EUROPEAN ASSOCIATION FOR VISUAL DATA SECURITY

SECURE

Visual Data Security White Paper

Brian Honan, BH Consulting

July 2012

Introduction

Welcome to Secure's White Paper on Visual Data Security.

As data gets ever more versatile and mobile, we want to make sure that individuals, businesses, organisations and governments across Europe are aware of the threats posed by visual data security breaches.

Simply put, visual data security is ensuring that information cannot be seen by unauthorised individuals. This is particularly important when dealing with private or sensitive information, and the threat of a breach has risen enormously with the shift in working practices towards increased mobility, flexibility and shared resources.

This White Paper has been commissioned to give some background to visual data security and provide simple, easy to follow advice on how to prevent a breach and protect individuals' personal data and organisations' commercially sensitive information.

It's not about constraining people's working habits or holding back the tide, but about embracing new trends and empowering employers and employees to take small steps to work in a safe and secure manner.

By promoting a greater understanding of these risks and the behavioural and practical procedures that can be adopted to reduce them, we hope to enhance data security across the continent.

We hope you find the Paper of interest. For any further information please don't hesitate to contact us on info@visualdatasecurity.eu.

Happy reading and stay secure!

Secure is:

1. Visual Data Security – The Weak Link in Information Security

The incomplete approach to data security

Data loss and theft has the potential to affect all of us – from private individuals to small businesses and multinational corporations. While awareness of the threat posed by a data breach is increasing, there is still a lack of understanding of the many ways in which such a breach can occur and, most importantly, little awareness of the often simple steps that can be taken to prevent personal and business data loss.

Whilst the vast majority of companies have taken some action to protect themselves through the installation of security software and hardware such measures, while important, only address part of the data security threat.

One core area of data security which is often overlooked is the very real possibility of a visual data security breach – the potential for sensitive, personal information and data to be seen, captured and utilised by unauthorised individuals. These risks are present wherever data is displayed on screen – whether that's inside or outside the office – and on any device, from smartphones to tablets and from laptops to desktops. Facing more frequent and more innovative data attacks, organisations must ensure that the defences they have in place protect against all potential data breaches and not just some.

The ever-increasing threat

The cost to businesses of data loss and cyber-crime is increasing rapidly. Europol has reported that the cost of cybercrime to companies worldwide is €750 billion a year[1]; a survey by Symantec and the Ponemon institute published in June 2011 found that 84% of British, French and German businesses had suffered some form of data breach[2]; and in March 2012 the U.S. Office of Management and Budget revealed that a total of 107,655 security incidents were reported in to it in 2011[3].

In his speech at the Lord Mayor of London's 2012 Annual Defence and Security Lecture, Jonathan Evans, the Director General of the UK's MI5 Security Service, argued that cyber-attacks from cyber criminals and enemy states pose a significant threat to the UK's economy. [4] Mr. Evans used the example of a "major London listed company", which suffered from a cyber-attack that resulted in an estimated loss of £800 million. That loss was made up of intellectual property losses and from "commercial disadvantage in contractual negotiations". In the United States the FBI have issued warnings that foreign nations are spying on US companies in order to obtain new technology and trade secrets for their own use.[5]

[1] https://www.europol.europa.eu/content/press/cybercrime-presents-major-challenge-law-enforcement-523
[2] http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=ponemon-cost-of-a-data-breach-2011
[3] http://www.reuters.com/article/2012/06/13/net-us-media-tech-summit-cyber-disclosur-idUSBRE85C1E320120613
[4] https://www.mi5.gov.uk/output/the-olympics-and-beyond.html?dm_i=XM9,UU64,6JFT42,2JDL5,1
[5] http://www.latimes.com/business/la-fi-economic-espionage-20120629,0,6452528.story

The above statistics do not include the impact on individuals, whose personal data may be lost following a security breach at a company to whom they entrusted their data. This can lead to those affected individuals suffering financial losses, emotional stress and damaged credit ratings. In the UK, the National Fraud Authority has estimated that the cost of identity theft is £2.7bn per year.[6]

For many organisations the focus of IT security initiatives has been on protecting such sensitive information electronically. To this end the majority of security investment is on tools and techniques such as encryption, designed to secure the information when it is in transit or while it is stored; on complex access control solutions to prevent unauthorised access; on sophisticated firewalls to restrict access between networks; and on Intrusion Detection Systems and anti-virus software to detect and block any cyber-based attacks. According to a report published by PwC, global spending on cyber security in 2011 was US$ 60 billion, with spending over the next three to five years likely to grow at a rate of 10% per year.[7]

Modern working trends and their impact on security

Today's modern workplace is no longer constrained by office walls or buildings. Mobile computing allows workers to work from home, hotels, remote offices, trains, airports, in fact from anywhere an Internet connection can be found. This flexibility enables businesses to be more productive and engage better with clients, colleagues and partners, while also providing the ability to enable employees be more productive and achieve a better work-life balance.

Flexible working practices are also taking hold in the office. Hot desking, where people move around the office and utilise space when and where they need it, challenges the organisation of the traditional office, and creates potential security issues where employees have different levels of security clearance or seniority. This flexibility is matched by trends towards sharing office space, often in the public sector, where functions for different departments or bodies can be carried out in the same space, creating security risks where data is displayed on screen.

The drive by many organisations to adopt a Bring Your Own Device (BYOD) strategy to allow employees more flexibility and productivity is also accelerating the growth in mobile devices, and correspondingly the risk of a data breach. A recent study by Good Technology shows that 45% of companies already have BYOD strategies in place.[8]

Technological advances have been key in enabling this explosion in remote working. Smartphones, home computers, laptops, ultrabooks, tablet computers, mobile broadband and Virtual Private Networks allow companies expand their computer networks outside the traditional physical boundaries of their own offices. According to research by Virgin Media Business, 64% of businesses now offer remote working for their employees, this is an increase of 357% from 2010 when only 14% provided this option.[9]

[6] https://www.identitytheft.org.uk/cost-of-identity-fraud.asp
[7] http://www.pwc.co.uk/en_UK/uk/assets/pdf/cyber-security-m-a.pdf
[8] http://media.www1.good.com/documents/Good_Data_BYOD_2011.pdf
[9] http://www.newbusiness.co.uk/news/mobile-working-massive-growth-seen

Increasing numbers of people are now taking advantage of the opportunity mobile working gives them to continue working outside the office. A Good Technology report shows that 93% of employees continue to work when they are out of the office,[10] with many working up to an extra 7 hours per week.[11] Of those surveyed, 38% said their job would be impossible without mobile access to their emails.

These statistics are backed up by a similar survey conducted by the Chartered Society of Physiotherapy, which found that nearly two thirds of the 2,010 people surveyed admitted to continue working outside the office up to an extra 2 hours per day, often while commuting.[12] Furthermore, a survey conducted by IDC found that 72% of workers in the United States have some form of work mobility.It also reported that by 2015, the number of mobile workers worldwide will reach 1.3 billion, representing a significant 37.2% of the global workforce.

The growing risks...

However, with these new working practices come a number of risks that organisations need to ensure are addressed properly. The most important asset of many businesses is the data they use to support their decision making processes, to develop their products and services, and to communicate sensitive business information. This data is vital to the survival of the business. But technological change means that this data is now accessible outside the physical security of the office.

Just as businesses find this data valuable, it can be equally as valuable to others such as criminal hackers, organised criminals, Hacktivists, disgruntled employees and, in some cases, nation states. Losing data can lead to direct financial losses, legal and regulatory issues, fines, and reputational damage.

An incomplete response

With the growing threats to information stored and processed on computers there is an ever growing list of regulatory, legal and industry compliance requirements for organisations. These can vary from industry to industry and from country to country. Although some regulations in Europe stem from the European Union's Data Protection Directive,[13] there is still a broad range of different privacy laws on how Personally Identifiable Information should be protected, such as the UK Data Protection Act, in different jurisdictions. Publicly traded companies in the United States have similar regulatory requirements under Section 404(a) of the Sarbanes-Oxley Act (SOX)[14].

[10] http://www.cityam.com/latest-news/failure-switch-increases-work
[11] http://www.infoworld.com/d/consumerization-of-it/stop-it-youre-working-extra-unpaid-day-week-196870?page=0,0&source=rss_infoworld_blogs
[12] http://www.bbc.co.uk/news/health-18490433
[13] http://ec.europa.eu/justice/data-protection/index_en.htm
[14] http://www.sec.gov/info/smallbus/404guide.shtml

The ever increasing legal, industry and regulatory requirements being placed on organisations means that companies need to ensure they are taking the appropriate measures to protect the sensitive information under their control. In the office, new working practices are throwing up new challenges, with greater flexibility changing the traditionally settled office environment. With the ever increasing mobile workforce, organisations need to look beyond the protections they have in their physical offices and take steps to ensure the security of that data when it is being accessed by their staff at home, while commuting, in hotels or coffee shops, or in airports.

However, despite the increasing awareness of the threats posed to computer systems, the various regulatory requirements, and the increasing investment in cyber security, the area of visual data security remains largely overlooked. Many organisations still fail to secure information while it is being displayed on computer screens. While data can be protected while it is stored on the computer, laptop, tablet or smartphone it has to be displayed on the screen for the employee to work on.

Accessing data on a computer screen can undermine the time and investment spent in sophisticated computer security solutions. Anyone else who has visual access to the screen, be that in an office, hotel, commuter train, coffee shop or airport can also read the data the employee is looking at. This gap in an organisation's information security strategy can leave it exposed to a security breach, and this could potentially lead to a loss of profit, a loss in competiveness, incurred costs from dealing with the incident, a negative impact on the organisation's reputation, a loss of confidence by customers and, depending on the type of data impacted, fines.

2. Visual Data Security – the ever present and growing threat

The simplicity of breaching visual data security

A Visual Data Security breach can happen in a number of ways, including:

- Unauthorised people viewing sensitive information while it is displayed on the screen
- Unauthorised people capturing images of sensitive information using high resolution digital cameras or smartphones with integrated high resolution digital cameras.
- Passwords or other sensitive information displayed on the screen which could subsequently be used by an attacker to access other systems.

An everyday occurrence

In a 2012 survey conducted by the UK Polling organisation ComRes, nearly ¾ of employees (71%) surveyed, have been able to see or read what someone is working on – either in the workplace or in a public place such as on a train, in an airport or a coffee shop. The results support a 2010 survey by People Security, which found that 80% of respondents had read material on another person's computer screen whilst on public transport, in a coffee shop or in shared work places[15]. 57% of people in a surveyed for the Visual Data Security Study 2010[16] said that they had stopped working on their laptops in public because of concerns over privacy.

A survey of IT professionals conducted by BH Consulting for this paper found that:

- 85% of those surveyed admitted to seeing sensitive information on screen that they were not authorised to see
- 82% admitted that it was possible information on their screens could have been viewed by unauthorised personnel
- 82% had little or no confidence that users in their organisation would protect their screen from being viewed by unauthorised people

The urgent need to raise awareness

An overwhelmingly majority (98%) of those surveyed by BH Consulting agreed that that it is important to educate individuals on the overall visual data security threat and how they can prevent a breach. However, only 56% currently had some sort of measures in place to safeguard visual data security. Of those that have put in visual data security safeguards the majority of these are relying on staff being both aware of policy and complying with it to prevent a security breach. Given these statistics and the increasing number of employees that are now working remotely or in a flexible

[15] http://solutions.3m.co.uk/wps/portal/3M/en_GB/MobileInteractive/Home/Products/PrivacyFilters/
[16] http://solutions.3m.com/wps/portal/3M/en_US/3MScreens_NA/Protectors/For_Organizations/Industry_Whitepapers/Visual_Data_Breach_Risk_Assessment/

office environment, there is clearly a major gap in many organisations' security defences when it comes to visual data security.

Mobile data capture

Digital cameras are now ubiquitous, as they are often used for Closed Circuit TV, embedded within computers and tablets, and built into most modern smartphones – of which over 1 billion are now sold every year.[17] These cameras can capture high quality images of data displayed on a screen, images which can be easily analysed by a human or modern computer programmes. They thus pose a clear risk to visual data security. In many cases the use of such cameras would go unnoticed by the person whose information was being captured. Once captured on camera the images of the screen can later be downloaded onto a computer for further examination and quickly shared with others via the Internet, email or social media.

The difficulty detecting a breach

Organisations will often never know if they have suffered a visual data security breach. Security breaches resulting from intruders hacking into a computer network or from a computer virus infection can be easily proven through evidence gathered in log files and other mechanisms. As there are no log files to record who looked at a computer screen at a particular time in a particular location this can falsely lead organisations into thinking visual data security is something not to be concerned about. In the past it would have been relatively easy to detect someone looking at and capturing data displayed on a screen in a public place, as they would have to be relatively close to the screen to do so. However, modern screen technology now provides for higher and crisper resolutions with better quality displays making it easier to see what is on the screen from further away.

Once an unauthorised user has seen and/or captured sensitive information there is no way to predict how they will react. They could keep the information to themselves and take no action. Equally, depending on the type of information exposed and whether it could lead to scandal or embarrassment for the organisation in question they could alert the media to the content. If the exposed information has monetary value it could be sold onto competitors, criminals or used to blackmail the affected company, or used to commit fraud.

[17] http://www.strategyanalytics.com/default.aspx?mod=reportabstractviewer&a0=6216

3. Examples of Visual Data Security Breaches

There have been a number of high profile cases where confidential information has been displayed publicly, leading to embarrassing security breaches. Notable public examples include:

- A senior UK civil servant who fell asleep on a commuter train leaving highly sensitive information displayed on his screen. A fellow passenger took two photographs of the information while it was displayed on the screen.[18] This was later reported in the national media.

- In the United States the private details of clients of a Bank of America branch office in downtown St. Petersburg were visible through the bank's windows to people on the street outside the bank's offices.[19]

- In their report on Data Loss Prevention[20] the consultancy firm Ernst & young cited a case they investigated for a client where "A call centre staff member provided screenshots of internal systems to fraudsters to help them reverse engineer an application."

- In August 2011 the UK's International Development Secretary was photographed leaving Number 10 Downing Street with sensitive government papers relating to Afghanistan on display.[21] These papers were caught on camera by news photographers and film crews.

- A similar blunder by the then Assistant Commissioner, Bob Quick, of the London Metropolitan Police Force's Counter Terrorism unit led to secret documents outlining a planned police raid on a terrorist cell being caught on camera as he entered Number 10 Downing street.[22] The blunder led to Mr. Quick's resignation from the position.

There are of course many instances of, often severe, corporate and private data loss from visual data security breaches which go unreported.

[18] http://www.dailymail.co.uk/news/article-1082375/The-zzzzivil-servant-fell-asleep-train-laptop-secrets-view.html
[19] http://www.tampabay.com/features/consumer/simple-fix-to-bank-security-breach-close-the-blinds/1139356
[20] Insights on IT risk, Business briefing, October 2011, Data Loss Prevention - Ernst & Young
[21] http://www.telegraph.co.uk/news/politics/8731143/Minister-accidentally-reveals-Afghanistan-documents.html
[22] http://www.telegraph.co.uk/news/uknews/5129561/Bob-Quick-resigns-over-terror-blunder.html

4. Legal and best practice implications

Whilst it is well established that organisations must have data protection safeguards in place to comply with legislation, such as the UK's Data Protection Act, there is little awareness that companies can be in breach of such legislation if they do not take adequate measures to prevent a loss of information from a visual data security lapse.

Best practice procedures – such as the ISO 27001:2005 Information Security Standard[23] and The Standard of Good Practise for Information Security developed by the Information Security Forum[24] – explicitly require organisations to take steps to ensure the visual data security their information. Such steps include:

> *"siting computer equipment (eg server console screens, workstations and printers) so that sensitive information cannot be overlooked" ISF The Standard of Good Practise for Information Security*
>
> *"information processing facilities handling sensitive data should be positioned and the viewing angle restricted to reduce the risk of information being viewed by unauthorized persons during their use," section 9.2.1 Equipment siting and protection of ISO 27002:2005*

As a result, it is becoming increasingly important that organisations address the area of visual data security and ensure that appropriate measures are taken to protect sensitive data from unauthorised access when it is on display, not only in public places but also in employee's homes and indeed within the organisations' offices themselves.

[23] http://www.iso.org/iso/catalogue_detail?csnumber=42103
[24] https://www.securityforum.org/?page=2011sogppublicorder

5. Steps to Improve Visual Security

In light of the increasing threat the UK government is undertaking a series of measures to improve its visual data security.[25] These measures include training, screen positioning, anonymising data and using privacy screens.

Other organisations need to follow the lead of the UK government and take proactive steps to protect their data from being accessed by unauthorised parties when displayed on computer screens.

There are a number of simple steps organisations should consider implementing in order to ensure they can better protect their sensitive data when being accessed by employees remotely. The following measures should be included into an overall Visual Security Policy which should include the following;

- Identify Sensitive Data:
  Knowing what sensitive data you need to be concerned about is a crucial step in determining how best to protect it. It is important to know what information, be that client details, business plans, or intellectual property, is sensitive and therefore should be protected.

- Classify Data:
  Once you have identified the key data sets for your organisation it is important to classify it according to its sensitivity. This makes it easier to determine who should have access to the data and what type of access that should be.

- Access Control:
  You should implement strict access control mechanisms to ensure only authorised personnel access the data. It is also important to ensure users only have access to the data they need to conduct their role.

- Know Where Your Data Is:
  Information can be easily copied from one location to another and users may download sensitive information onto their portable device to work on. You should conduct regular audits to ensure that sensitive data is located on authorised systems and not located on systems or devices that are not authorised.

- Monitor Access:
  Make sure that audit trails and security logging are set up to monitor who accesses data and when. This can alert you to users who may be attempting to copy sensitive data onto their personal device or provide evidence to investigate a potential breach.

[25] http://www.guardian.co.uk/government-computing-network/2011/jun/23/whitehall-visual-data-security-training

- Regularly Review Remote Access:
  Regular reviews of who has accessed data and sensitive systems remotely should also be conducted. These reviews can help determine whether authorised users are accessing data from secure or insecure locations.

- Manage Remote Access:
  It is important that only those authorised to access sensitive data from outside the organisations network do so. Regular reviews of the remote access solution, such as a VPN (Virtual Private Network), employed should be conducted to ensure that those with remote access are authorised. What systems and data users can access remotely should be configured so that they only access those systems and data they require to do their job remotely. Remote access to systems not required for their role should be removed.

  In addition, consideration should be given to the levels of access given to remote users depending on their location when accessing the data. If the remote user is attempting to access the data from a trusted location such as their home or a remote office then that access could be granted, however if they are attempting to access the data from an untrusted location such as a wifi-hotspot or via mobile broadband then access could be denied or the data available restricted.

- Password Protected Screen Savers:
  It is important that when users are not using their computers that information on the screen is secured. In particular if the user should move away from their computer and leave it unattended it should not be possible for someone else to access the screen. Information on unattended screens can be protected by the use of password protected screen savers which can automatically activate after a predefined period of inactivity on the system.

- Security Awareness:
  One of the most important measures that can be taken to improve visual security is to train staff of the threats to visual data security and what steps they can take to address them. When working in public places users should be encouraged to be aware of their surroundings and to ensure that any data on their screens cannot be overlooked. Users should also be trained to turn off their screens or computers if they feel their screen is being observed by unauthorised personnel and should be encouraged to report suspected breaches to management. For example, if they feel that suspected breach was a deliberate action by a fellow member of staff this could highlight a disgruntled or malicious employee.

- Privacy Screens:
  For those users who regularly work on sensitive information or who in public areas – be they branches, stores, or simply public areas that the user can work from such as coffee shops or public transport – privacy screens should be deployed on each computer to reduce the risk of sensitive data being overlooked by unauthorised personnel.

- Siting of Equipment:
  Computer screens should be positioned and/or angled in such a way to make it difficult for unauthorised personnel to view them. Computer screens near windows should not be positioned so they can be viewed from outside the building. Likewise computer screens in public areas should be angled so they can only be seen by staff members and not by members of the public. Staff members who work from home or from remote offices should be given guidance as to how they should position their computer so it is not viewable by unauthorised personnel. Similarly, employees who regularly work in public places such as hotels, coffees ships or public transport should be trained on how to place and use their computer equipment so it is not easily overlooked.

6. Summary

Visual data security is at risk whenever data is displayed on screen, whether that's in the office or elsewhere. It is clear that the continued growth in flexible working practices, including remote and mobile working, is making protecting sensitive data an increasing challenge that organisations must address. Tried and tested solutions are available as part of the security frameworks to protect electronic data while it is stored on remote devices and while it is being transmitted to and from those devices. However, the Achilles heel in these security frameworks is poor visual data security. The studies carried out to support this paper highlight that, while there is some awareness of the risks posed by poor visual data security there is still a lot that needs to be done to address those risks. Organisations need to review their overall security frameworks and ensure that visual data security forms an integral part of their security strategies.