clearswift

Clearswift Insider Threat Index (CITI)

US Edition

LOUDHOUSE

www.clearswift.com

Contents

Executive Summary

The threat to data security does not solely exist outside the borders of the organization. Today's modern and convoluted enterprises have become breeding grounds for internal data security breaches. Coca Cola's 2014 data breach, in which details of over 70,000 of its North American employees were leaked, act as a reminder of the threats which exist. Although security breaches are unlikely to be malicious in nature, the risk of accidental breaches present a credible risks to organizations. As critical information and sensitive data within the business continues to grow, managing the potential threats within is an important priority.

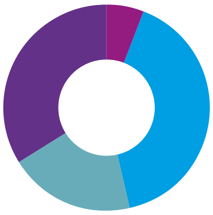
The Clearswift Insider Threat Index (CITI) is a global study which looks to explore and understand the changing nature of the insider threat to business. This particular report focuses on the research findings within the US. As with the CITI global study, the US research takes the views of both businesses and employees to provide a complete view of the insider threat and how it is being managed.

The findings show that the threat within is a growing problem for US firms, with a greater proportion of breaches originating *within* the extended enterprise. Businesses are yet to fully account for the security implications brought about by working trends, whether through remote working or employees using their own personal devices and applications for work purposes. With no real security structure in place and employees often ignorant of the consequences, it will only become a matter of time until a significant data breach occurs.

US employees are more data conscious than other regions, however more needs to be done to make them aware about the implications of a security breach. Increased ownership of data along with greater training and education will provide workforces with the foundation needed to create a safer working environment. With this, employees can fully utilise working trends while ensuring the security of the business.

Sample overview: Business

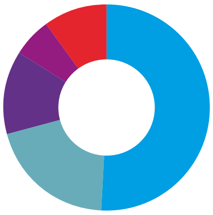
201 US decision makers responsible for Data Loss Prevention (DLP) strategy completed an online survey during January 2015

Sector	Sample Size	Company size
Government	40	
IT / telecoms	40	
Finance	37	
Manufacturing / engineering / construction	34	
Transport	18	
Pharmaceuticals	10	
Business services / media / publishing	9	
Utilities / energy	8	● 500 – 999 employees 6% ● 1,000 – 3,999 employees 41% ● 4,000 – 7,999 employees 20% ● 8,000 or more employees 34%)
Critical infrastructure	2	
Defence	1	
Other	2	
Total	**201**	

72% of businesses say they are more concerned about internal security threats than 12 months ago.

Sample overview: Employees

1,000 full or part time office workers across the US, who have access to and use either a desktop or laptop completed an online survey during December 2014

Sector	Sample Size	Company size
Manufacturing / engineering / construction	207	
Finance	151	
IT / telecoms	148	
Business services / media / publishing	140	
Local government	81	
Transport	60	
Pharmaceuticals	48	
Utilities / energy	38	● 2 – 499 employees 51%
Defence	18	● 500 – 999 employees 20%
Critical infrastructure	15	● 1,000 – 3,999 employees 13%)
Other	94	● 4,000 – 7,999 employees 56%)
Total	**1,000**	● 8,000 or more employees 10%)

Some of the key stats include:

92% of organizations have experienced a data breach in the last 12 months – of these, **40%** say they have seen growth in the number of internal breaches

The insider threat is real, it is growing and businesses are not taking it seriously enough

- 92% have experienced an IT or data security incident in the last 12 months
- 74% of breaches originate within the extended enterprise – either amongst employees (40%), third parties (22%) or ex-employees (12%) – with 26% originating outside the organization
- 72% are more concerned about internal security threats than 12 months ago
- 76% believe internal security threats are still not treated with the same level of importance as external threats by the Board
- Reputational damage (67%), financial penalties (62%) and reduced employee morale (42%) are the key risks associated with internal security threats

BYOD and cloud coupled with a lack of user awareness are seen as biggest reasons for an increased insider threat

- Two-thirds (67%) of internal security breaches originate from inadvertent error – one in three (33%) is due to malicious intent
- Increases in cloud apps outside the jurisdiction of IT (52%), a lack of awareness / understanding of data security threats (48%) and increases in viruses introduced via personal devices (37%) are the biggest reasons for internal security breaches increasing
- Removable storage devices (49%), users not following protocol (47%) and employees using non-authorised applications (40%) are seen as the biggest internal security threats

37% of employees have access to sensitive data at work that they think someone of their role or seniority shouldn't access

Businesses see one third of critical information being at risk and more than half of employees potentially likely to cause a data security breach

- 29% of critical information is seen at risk from an internal security breach
- Businesses believe around half (54%) of their workforce could cause an accidental internal security breach, with 5% potentially causing a malicious breach
- The 'enemy within' is seen as most likely to be a middle manager (33%) who works in the finance department (46%)

67% believe their business will experience a serious information breach in the next 24 months

Employees say they have access to data they shouldn't and while they recognise the risks associated with data breaches, still do things that leave sensitive data exposed

- 37% have access to sensitive data at work that they think someone of their role or seniority should not actually have access to
- Over a third (36%) believe it is their responsibility to keep company data safe and are personally concerned about causing a security breach
- Despite this, employees do things that leave sensitive data exposed such as sending emails to the wrong person (43%) or leaving their PC unlocked when not using it for an extended period of time (26%)
- 78% of employees think people who leak sensitive business data should be held to account / punished

The insider threat represents a ticking time-bomb for businesses and one that they are unprepared for

- 67% believe their business will experience a serious information breach in the next 24 months, resulting from employee behavior – 37% see this happening within 1 year
- 37% think it is difficult to pinpoint the exact source of internal data breaches in their organization – only 16% are able to spot unusual activity on their network immediately
- Educating employees on how to safeguard critical information (72%), making employees care more about the ramifications of a breach (57%) and increasing investment in Data Loss Prevention tools (50%) are the biggest priorities in minimizing the risk of internal security breaches.

Businesses must recognise that the nature of today's workforce has changed. Technology has allowed employees to become more flexible, intuitive, and ultimately, results-driven. While this cultural shift stands to benefit businesses and employees alike, it doesn't meet all their business objectives, namely data security and compliance. Companies must become more forward-thinking and proactive. Those who balance collaboration with security and processes stand a better chance of success in the years ahead.

> "Companies must become more forward-thinking and proactive. Those who balance collaboration with security and processes stand a better chance of success in the years ahead."

Research Methodology

Businesses: 201 decision makers responsible for Data Loss Prevention (DLP) strategy in organizations with 500+ employees across a range of sectors completed a survey during January 2015

Employees: 1,000 full or part time office workers across the US who have access to and use either a desktop or laptop completed a survey during January 2015.

The threat to data security is higher in the US than in other regions in the study. Over the last 12 months, **92%** of businesses experienced some form of data security breach, the highest seen within the Clearswift Insider Threat Index (CITI).

The growing insider threat

The threat to data security is higher in the US than in other regions in the study. Over the last 12 months, 92% of businesses experienced some form of data security breach, the highest seen within the Clearswift Insider Threat Index (CITI). However, while organizations may be quick to look at threats outside the business, in reality, the danger exists closer to home. On average, nearly three quarters (74%) of security of breaches originated within the extended enterprise, either among employees (40%), suppliers (22%) or ex-employees (12%). Just over one in four incidents (26%), on average, originated from outside the organization (*see Figure 1*).

Among those who have experienced a data breach, 40% reported an increase in the number of internal security breaches over the last 12 months, compared to just 17% experiencing a decrease (*see Figure 2*). The rise in internal security breaches has left many US businesses uncertain about the dangers which lie ahead. Nearly three-quarters (72%) are more concerned about internal security threats than a year ago. With new technologies becoming common place within businesses, the dangers within will only persist. Over seven in ten (71%) think social media has exacerbated the internal security threat.

Businesses can no longer afford to ignore the threats to critical information and sensitive data by employees. Greater education around the management and use of critical information and sensitive data is a critical first step in creating a safer working environment. However, as little as 22% believe their company does enough to make employees aware of how they should be protecting critical business information.

Reputational damage (67%), financial penalties (62%) and reduced employee morale (42%) are the key risks that businesses associate with internal security threats. However, as seen with other regions in the Clearswift Insider Threat Index (CITI), such risk is not recognised at Board-level. Over three-quarters (76%) believe that internal security threats are still not treated with the same level of importance as external threats by the Board.

Figure 1: Source of security threats in the last 12 months amongst those who have experienced a security breach

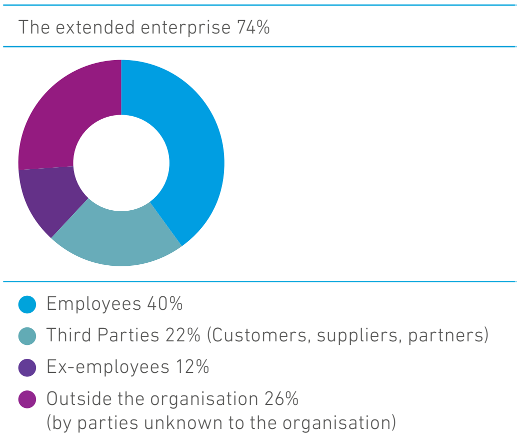
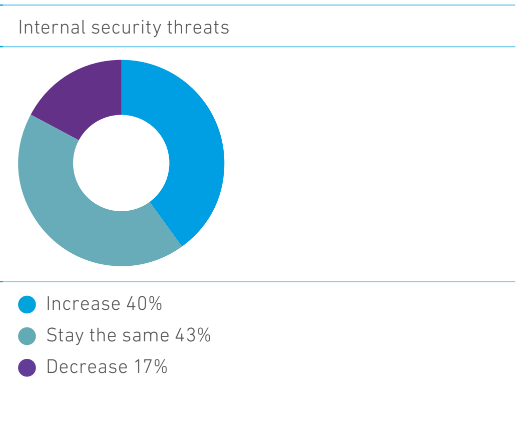


Figure 2: Growth in internal security threats in last 12 months amongst those who have experienced a security breach



Over half (52%) believe that the use of personal cloud applications, such as social collaboration tools, is the main reason for internal security threats increasing within their business.

Reasons for increasing insider threats

The blurring lines between personal and work-based technologies, although beneficial to both employees and employers, presents an immediate data security challenge. The availability of new devices and applications create an opportunity for workers to become more productive, but at the expense of data protection. Just under half (49%) of US businesses believe removable storage devices, such as USBs, is the biggest security threat to their organization (*see Figure 3*). Furthermore, users not following company protocol (47%) and employees using non-authorised applications for work purposes (40%) present a further threat for businesses.

With remote working a growing trend amongst many US businesses, internal security risks are likely to persist within organizations. Just under a third (31%) believe employees accessing company networks via their own mobile devices presents a significant threat to data protection.

IT departments are left with a lack of visibility around possible security threats, as workers become more and more reliant on their own technologies. Personally-owned technologies, often outside the jurisdiction of the IT department, have become accepted tools of the job. But more often than not they come without the relevant security measures. Over half (52%) believe that the use of personal cloud applications, such as social collaboration tools, is the main reason for internal security threats increasing within their business (*see Figure 4*). A lack of awareness and understanding around data security issues (48%) and an increase in viruses brought about by personal devices (37%) only further compounds the issue.

In an environment where devices and applications are left unchecked, inevitably both employees and businesses will become complacent. Although less reported and highlighted, the vast majority of data security incidents (67%) which have occurred are either inadvertent or accidental. Around a third (33%) are caused maliciously by someone within the enterprise. While businesses may be more restricted in the measurements they can take to protect against malicious security threats, they can take significant steps in reducing the number of breaches which arise inadvertently.

Figure 3: Biggest internal security threats to organizations

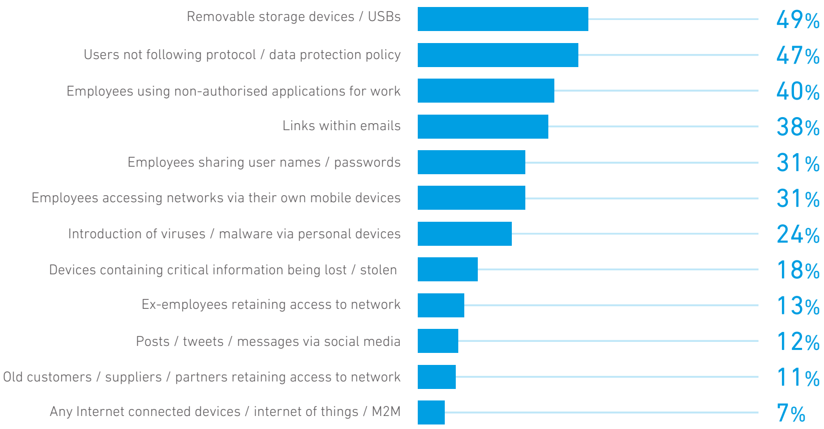
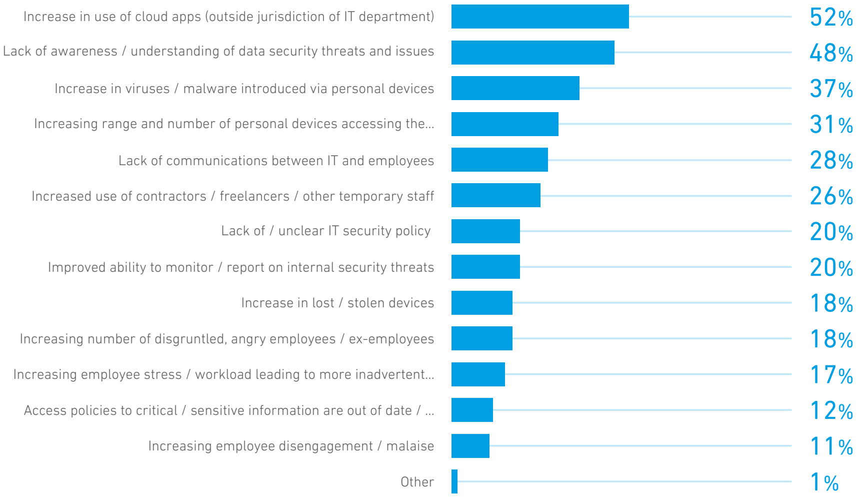


Figure 4: Reasons for increased insider threat to businesses



The pervasive insider threat

The insider threat exists across the whole organization. However, certain areas of the enterprise are more vulnerable than others. With higher volumes of sensitive data around company performance and profit and loss expectation, nearly three-quarters (74%) believe their critical information lies within the finance department (*see Figure 5*). HR (69%) and legal / compliance (65%) are also believed to be departments most likely to store sensitive data or critical information. However, as seen in the UK (19%), just 18% believe sensitive data resides within customer services. With large volumes of customer information housed here, businesses should give greater weight to its sensitivity.

Internal threats exist in many different shapes and sizes. However, identifying the business areas most likely to cause a breach, either maliciously or accidently, is vital. Businesses believe 29% of all critical company information could potentially be exposed by an internal security threat. In practice, over half of the US workforce (54%) is perceived as potentially able to cause an accidental internal security breach, with 5% potentially causing one maliciously. As such, no area of the organization is exempt from risk.

According to the Clearswift Insider Threat Index (CITI), the biggest internal threat among US workers are middle managers (33%) who work within finance (46%) and are located on-site (69%). While this helps paint a picture of the threat within, in reality the cause of security breaches can originate from any area of the organization. Certain departments may contain more sensitive data over others, but the truth remains that the insider threat exists throughout the business.

As seen globally within the Clearswift Insider Threat Index (CITI), accidental employee threats are seen to present the largest threat to all sorts of data, whether this be product / service data (45%), transactional data (45%) or employee data (44%) (*see Figure 6*). However, ex-employees present a notable threat to data. Over one in five (22%) believe ex-employees are the most likely group to pose a security threat through accessing employee data.

Figure 5: Departments where sensitive data is seen to reside

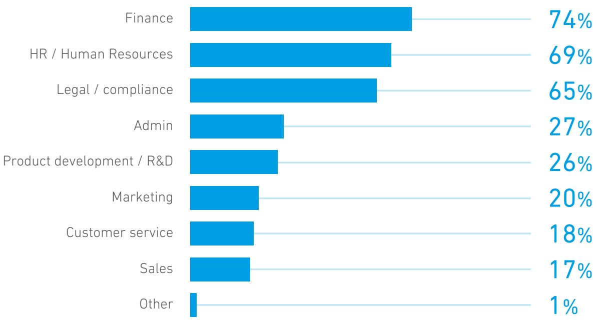
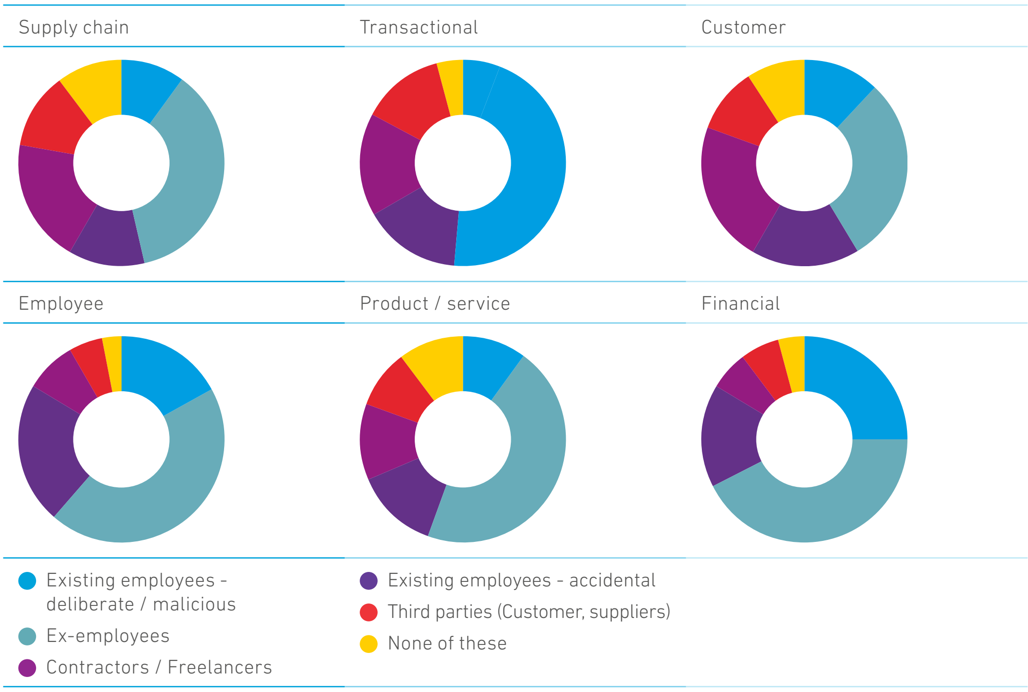


Figure 6: Most likely internal security threat by data type



Access all areas

US workers, similar to other workers within the Clearswift Insider Threat Index (CITI), have access to a diverse set of data. Customer (69%), financial (57%) and product (56%) data are the most likely types of data that employees have access to at work (*see Figure 7*). Nearly half (46%) have access to transactional data. Given the inadvertent threat which employees pose to the business when handling sensitive data, this is particularly alarming. Over a third (37%) have had access to critical information at work that they think someone of their role or seniority should not actually have access to.

However, employees recognise the risks involved. Workers believe that should financial (59%), customer (54%) or transactional data (51%) be compromised, it will likely cause considerable damage to their business. Indeed, as with other regions, US workers rank employee behavior resulting in the loss of sensitive data as the most serious offence to their employer. Such an act is considered more serious than putting in false expense claims, taking company goods without permission or taking unauthorized time off.

US employees are more security conscious than other regions in the study. Over a third (36%) believe it is their responsibility to keep company data safe and are personally concerned about causing a security breach, significantly higher than both British (23%) and Australian workers (27%). Loss of future business (66%), reputational damage (62%) and financial penalties (52%) are areas they believe their employers are most concerned about. Over half (52%) see litigation / legal action as a further concern, a concern which is notably high in the US compared to Germany (37%).

Despite US workers being more cautious than other regions, accidents and inadvertent errors still do occur. 43% have sent an email to the wrong recipient in the past, with over one in four (26%) leaving their computer unlocked when not using it for an extended period of time (*see Figure 8*). Employees also fall into bad habits and practice. A quarter of workers (25%) use the same passwords for applications both at work and at home.

Businesses feel employees are too apathetic to care about the implications of a security breach. 62% think employees don't care enough about the implications of a security breach to change their behaviour. However, in reality, the issues around data security must be prioritized more across the business, ensuring employees are held to account. Over eight in ten (84%) employees believe those who leak critical business information should be responsible for their actions.

Figure 7: Types of data that employees have access to

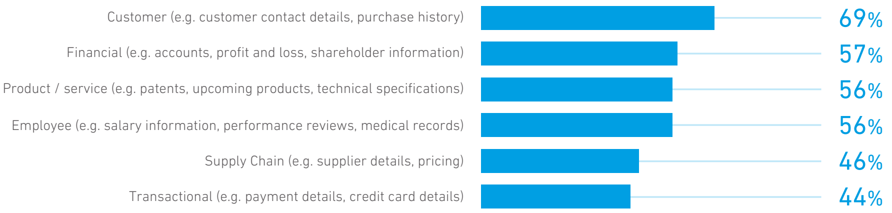
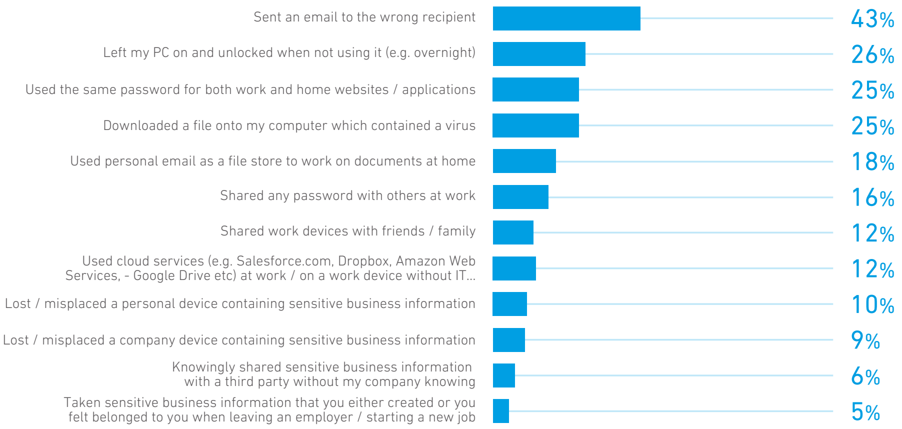


Figure 8: Employee behaviours with sensitive data



Time is of the essence for US businesses. Organizations will ultimately suffer sooner than they think if insecure internal practices and processes are left unaddressed.

The imminent insider threat

US businesses are no different to other regions in their ability to spot and deal with internal breaches. 37% believe it is difficult to pinpoint the exact source of internal data breaches in their organization. Due to the dynamic, interconnected and intricate nature on the modern enterprise, knowing where and when the next breach will occur is difficult. Indeed, many breaches may even go unnoticed. Just 16% of organizations say they are able to spot unusual or suspicious activity on their network immediately.

Failure to prepare and defend against the rise in internal threats is likely to spell trouble for many businesses. Over two-thirds (67%) believe their business will experience a serious information breach resulting from employee behavior in the next 24 months (*see Figure 9*). Critically nearly four in ten (37%) see this happening within the next 12 months. Time is of the essence for US businesses. Organizations will ultimately suffer sooner than they think if insecure internal practices and processes are left unaddressed.

The key challenge, however, is ensuring businesses benefit from the new working practices brought about by technologies while upholding data security. Nearly three-quarters (73%) think it is difficult to balance employee privacy and organizational control when it comes to data security, much higher than in the UK (61%).

Education, training and transparency are key to managing the insider threat. Employees are primarily concerned with getting the job done, regardless of what tools and applications they use. A reactive policy of blocking technologies is likely to prove futile as users will inevitably find a work-around. Educating employees about how to safeguard critical information (72%), making employees care more about the ramifications of a breach (57%) and increasing investment in Data Loss Prevention (DLP) tools (50%) are the biggest priorities needed to minimize the risk of internal security breaches (*see Figure 10*).

Figure 9: Time left until critical information security breach

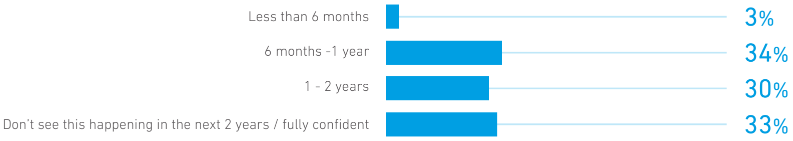
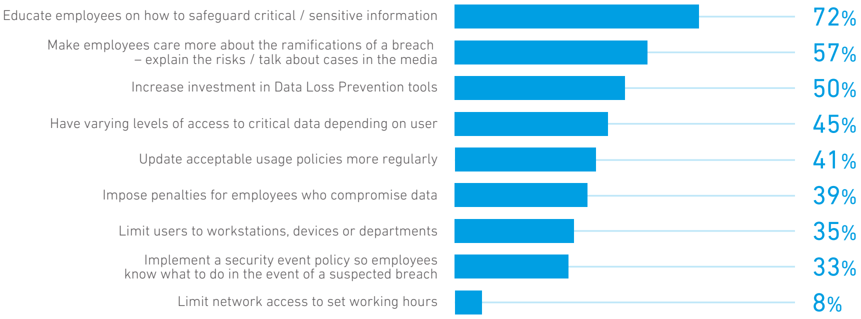


Figure 10: Actions needed to minimise internal threats



"Nearly three-quarters (73%) think it is difficult to balance employee privacy and organizational control when it comes to data security."

Conclusion

The US typifies the rise in internal threats seen across global businesses. While many may associate an internal 'threat' as malicious intent to steal or sell data, in reality, often such a threat is borne from inadvertent and human error. The dynamic of the US workforce has changed significantly in recent years. Personal technologies and applications have enabled employees to become more flexible and productive. However, without full visibility of the devices, applications and practices used, businesses are leaving themselves vulnerable to a significant data security breach.

Controlling and managing these new working trends must be driven from the top of the business if it is to be a success. However, perceptions around security threats must change first. For those at Board level, the greatest threat to security is still seen to reside outside the business, despite the majority of breaches originating from within the extended enterprise. Without the key issues around internal security being prioritized at the top of the business, ultimately the problem perpetuates.

US employees, in particular, are data conscious and aware of the implications to data security should sensitive data be compromised or otherwise mismanaged. However workers, driven by their desire to get the job done productively, often sacrifice data security in the process. Whether accessing the network with an unregistered device or using their own cloud application at work, data security is often an afterthought.

In order to control the rise in internal security incidents, US employees need to become accountable for their actions. Greater education around the importance and implications of internal breaches, in conjunction with improved data protection tools, is a critical first step. By taking responsibility, both employees and companies will benefit from new working trends safely and securely.

"Workers, driven by their desire to get the job done productively, often sacrifice data security in the process. Whether accessing the network with an unregistered device or using their own cloud application at work, data security is often an after thought."

clearswift

Clearswift is trusted by organizations globally to protect their critical information, giving them the freedom to securely collaborate and drive business growth. Our unique technology is specifically designed to mitigate the insider threat today, and tomorrow. We offer a straightforward and free health-check to organizations who are concerned about the insider threat vulnerability. To take advantage of this or to speak with Clearswift about how an adaptive data loss prevention approach may benefit your business, contact us today on **www.clearswift.com/contact-us** or email **CITI@clearswift.com.**

United Kingdom
Clearswift Ltd
1310 Waterside
Arlington Business Park
Theale
Reading, RG7 4SA
UK

Germany
Business Excellence
IM Mediapark 8
50670, Koeln
GERMANY

United States
Clearswift Corporation
309 Fellowship Road
Suite 200
Mount Laurel, NJ 08054
UNITED STATES

Japan
Clearswift K.K
Shinjuku Park Tower N30th Floor
3-7-1 Nishi-Shinjuku
Tokyo 163-1030
JAPAN

Australia
Clearswift (Asia/Pacific) Pty Ltd
Level 17
40 Mount Street
North Sydney
New South Wales, 2060
AUSTRALIA

www.clearswift.com