy Guidelines.

Organisations should encrypt the data they hold.
Encryption needs to be strong, easy to use and implement.

4 Increased accountability imposes more of the externalities of data breaches on the organisations, which should cause them to increase efforts to prevent data breaches and mitigate their impact.

Users' rights and interests should come first. Organisations should make data security a key part of their governance. Stronger incentives are needed to protect personal information and to increase accountability for those who hold the data. There should be sanctions for poor practices, and remedies for affected individuals.

5 Catalyse a vibrant market for trusted independent assessment of data security measures so that organisations can credibly signal their level of data security. Credible security signals enable organisations to indicate that that they are less vulnerable than competitors, and increases the incentive to invest in better data security.

In summary, our message to organisations is:

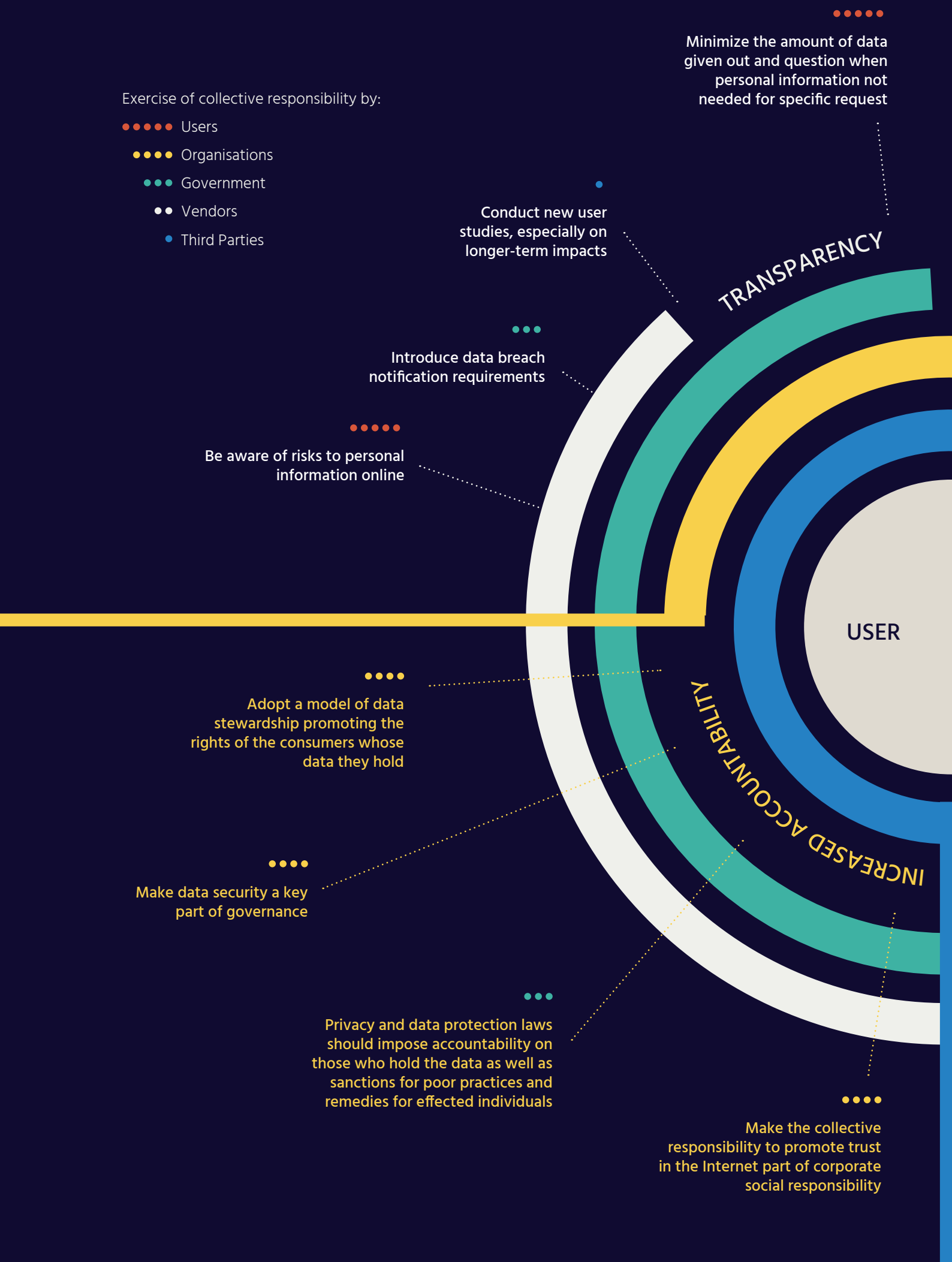
- Personal data is precious and priceless – protect it!
- Collect only what is absolutely necessary and encrypt what you keep
- Destroy data when it is no longer in use
- Restrict access to those who need to know
- Signal the level of data security you provide
- Be more transparent about data breach incidents
- Be alert to breaches, prepare, notify and act immediately

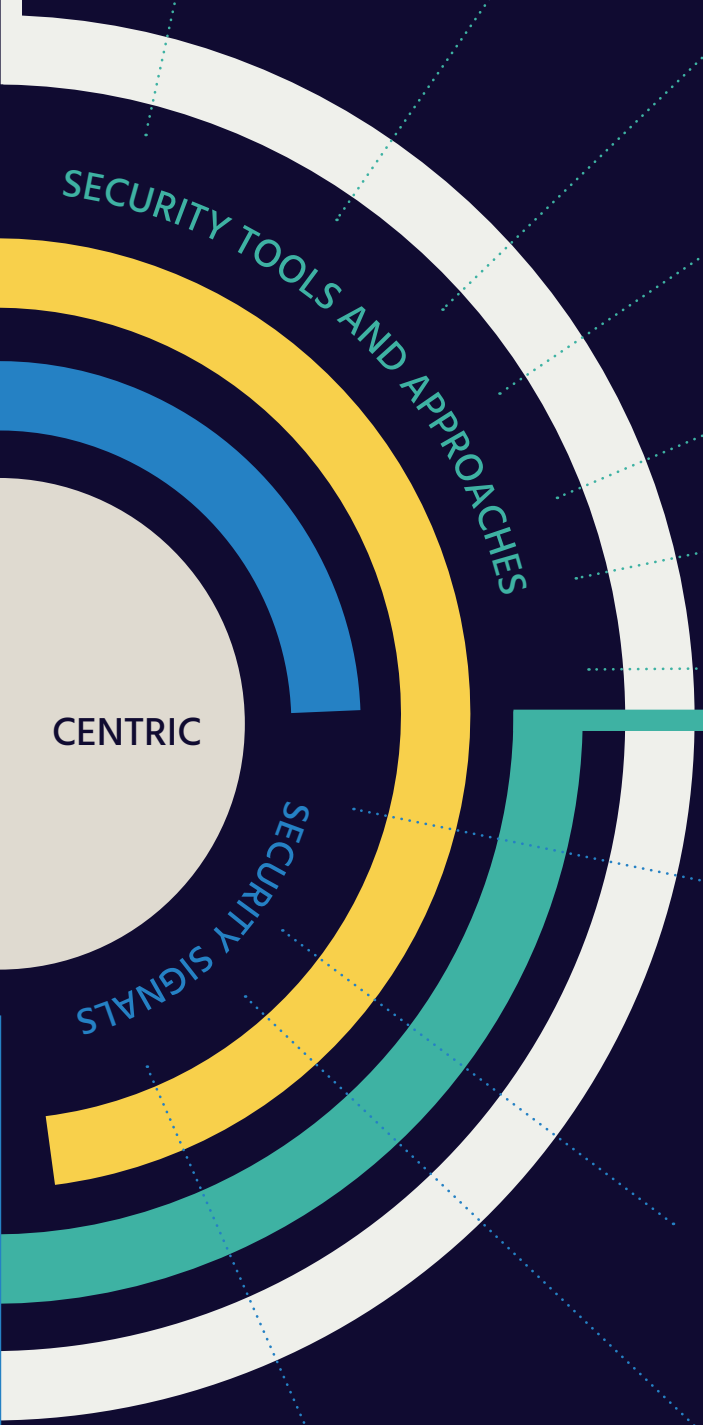
While organisations holding data are central to efforts to combat data breaches, we believe collaborative multi-stakeholder efforts are necessary, and summarise our recommendations across five main stakeholders, as follows.

- Organisations holding the data and subject to the data breaches
- Users whose data as customers is the target of data breaches
- Vendors of security equipment and solutions to help prevent and mitigate data breaches

- Third party agents, who can help to study data breaches and review equipment and security standards
- Government in the role of creating policy and laws that can address data breaches

We note again, in addition to the specifics of preventing and mitigating data breaches, all of us, as stakeholders in the Internet, have a collective responsibility to make the Internet a safer place for everyone. Actions to prevent data breaches of one organisation may help prevent them for others, and together we can all work to help restore and promote trust in the Internet. Further, as shown in the following diagram, these efforts should be user-centric, focused on protecting the privacy rights of users, in preventing a breach, and in addressing the impact on users following any breach.


Exercise of collective responsibility by:
Users
Organisations
Government
Vendors
Third Parties
Minimize the amount of data given out and question when personal information not needed for specific request
Conduct new user studies, especially on longer-term impacts
TRANSPARENCY
Introduce data breach notification requirements
Be aware of risks to personal information online
USER
Adopt a model of data stewardship promoting the rights of the consumers whose data they hold
INCREASED ACCOUNTABILITY
Make data security a key part of governance
Privacy and data protection laws should impose accountability on those who hold the data as well as sanctions for poor practices and remedies for effected individuals
Make the collective responsibility to promote trust in the Internet part of corporate social responsibility



Help defend against social engineering attacks at work and home

Encourage voluntary industry codes of conduct and other outcomes favouring data minimisation

Organisations should not start from the premise of what data are available, but rather what are the minimal data needed to provide the desired services

Develop new tools for prevention and mitigation that are easier to use and update

Apply tools and train employees to stop social engineering attacks

Deploy best practices in system and network security architecture[35]

Apply encryption as the norm for data in transit and at rest

Support the development of independent and credible third parties for developing security signals

Consider safety mandates where market forces not sufficient

Trusted independent third parties can play a critical role in verifying the level of data security offered by service providers

Improve their own security signals, while considering them when connecting with other organisations

Footnotes

[1] See http://www.internetsociety.org/collaborativesecurity

[2] http://www.internetsociety.org/preserving-user-centric-internet

[3] For Windows 7, introducing automatic updates led to 90% of users upgrading within one week. See https://blogs.msdn.microsoft.com/b8/2011/11/14/minimizing-restarts-after-automatic-updating-in-windows-update/. Apple had the ability to automatically update for several years before first using it in late 2014 in response to a critical security vulnerability. See http://www.cnet.com/news/apple-updates-macs-without-asking-but-its-to-foil-hackers/. This feature could be turned off.

[4] Of course, not all of these hacks were necessarily caused by social engineeering, but the results are well within the potential outcomes of social engineering. For more information about preventing social engineering, see https://digitalguardian.com/blog/phishing-attack-prevention-how-identify-avoid-phishing-scams.

[5] As noted by Bruce Schneier, "The problem isn't that people are idiots... The problem is that the OS trusts random USB sticks." See https://www.schneier.com/blog/archives/2011/06/yet_another_peo.html.

[6] Two-factor authentication requires two components, which can include something that the user knows, and something that the user has. For instance, getting money out of an ATM machine requires both a PIN (something the user knows) and a bank card (something the user has) – neither is sufficient alone. On the Internet, two-factor authentication used to involve a physical token that generated a unique code (often time-sensitive) that was used along with the user password; now, with widespread mobile phone use, the website has other options. For example, it can send an SMS message to the user's mobile phone, which can be used alongside the password.

[7] See, for instance, https://www.m3aawg.org/sites/default/files/M3AAWG_AWPG_Anti_Phishing_Best_Practices-2015-06.pdf.

[8] See http://www.tomsguide.com/us/password-manager-pros-cons,news-19018.html for a sampling of the discussion for and against password managers.

[9] See, for example, http://www.wired.com/2016/01/you-need-a-password-manager/

[10] See http://gizmodo.com/am-i-an-idiot-for-still-using-a-password-manager-1711673486.

[11] The terms of Dashlane state (capital letters theirs): OUR TOTAL LIABILITY TO YOU FOR ALL CLAIMS ARISING FROM OR RELATED TO THE SITE OR THE SERVICES IS LIMITED, IN AGGREGATE, TO ONE HUNDRED DOLLARS (U.S. $100.00). See https://www.dashlane.com/terms.

[12] While a password manager, like other services, may have one or more security badges present, most users would not be able to assess their significance. See https://www.dashlane.com.

[13] We note that these recommendations are by no means exhaustive, but rather are illustrative. For instance, data partitioning– the practice of storing data separately so that any single piece, if breached, is not sufficient – is another option for securing the data that remains after data minimisation.

[14] See http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm.

[15] See https://ico.org.uk/for-organisations/guide-to-data-protection/principle-3-adequacy/, and see also http://www.forbes.com/sites/bernardmarr/2016/03/16/why-data-minimization-is-an-important-concept-in-the-age-of-big-data/#a111dfb327fd.

[16] For more on data misuse, see https://www.bcgperspectives.com/content/articles/big-data-advanced-analytics-technology-digital-bridging-trust-gap-hidden-landmine-big-data/?utm_source=201607&utm_medium=Email&utm_campaign=Ealert.

[17] See http://www.techrepublic.com/blog/it-security/why-does-an-android-flashlight-app-need-gps-permission/.

[18] See, for example, the note from the US Social Security Administration on the connection between social security number and identity fraud, at https://www.ssa.gov/pubs/EN-05-10064.pdf

[19] See http://www.internetsociety.org/encryption for more details.

[20] See http://www.pcworld.com/article/2982919/security/ashley-madison-coding-blunder-made-over-11-million-passwords-easy-to-crack.html.

[21] WhatsApp introduced end-to-end encryption for all communications on its app, see https://www.wired.com/2016/04/forget-apple-vs-fbi-whatsapp-just-switched-encryption-billion-people/, while Apple has done so for data on iPhones, see https://www.wired.com/2014/10/golden-key/. We note that in both cases, encryption is by turned on automatically; for WhatsApp in fact it cannot be turned off.

[22] The Netherlands implemented a data breach notification law as of 1 January 2016, ahead of the EU, and in a foreshadowing of what is to come, already 1500 data breaches were notified in the first four months. See https://iapp.org/news/a/130-days-1500-notifications-does-dutch-breach-rule-foreshadow-gdpr/

[23] See https://www.dashlane.com/terms. We note that this is not unique to the password manager we took this example from, but rather an example that is common to online services. While the ability to impose such terms, and to enforce them, might vary by country, overall they do emphasize the desire and attempt by providers to limit their own liability.

[24] On the other hand we have to consider that an insolvent company will not be able to compensate their customers either. These are trade offs with potential unintended consequences. A robust cyberinsurance market may enable companies with better security to increase their liability levels without financial risks.

[25] Disallowing a class action suit increases transaction costs, because each customer must separately sue the company, which raises their costs, rather than working together which would be more efficient.

[26] For a broad discussion of ethical data handling, see https://www.internetsociety.org/sites/default/files/Ethical%20Data-handling%20-%20v2.0.pdf.

[27] See http://www.dataguidance.com/international-ashley-madison-report-likely-to-serve-as-benchmark/

[28] The company, a startup called UpGuard, has developed the Cybersecurity Threat Assessment Rating (CSTAR) that provides cyber risk scores based on an external assessment from the public web, and an internal search. See http://www.forbes.com/sites/brucerogers/2016/02/11/upguard-out-to-disrupt-7-5-billion-global-cybersecurity-insurance-market/#6b7370112dda.

[29] See http://www.ul.com/newsroom/pressreleases/ul-launches-cybersecurity-assurance-program/. See also http://arstechnica.com/security/2016/04/underwriters-labs-refuses-to-share-new-iot-cybersecurity-standard/

[30] Id. See also http://blogs.cfr.org/cyber/2015/12/18/qa-with-peiter-zatko-aka-mudge-setting-up-the-cyber-independent-testing-laboratory/. Of course, the question would be how to convince users to trust this certification over any other.

[31] See APEC Cross-Border Privacy Rules Program Requirements, which can be downloaded from this page http://www.cbprs.org/GeneralPages/APECCBPRSystemDocuments.aspx

[32] See http://www.nist.gov/cyberframework/. The NIST website states about the Framework: "Recognizing the national and economic security of the United States depends on the reliable function of critical infrastructure, the President issued Executive Order (EO) 13636, Improving Critical Infrastructure Cybersecurity, in February 2013. The Order directed NIST to work with stakeholders to develop a voluntary framework – based on existing standards, guidelines, and practices - for reducing cyber risks to critical infrastructure.

Created through collaboration between industry and government, the Framework consists of standards, guidelines, and practices to promote the protection of critical infrastructure. The prioritized, flexible, repeatable, and cost-effective approach of the Framework helps owners and operators of critical infrastructure to manage cybersecurity-related risk."

[33] According to one NIST policy advisor, "Organizations also can readily use the framework to communicate a current or desired cybersecurity posture between a buyer or supplier, potentially strengthening the security of their supply chains," See http://thirdcertainty.com/featured-story/few-adopt-nist-cybersecurity-guidelines-but-that-could-change/. Another example of government certification that can also help send a signal to other organizations is the Federal Risk and Authorization Management Program (FedRAMP)accreditation for cloud services. See http://www.zdnet.com/article/microsoft-amazon-both-receive-highest-fedramp-status-for-their-government-clouds/.

[34] For more on permissionless innovation, see https://www.internetsociety.org/internet-invariants-what-really-matters..

[35] For a broader view of the efforts needed to combat data breaches, see the Online Trust Alliance 2016 Data Protection & Breach Readiness Guide, at https://otalliance.org/resources/data-breach-protection.

ANGLER

A popular exploit kit in 2015 is called Angler. According to one source, it might cost up to USD 30,000 to buy, but could return millions in revenues just from imposing ransoms on users to get their data back. Other uses include accessing login details for a further attack. The kit is 'user-friendly' from the attacker perspective, and continuously updated to evade attacks and find new vulnerabilities.

ASYMMETRIC INFORMATION

Asymmetric information arises when one party to an agreement or exchange has more information than the other about the object of the exchange. For more details, see the 'Economics 101' section.

CREDIBLE SIGNAL

A way to avoid problems resulting from asymmetric information is for one party to a transaction to send a signal that reveals relevant information to the other party. In order to be effective, the signal must be credible. For instance, to get around the problem of asymmetric information about the quality of a used car, the seller of a high quality car may offer to provide diagnostic information from an independent mechanic, as a means to justify an increased sales price. This is an offer that a seller of a low quality car would not make, as it would reduce the sales price.

DATA BREACH

What is a data breach? "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a public electronic communications service"
The Information Commissioner's Office (ICO) of the UK[1]

EXTERNALITIES

Positive or negative externalities arise when a decision taken by one party provides a benefit, or harm, to other parties, who have no voice in the decision. For more details, see the 'Economics 101' section.

FINANCIAL ACCESS

Financial access theft, such as credit card information, may enable someone to use the credit card, but as soon as it is reported, the card is no longer usable. Identity theft, on the other hand, enables the thief to apply for credit cards in this identity – which may only be discovered when the real person's credit starts to suffer, and can sometimes take years to reverse.

KNOWN VULNERABILITY

A known vulnerability is, as the name implies, a vulnerability that is known; the aftermath of a zero-day exploit. These vulnerabilities typically have patches, but these patches are not always used, resulting in a surprising number of data breaches from known, and thus preventable, vulnerabilities.

MALWARE

The Wikipedia definition for Malware is an umbrella term used to refer to a variety of forms of hostile or intrusive software, including computer viruses, worms, trojan horses, ransomware, spyware, adware, scareware, and other malicious programs. It can take the form of executable code, scripts, active content, and other software.

MARKET FAILURE

In economics, we say there is a market failure when a market outcome is not efficient. A market outcome is efficient when no one could be made better off without harming someone else. One example of a market failure is monopoly power – when one company controls the market and can set prices higher than in competitive markets, then there will be potential customers who are willing to pay the cost, but

not the inflated monopoly price. This excess demand is inefficient. In the case of a market failure, there is an argument that a third party could intervene. This is the role, for instance, of competition or antitrust authorities in governing market power.

PHISHING

Phishing is a form of social engineering, in which typically an email is sent that appears to be legitimate, and requests a user to log in to a fake website as a means to capture their password. By spamming large numbers of users, the hackers can capture information that may lead to a data breach of an organisation associated with the user who was tricked.

PLUGINS

Software providers can enable third-party developers to add features to their software through plugins. For instance, web browsers enable plugins to be developed and installed by users to run audio, video, or offer other features such as changing the look and feel of the original software.

A common example of a plugin is Adobe Flash, which enables audio or video playback on web browsers. Developers of video content can make it available in Adobe Flash, and users will be prompted to download the Player plugin to view such content, if they do not already have it.

RECORD

A record is defined here as the personal information that corresponds to an identifiable person, which was lost or stolen in a data breach.

SIGNAL

When it is difficult for customers to distinguish the quality level between goods or services, asymmetric information poses a problem. In particular, the seller with high-quality items wants to distinguish themselves from the lower-quality sellers. One solution is to send a desirable signal to potential customers – to be credible, the signal must be one that only high quality sellers can make. Branding is one type of signal – a company that invests in advertising its brand sends a signal it knows it is high quality and will be able to recoup its investment. Banks attempt to send a similar signal by investing in expensive buildings. However, given the importance of banks in the economy, governments may support deposit insurance as the ultimate credible signal to customers that their deposits are secure.

SOCIAL ENGINEERING

Social engineering is a set of techniques whereby employees may be tricked into giving up confidential information relevant to data security, such as their password or other identifying information. One common form of social engineering is known as phishing. More information on social engineering is in the issues section.

ZERO-DAY EXPLOIT

A zero-day exploit takes advantage of a zero-day vulnerability. A zero-day vulnerability is a computer software vulnerability that was unknown or undisclosed before it was exploited for the first time, leaving the developer of the software with zero days to patch the vulnerability when the exploit occurs. As such, zero-day vulnerabilities are a significant threat to data security. They have value for attackers, who can construct their own exploits, sell them on the black market, or sell the information about the vulnerability to the software developer so they can be patched.

[1] See https://ico.org.uk/for-organisations/guide-to-pecr/communications-networks-and-services/security-breaches/.