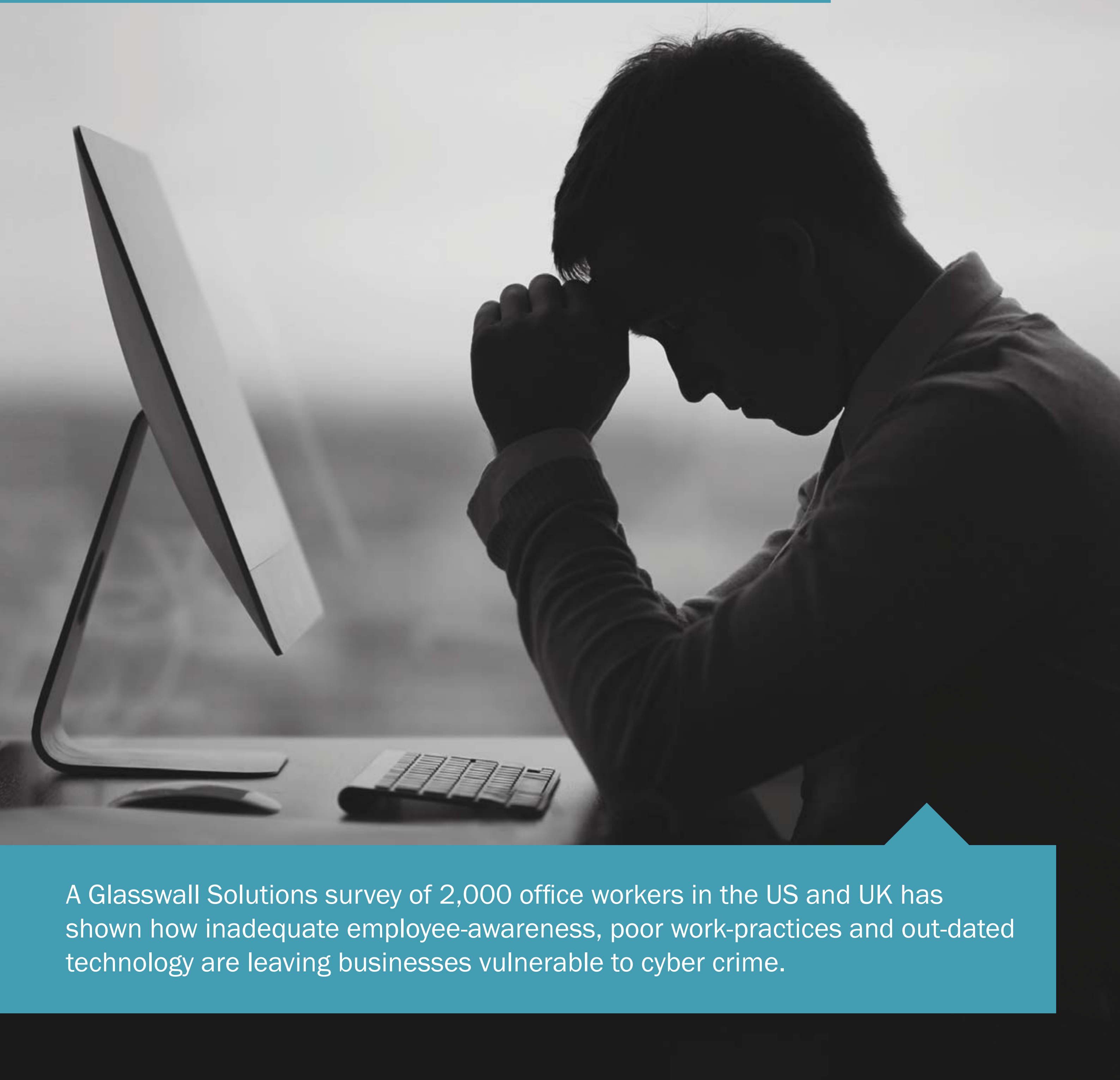
GLASSWALL
TRUST EVERY FILE

Your employees won't protect you

Why businesses need an innovation injection to stay safe from cyber threats



A Glasswall Solutions survey of 2,000 office workers in the US and UK has shown how inadequate employee-awareness, poor work-practices and out-dated technology are leaving businesses vulnerable to cyber crime.

Introduction

“As the scale of cyber attacks on major businesses steadily increases, significant new research by Glasswall Solutions across the US and UK reveals findings that anyone at board level must heed: office-workers cannot be relied on to protect the businesses they work for. A combination of inadequate threat-awareness, poor work-practices and out-of-date technology is leaving even the most dynamic businesses wide open to the increasingly sophisticated attacks devised by cyber criminals.

This white paper will reveal how a flammable mixture of complacency and ignorance now threatens to destroy many businesses. Employees are only vaguely aware of cyber-threats and not confident their organisation knows how to tackle them.

Surveying a thousand office-workers employed by medium-to-large businesses in each country, the research demonstrates how lax approaches to the huge dangers in the main threat-vector – email attachments – are exposing organisations to hacking, ransomware and zero-day attacks.”

Greg

Greg Sim
CEO
Glasswall Solutions

GLASSWALL™
TRUST EVERY FILE

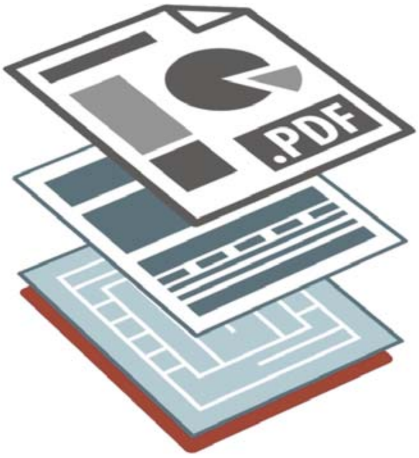
The threat from attachments

Attached to what seems a legitimate email, everyday file-types such as Word, Excel, PDF or PowerPoint are now used in 94 per cent of cyber attacks.

Laden with malicious code that is cleverly hidden in either the content or the structure of the file itself, a simple click is all it takes to give hackers access to a business's data, systems, assets and intellectual property.

Once activated, the code, which is unrecognisable to conventional anti-virus or sandboxing solutions, will trigger a malware download that can immediately steal a business's most critical data, or hold it to ransom. Alternatively, a zero-day exploit can scuttle through a business's network and hide away undetected, ready to detonate at a time of the criminal's choosing.

This Glasswall Solutions research helps explain why organisations are so vulnerable to these attacks, examining the threats from the employee's perspective as well as exploring how businesses are approaching this growing menace. It reveals how staff feel they are not being given the right tools to help them protect the organisations they work for, and how they also have inadequate understanding of how a few simple clicks on an innocent-looking email attachment can lead to disaster.

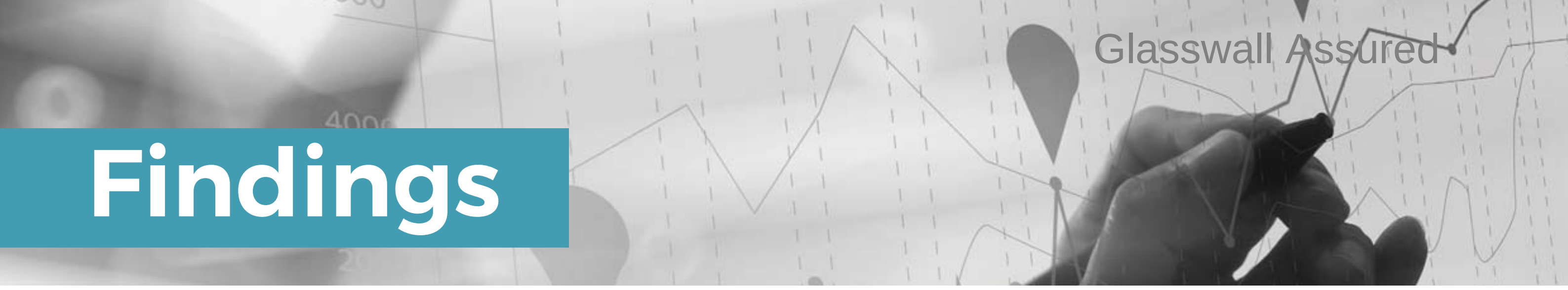


The scale of cyber crime

The scale of the problem now faced by businesses of every size should not be underestimated. Last year, for example, UK government research found that two-thirds of major businesses in the country had been hit by a cyber-attack over the previous 12 months. Its Cyber Security Breaches Survey revealed that most of the attacks involved viruses, spyware or malware and that a quarter of large firms experiencing a cyber breach did so at least once a month, with some attacks costing millions of pounds.

The US Department of Justice estimates that ransomware attacks alone quadrupled to 4,000 per day between 2015 and 2016. Repeating the same warnings, the UK's National Cyber Security Centre (NCSC), has said the first half of 2016 saw an almost threefold increase in ransomware variants compared with the whole of 2015. In the three months after the NCSC was created last year, the UK was subject to 188 "high-level" attacks sufficiently serious to warrant the agency's involvement. Its report on the threats to UK business says attacks around the world in 2016/2017 have been bolder than ever.

The impact is severe. The average annual cost of cyber-attacks to companies worldwide is pegged at more than $9.5 million by the Ponemon Institute, with the damage to reputations for efficiency and security incalculable.



Findings

Where traditional email security falls down

In too many businesses, there is a low level of awareness among office employees of the scale of cyber crime and the threats their employer faces. Only a third (33 per cent) of US and UK office-workers surveyed, for example, thought the business employing them had been a victim of a cyber attack, despite thousands of attacks being launched every year against businesses. Almost a quarter (24 per cent) simply did not know if the business they work for had been attacked.

Superficially however, there is far greater comfort to be had from the 75 per cent who recognise that they receive email attachments which are suspicious. Yet despite the awareness that potentially dangerous emails are in circulation, far too many office-workers are willing to click open the attachments that come with them – even when the sender is completely unknown.

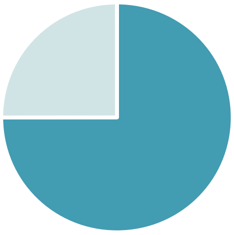
62 per cent of those surveyed admitted they do not usually check the legitimacy of email attachments that come from unknown sources. A dangerous minority of 15 per cent said they always or usually trust email attachments sent by people they have never even heard of. Between them, these groups of employees are liable to open up any organisation, offering a virtual welcome mat to hackers.

When the survey questions turned to emails from known contacts, the picture is also similarly worrying. Asked what they do with emails from colleagues, suppliers or customers, 83 per cent of UK and US employees said they always or usually open attachments that accompany them.

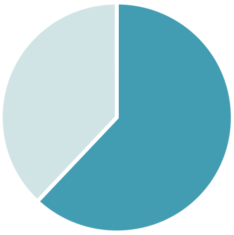
It may be entirely natural for employees to open attachments from what appear to be their colleagues or friends, but with social engineering and the use of phishing emails having grown exponentially, this is no longer an acceptable practice. Criminals now routinely create emails that look as if they have come from someone the recipient knows, using information that can include data sourced from social media, business website and directories, or metadata stripped out of unprotected company documents that give away email addresses or other internal details.

The readiness of employees to click open files without examining their authenticity creates a worrying state of affairs for any business. How can it rely on its employees to spot threats and respond to them in a way that eliminates the risks?

Only 30% of office-workers believe their employer has been subjected to cyber attack



75% receive suspicious emails



62% don't check email attachments from unknown sources

Everyday kinds of attachments

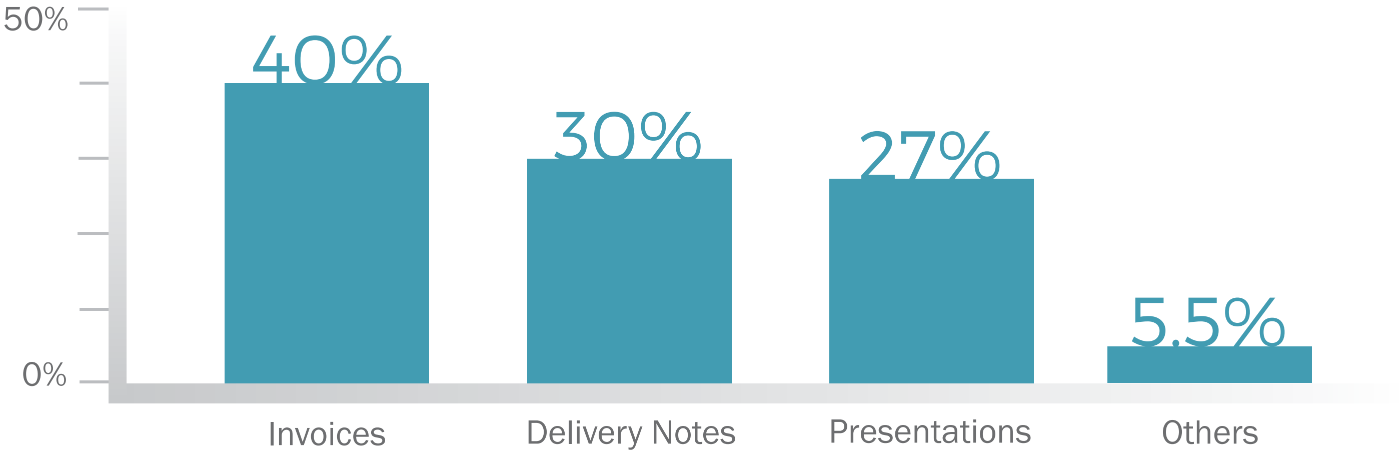
To gain some sense of what triggers an employee’s suspicions, the survey also asked office-workers to identify the most common types of suspicious email attachments they receive. In each country, invoices were selected as being the most suspicious attachment from a list that included delivery notes and order forms.

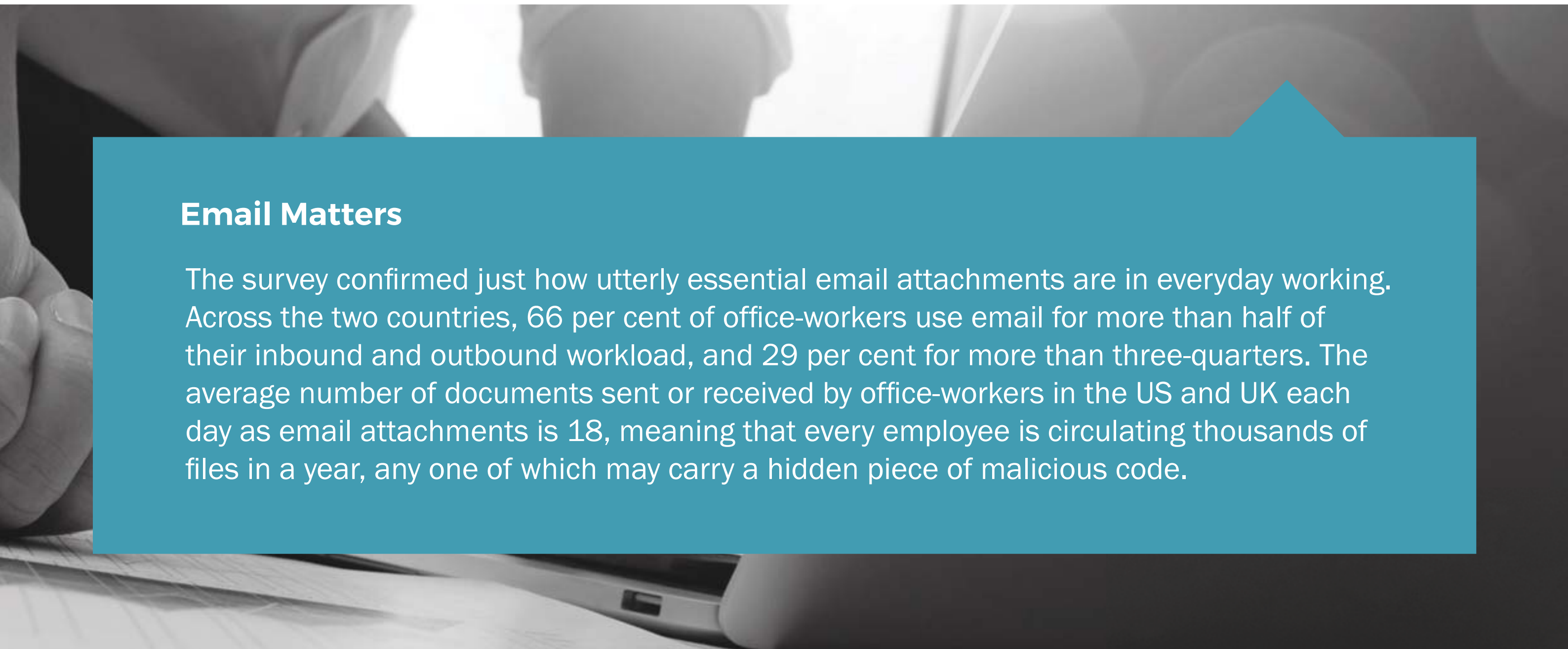
Only a tiny percentage (5.5%) thought “other” types of attachments were suspicious. Asked to name them, respondents identified various types of ploy such as prize-winning links or emails with multiple addressees. Yet only two people named Word documents as being suspicious and only two said they regarded “spreadsheets” as a potential threat, despite the continuing prevalence of these file-types in the perpetration of successful cyber-attacks.

The choice of invoices as the most commonly received suspicious attachment is likely to reflect the justifiable belief that pro forma documents of this type, bearing little personal information and likely to be carrying macros, are among the easiest to subvert for criminal purposes.

In the UK, however, the proportion viewing invoices as the most threatening from the list of attachments was higher (46 per cent) than in the US (34 per cent). Among the other options, delivery notes were viewed with greatest suspicion by a third of respondents in the US (33 per cent) compared with 26 per cent in the UK.

The most common types of suspicious email attachments received in the UK and US





Email Matters

The survey confirmed just how utterly essential email attachments are in everyday working. Across the two countries, 66 per cent of office-workers use email for more than half of their inbound and outbound workload, and 29 per cent for more than three-quarters. The average number of documents sent or received by office-workers in the US and UK each day as email attachments is 18, meaning that every employee is circulating thousands of files in a year, any one of which may carry a hidden piece of malicious code.

Have I clicked on something I shouldn't have?

Even though employees say they are aware of the dangers in emails, the results exposed how a poor understanding of the dangers in attachments remains a significant vulnerability for businesses. 71 per cent of respondents said they had never opened up an attachment that turned out to be corrupt, or did not know if they had, despite the increasingly vast number of weaponised attachments now in circulation.

What should I do?

The circulation of information about potential threats is vital to the protection of any organisation or business. Yet not only do employees have to recognise what might be a danger, they have to communicate their concerns so that the business can respond in time.

At first sight it appears encouraging that the majority of office-workers in the survey said that once they have clicked open a suspicious attachment, they will always report the fact, with similar percentages across each country (an average of 77 per cent). A sense of duty was the primary reason given (78 per cent), with 79 per cent across both countries saying they would report suspicious cyber-activity to their IT team.

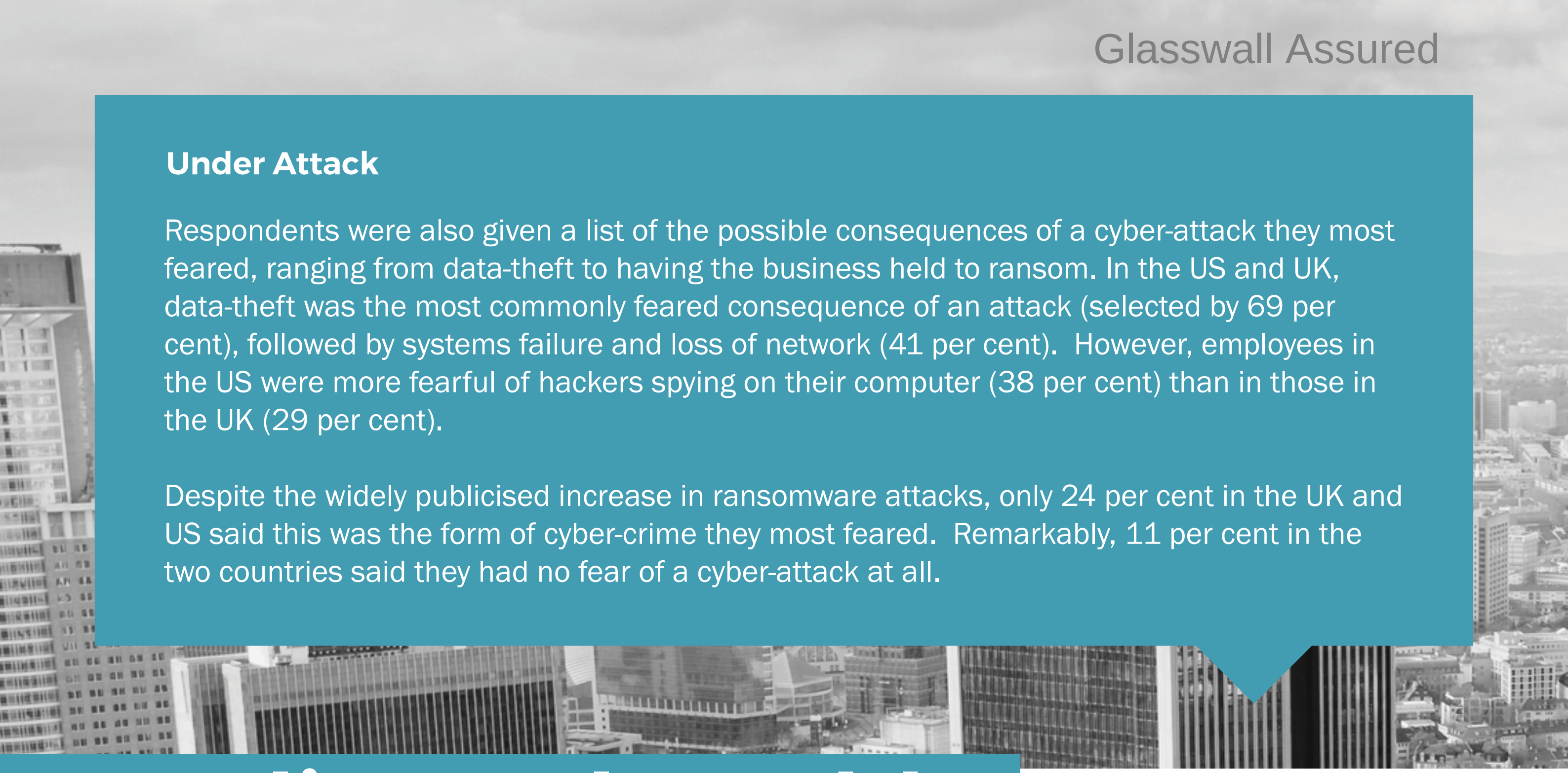
Nonetheless, in each country barely more than a third said the reason they would inform someone in their company was because it has a policy in place about such eventualities (36% in the UK and 38% in the US). When it comes to reporting potential security threats it seems the majority of businesses rely on the good nature of their employees.

Differences emerged, however, between the two countries in terms of the attitudes of employees. 51 per cent of US employees said they would not report having opened an email attachment that was corrupt because they do not regard it as important, whereas in the UK the corresponding figure was only 35 per cent. 25 per cent in the US said they would avoid reporting because they would be worried that to do so would jeopardise their job, compared with 32 per cent in the UK.

Most worryingly, a significant minority of 16 per cent think that cyber attacks are not their concern.

16% think cyber attacks not their concern

The lesson from this is that while slightly more than three-quarters of employees will report something they have done that may have compromised security, more than one-in-five will not. It may appear reassuring that the majority of employees have a sense of duty, but this will not be sufficient to protect a business from sophisticated cyber-attacks.



Under Attack

Respondents were also given a list of the possible consequences of a cyber-attack they most feared, ranging from data-theft to having the business held to ransom. In the US and UK, data-theft was the most commonly feared consequence of an attack (selected by 69 per cent), followed by systems failure and loss of network (41 per cent). However, employees in the US were more fearful of hackers spying on their computer (38 per cent) than in those in the UK (29 per cent).

Despite the widely publicised increase in ransomware attacks, only 24 per cent in the UK and US said this was the form of cyber-crime they most feared. Remarkably, 11 per cent in the two countries said they had no fear of a cyber-attack at all.

Feeling vulnerable at work

Among the more worrying findings were those related to employee vulnerability, with office-workers feeling their supervisors do too little to protect them. While 38 per cent said they feel vulnerable because cyber attacks are on the increase, 18 per cent do not feel their employer has installed adequate protection or offered them the right kind of guidance. Another 15 per cent admitted they feel vulnerable because they do not know what threats look like.

Some 16 per cent, however, said they are more aware of the dangers because of previous experience, believing that as a result they have been targeted before, they are likely to be targeted again.

Taking the pressure off employees with technology

With cyber attacks constantly in the headlines, the survey asked office-workers what their employer could do to make them feel safer. The most popular option was ensuring the right technology is available, with more employees in the US regarding this as a priority (64 per cent) than in the UK (58 per cent).

64% in US want the right technology to protect them

Cyber security training was selected by 52 per cent as the next most popular choice, followed by the provision of handbooks on the subject (33%). As much as office employees may feel a personal sense of responsibility and want their organisations to do more to enhance cyber security, they realise that in a medium-to-large-sized business, technology will be the most effective solution.

Faith in the boss

If employees are going to feel protected, they need to feel the top team knows what it is doing about cyber security. Unfortunately, the results show that many staff have little faith in the steps their senior executives are taking. In the US, 24 per cent of those polled either believe their company leaders have no understanding of cyber-risks or they just don't know whether they are understood at senor level. In the UK the figure was even higher – 34 per cent.

Conclusion

The danger of sticking with old approaches

This Glasswall Solutions research shows that employees are worried about cyber security. The border and endpoint security solutions currently deployed by their employers including anti-virus, firewalls and even sandbox technology are failing to dispel their fear of opening an attachment in the pursuit of just doing their job.

For many of these employees, sending and receiving emails is one of the most common activities at work. Asking them to double-check every attachment is not a realistic prospect, since not only would it require a significant change in behaviour it would also risk a huge slowdown in productivity.

The survey findings paint a picture of inconsistency. While many office-workers are aware that emails can contain severe security threats, they may not be aware of the exact way in which they can help prevent them succeeding. It is also apparent that substantial proportions of employees at the medium-to-large businesses are too accustomed to poor practices with new rules or fresh guidance having little effect.

In the face of ever-more devious, numerous and sophisticated cyber attacks, the only approach that will work is one of innovation. This means using a solution that stops all threats at the door before they enter a network. To achieve that requires advanced file-regeneration technology that will conduct deep inspection of email file attachments by comparing them to the manufacturer's standard at the byte-level.

Within fractions of a second of the process starting, Word, Excel, PDF and PowerPoint files are regenerated as sanitised documents, free of any malicious code, malware or subtle tinkering with the structure that will act as a trigger to a cyber attack as soon as the attachment is opened.

Once businesses have this technology in place, those agonising, split-second decisions about whether to open an attachment are taken out of the hands of the office-worker, who is free to conduct their day-to-day business without fear of infecting their employer's entire system or instigating a devastating zero-day or ransomware attack.

Not only is the burden lifted from the shoulders of the employee, but the business itself is set free to decide on the level of risk it is prepared to accept in relation to each file-type and how they should be used by departments or individuals.

It is an innovative and unique technology-based solution that takes the burden of protection off employees by keeping hackers and criminals outside the door.

GLASSWALL™
TRUST EVERY FILE

CONTACT US FOR A FREE TRIAL

☎ UK: +44 (0) 203 814 3900
USA: +1 (866) 823 6652

info@glasswallsolutions.com
www.glasswallsolutions.com

in Glasswall Solutions limited

@glasswallnews