CYBER SECURITY THREATS ON THE RISE

Resolving Perception & Reality

Whitepaper

TalkTalk Business

JUNIPER RESEARCH

Contents

Executive Summary

- Juniper Research analysed trends from a Vanson Bourne survey of 200 UK businesses of varying sizes about their experience of and attitude to cyber security and cyber attacks.

'No UK business is safe'

- 74% of UK businesses think they are currently secure.
- Yet the research shows that 50% of respondents have been attacked, including 45% of SME respondents and 55% of larger enterprises.
- 'Are we safe?' is the wrong question – rather, ask 'what risks are being taken and how they can be minimised?'
- **Recommendations**
    - Have a plan in place but don't assume you are secure because of it. Staff need to know what to do in the event of a breach, and must be aware of what risks they are taking at work.
    - Put the plan into practice – while 87% of businesses have a plan in place, only 27% conduct penetration tests and only 26% hold regular training and roleplay sessions. Without regular reinforcement and testing, guidelines and plans may be focused on securing the wrong area of business, meaning successful attacks do more damage than necessary.
    - Regularly review policies to ensure that they are robust enough to deal with threats when they arise, as well as accounting for any changes in IT infrastructure or company practices. Integrating new systems into a secure framework is a vital part of this process to ensure that business expansion does not increase vulerabilities.

'Cyber security Is not just for IT'

- Cyber security is still being pigeonholed as an IT problem - 70% consider the IT department responsible for handling security threats, while almost two-thirds believe cyber security is not their department's responsibility.
- However, most respondents report engaging in a range of insecure practices.
- **Recommendations**
    - Ensure that all employees are made aware of the fact that security is an enterprise-wide issue. Employees need to know what they and their departments can do to minimise risks.
    - Provide regular training across the business to ensure employees and departments are aware of their responsibilities.
    - Train new inductees thoroughly in company cyber security procedures. With few standard cyber security practices throughout the business world, new starters' lack of knowledge or old habits may increase vulnerabilities or an inadequate response to a cyber attack.
    - Cyber security management must be led from the top. CxOs and board members need to be aware of cyber security issues and be able to plan for and respond to cyber attacks.

1.1 Introduction

Cyber security is a big concern for businesses of all sizes, one which can cost them millions of pounds in lost data, lost time and lost customers. As more and more business infrastructure moves online, so do those wishing to destroy or defraud that infrastructure. But are companies doing the right things to prevent cyber attacks and/or mitigate their effects?

Attacks may come in a number of forms, including:

- Denial of Service – an attack that causes loss of services to users, typically the loss of network connectivity, by consuming bandwidth of the victim network or overloading the computational resources of the victim's system.
- Network spoofing – which involves an attacker setting up a rogue network access point using Wi-Fi or GSM, then inviting users to connect to the network. This enables the attacker to intercept and leak sensitive information and carry out further attacks.
- Ransomware – where malicious software encrypts data on the network, after which its creators demand a ransom to decrypt the affected files.
- Hacking– where cyber criminals exploit a vulnerability within the network to gain access to personal and/or corporate data, including financial information.

At the very least, a data breach has the potential to cause considerable inconvenience, as employees and/or customers may need to change passwords and (if financial details have been exposed) card details; at worst, it can lead to significant churn away from a particular company, together with possible remuneration requirements and regulatory fines.

According to Gemalto's Breach Level Index, more than 3.6 billion data records have been compromised in publicly confirmed data breaches worldwide since 2013.

Furthermore, a number of well-publicised data breaches at leading online sites has exacerbated both public and industry concerns. While the most high-profile data breaches will be those impacting larger enterprises, all enterprises are susceptible. The impact on smaller players can be even more devastating, given that the average cost of a significant data breach is over £65,000.[i]

In addition, there is a growing body of evidence to suggest that smaller enterprises are becoming more attractive to cyber criminals, with a rise in the scale of malware attacks.

The costs can come from a variety of sources:

- Theft of financial information – a company's bank details, and/or those of its employees and customers may be stolen, with the potential for funds within the exposed accounts to be stolen in turn.
- Internal disruption - if a company's website and/or systems are brought down by a cyber attack, its ability to sell, promote and possibly manufacture its products is likely to be severely constrained or curtailed until the site is secured, which may take several working days.
- Loss of trust – if data is exposed and customers suffer as a result, then affected companies may well receive a backlash in the form of other existing customers (and potential customers) becoming concerned for

the safety of their own data and migrating to an alternative service provider. There may also be an additional negative impact in that brand value may be adversely affected.

- Financial penalty – if personal data is compromised, the company may be liable to fines from a regulator and/or legal action from affected parties.
- IT costs – the costs of emergency IT work, to clean up affected areas in the company's systems.

No company can be 100% secure. It is critical for all businesses, whatever their size, to ensure that they not only have solutions in place to minimise the risk of successful cyber attacks, but also plans to address breaches if or when they occur. Furthermore, it is crucial that all employees are made aware of these plans and of the actions they need to take both to minimise a company's susceptibility to an attack and, in the event of a breach, to reduce the scale of its impact.

This report reveals that, despite increased concern and spend on cyber security over the last year, there is a high degree of complacency in regard to cyber security and few common practices in response to this threat. This will lead to continued confusion about how to prevent and contain the threat posed by cyber attacks.

1.1.1 Methodology Overview

Fieldwork was conducted by Vanson Bourne between 10th and 17th June 2016, surveying 200 UK businesses of varying sizes about their experience of and attitude to cyber security and cyber attacks. The survey was distributed via an online platform and was weighted by organisation size to reflect the business makeup of the UK. In total, 100 respondents were from businesses with 250 or less employees and 100 were from businesses with over 250 employees.

1.2 Key Findings

1.2.1 Cyber Security is an Increasing Problem for All Businesses

50% of respondents reported that they had been the victim of a cyber attack, showing that businesses are equally likely to be attacked regardless of size. Of these attacks, 29% resulted in a data breach. Two-thirds of reported attacks happened within the past year.

1.2.2 Businesses Think They are Secure, but Probably Aren't

In spite of the high incidence of cyber attacks, almost three-quarters (74%) of companies feel that they are currently secure when it comes to digital threats, despite half of those companies reporting having experienced a cyber attack. In addition, 86% of respondents think they are doing enough to mitigate the impact of cyber security attacks, including over 50% of companies who have knowingly suffered a data breach.

A significant minority (27%) of SMEs (Small and Medium Enterprises) believed that they were secure because they were 'too small' to be of interest to cyber attackers, while 56% felt they were secure because they 'have the right policies in place'. These beliefs have little basis in reality, with 59% of those expressing the former view and 53% of those expressing the latter having already experienced attacks.

1.2.3 Lots of Effort is Going into Cyber Security, but is it in the Right Place?

Many management teams are concerned about cyber security and the respondents in more senior posts are more likely to be concerned. This in turn means that more money is being spent on cyber security. However, those businesses where cyber attacks could have the biggest impact are also the least worried about it and therefore less likely to increase spend on the matter.

1.2.4 Cyber Security is a Matter for Everyone, not Just the IT Department!

Most respondents still think it's enough to have the IT or security department involved in mitigating the effect of cyber attacks. 70% consider the IT department responsible for handling security threats and almost two-thirds believe that it is not their department's responsibility. Despite this, many respondents engage in insecure practices, possibly with the consent of management.

However, cyber security is not a matter to be addressed purely by siloed IT departments, but for the entire business. It is critical that IT engineers talk to the rest of the business and vice versa. Inter and intra-departmental communication is essential.

Only by making all employees aware of the nature and scale of potential risks, the steps that need to be taken to reduce them and of the procedures to follow in the event of a breach, can a company truly develop a secure ethos.

1.2.5 There's Confusion About Data Breaches Before They've Even Happened

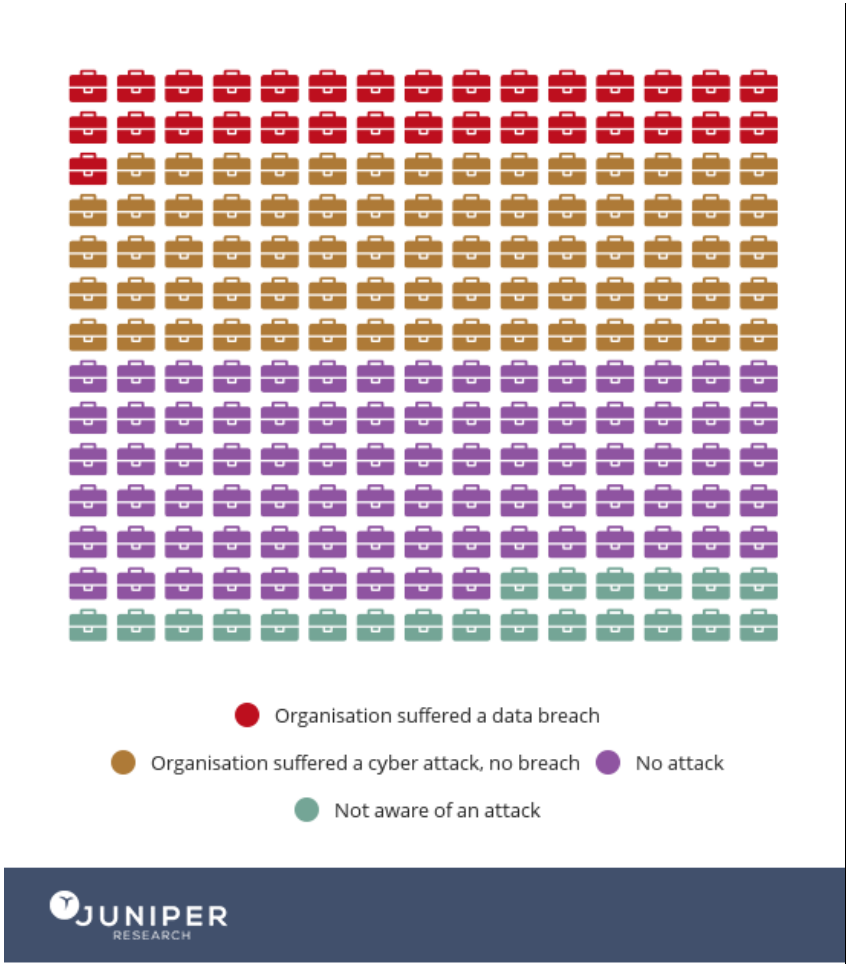
Respondents reported a range of measures in place to be actioned in the event of a data breach, but few reinforce it with regular training, if there is training at all. This means that responses to cyber attacks, unless seen by a relevant person from the start of the incident, are unlikely to be dealt with consistently.

1.3 The Scale of the Cyber Security Problem

1.3.1 It is Widespread

Half of all businesses surveyed claimed to have been the victim of a cyber attack, over a quarter of which resulted in a data breach.

Figure 1: Cyber Attack Incidence



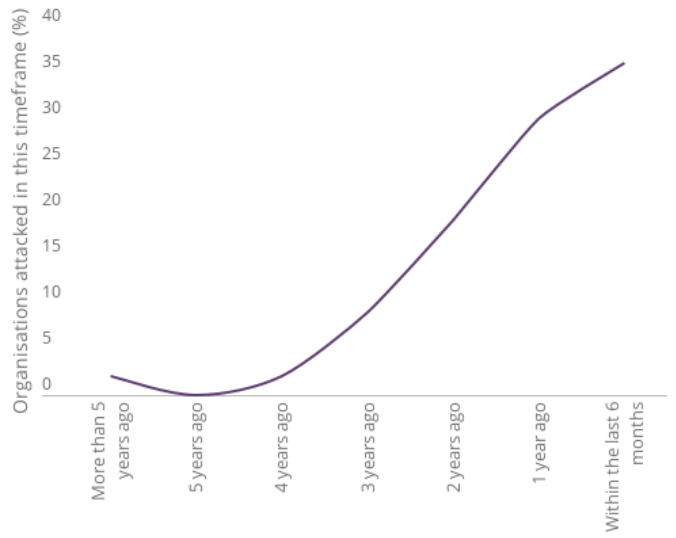
- As this figure relies on awareness of an attack taking place, actual incidents of attacks could be much higher. For example, a recent survey by Ipsos Mori claims that 65% of larger businesses have experienced a cyber attack in the past year.[ii]
    - This lack of awareness in effect makes negative assertions of cyber attacks worthless, as breach detection cannot be totally accurate. As over 40% of respondents assert that they have not been breached, this highlights the lack of awareness of the nature of cyber security detection and prevention.
- Attacks on SMEs (businesses with 250 or less employees) are more likely to result in a data breach.[iii] This is generally because SMEs do not have the resources to dedicate to cyber security, resulting in less measures being taken to prevent or mitigate cyber security threats.
- SMEs are also significantly less likely than larger businesses to consider cyber security a problem.[iv] However, attacks on smaller businesses can be a bigger problem due to the costs having a bigger relative impact on their bottom line; on average, the cost of a data breach costs over 19% of an SME's revenue.
    - More than a quarter of SMEs think that their size makes them an unattractive target, but both small and large businesses are equally likely to be attacked.[v]
    - Respondents from SMEs are significantly less likely than larger businesses to consider that they are not taking any risks with regard to cyber security threats across both devices and work processes,[vi] implying that they are less aware of which work practices are potentially insecure.

Figure 2: Do Businesses Think They Are Secure?

1.3.2 It is Increasing…

Attacks on businesses have been increasing exponentially for the last 4 years, with over a third of reported attacks happening in the past 6 months. This increase is potentially due to higher levels of concern around cyber security, which is driving up awareness of cyber attacks when they happen.

Figure 3: Cyber Attack Timescale



- This is particularly the case for larger businesses, which are significantly more likely to have suffered a cyber attack within the last 2 years than SMEs.[vii]

1.3.3 …and Getting More Attention

Half of C-level executives and board members are more concerned about cyber security than they were this time last year, but it seems most businesses need a wake-up call to address that concern. The majority of the businesses increasing spend are those that have already suffered an attack.

Figure 4: Who is Increasing Cyber Security Spend?

- Those increasing cyber security spend showed significantly higher concerns about business reputation and penalties from regulators than those who either maintained current spend or decreased it.[viii] Other concerns, including loss of data or service, are broadly similar across groups, regardless of levels of spend.
- The highest level of concern across all respondents was regarding loss of data, but this does not by itself appear to motivate higher levels of spend on cyber security.
- Waiting until it happens to increase spend is not an option for many businesses, who may suffer irreparable damage to their reputation and customer base from a single incident.
- Over three-quarters of businesses have a board that is involved in assessing cyber security preparedness, but only a quarter have a dedicated security executive.
- This means that they are likely to not be as aware of the nature and extent of cyber security problems, leading to gaps in knowledge and in business practices.

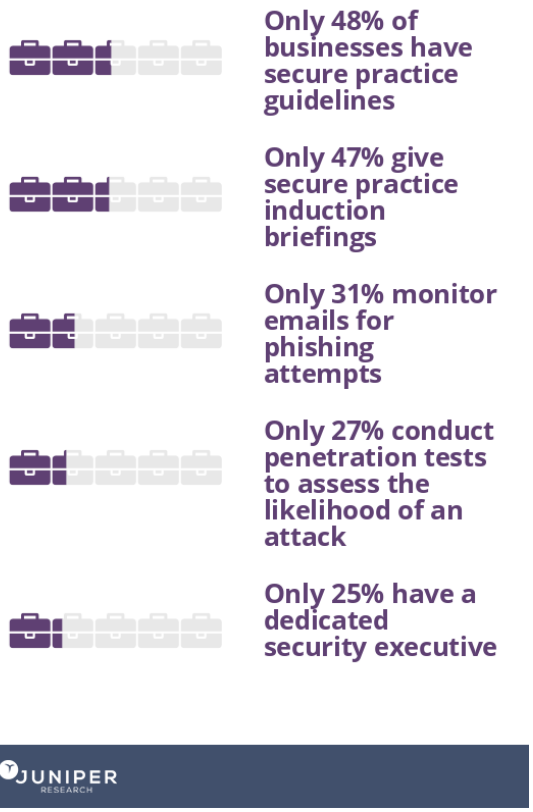
1.4 Current State of Cyber Security Planning

1.4.1 Plans & Procedures, but no Practice

87% of businesses surveyed have some form of continuity plan in place, whether administered by the business itself or by a third party. However, while contingency plans are in place, fewer than half of businesses have secure practice guidelines or similar methods of ensuring staff follow secure practices.

- This inconsistent approach means that exactly what the response should be to a given cyber security threat is confused, which is particularly problematic for new employees who are unused to a given company's guidelines.

Figure 5: Actions Businesses Take to Mitigate the Impact of a Cyber Attack



- Of the businesses who have such policies in place, around two-thirds review them regularly. However, only a third of those who often review their policies hold regular training on secure practices, meaning that employees' knowledge of these is often likely to be out-of-date.
    - In addition to being old, these policies are likely to be ineffective; having secure practice guidelines or policies in place has little impact on whether the business engages in insecure practices.[ix]
    - It is probable that there is a low level of awareness among businesses that individual staff practices can impact cyber security, beyond ensuring that they take a few well-known safety precautions (such as not opening phishing emails).
- Despite this scattergun approach to cyber security, only 3% of respondents reported having no measures at all in place.
    - This means that one of the biggest problems in business cyber security is not that there are no measures in place, but that they are inconsistently applied, and not reinforced.
- The contingency-focused mentality leads to a 'curative', rather than 'preventative' approach to cyber security, with all the increased costs and vulnerabilities that this implies.

1.4.2 'We're Secure, We Just Don't Know How Secure'

- 76% of respondents consider that their businesses are secure, while 26% of respondents considered they were not taking any risks with their working processes. A similar number believe that there is no risk to the business through their current device practices.

- Over 80% of founders, C-level executives, board members and directors believe they are doing enough to mitigate the impact of cyber attacks, but less than 60% think they have the right policies in place to be secure.[x]
- These findings highlight a high degree of complacency with regard to cyber security; there is a blanket level of security assumed, while details are relatively thin on the ground.
- 'Are we safe?' should not be the primary question asked by enterprises with regard to cyber security, which instead must be considered in terms of what risks are being taken.
    - For example, nearly a third of all respondents were concerned about data theft from ex-employees, but over a quarter of those concerned do not have policies in place to deal with it.

Figure 6: Concerns About Ex-Employees

29% of UK businesses think they are at risk of data theft from ex-employees

26% of those businesses do not have procedures in place to minimise the risk of ex-employee data theft

JUNIPER RESEARCH

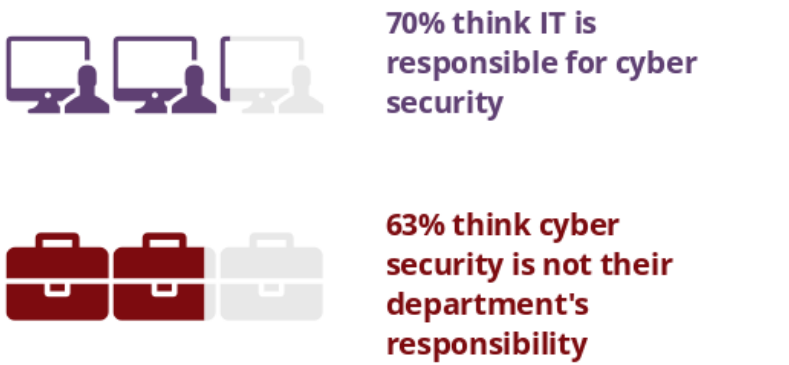
1.4.3 'Cyber Security? Talk to IT, Then Maybe Come to Us'

More than half of all respondents believed that it was the task of one department to mitigate cyber security threats, while 30% believe it is just the responsibility of the IT department.

- Only 29% of respondents would inform a security team of a data breach. This is potentially because relatively few businesses (particularly small businesses) have dedicated security teams; it may also be the case that the individuals in question would either contact another department or

individual in the first instance, or might simply feel that it was not their responsibility to report the incident.

Figure 7: Who is Responsible for Cyber Security?



- This attitude is reflected in how cyber security is addressed as a whole, with only 35% of respondents reporting that their business assesses cyber security threats across all departments.
    - This approach is slightly more common among larger companies, with 39% of those with 251+ employees reporting a multi-department approach compared to 31% of smaller businesses.
- Note however that conducting multi-department assessments will not in itself make staff more likely to consider that their own department needs to be responsible for countering cyber security threats.

TalkTalk Business Case Study

Transforming the Ways that Businesses Approach Cyber Security

As with most large organisations, TalkTalk worked hard to ensure the company was secure against potential cyber attacks, but in October 2015 they were subjected to a targeted attack on their website.

TalkTalk's approach to be open and honest with their customers about the attack from the beginning meant there was a lot of discussion about it at the time, but also helped the company's recovery. Customers have responded well to the regular and frank communications from the company, leading to lower churn, higher trust figures and improved brand consideration. This approach has also made sure they have learnt and changed the way the business addresses cyber security internally.

Charles Bligh, MD of TalkTalk Business, Technology and Security, shares his insights and what lessons other enterprises facing attacks should take into consideration:

"One of the major lessons for us has been if an organisation asks 'are we safe', they are looking at cyber security the wrong way. No company can ever be 100% safe online. Instead, the question for businesses to ask is 'what risks are we taking by doing, or not doing, something?'

"Over the past year, we've learnt from our experience and changed our attitude towards cyber security, by turning it into a business issue. Cyber security is no longer just a technology issue for the IT team to manage. All teams receive regular training and role play exercises to ensure that we have plans and processes in place should another incident ever occur."

Any business that has ever had a cyber attack will tell you that they never expected it, even with all the processes in place. Businesses need to ask themselves tough questions. What would they do? Would they tell their regulator and customers if attacked? They should put this into a clear framework which is regularly practiced and reviewed. For example:

1. Plan – how would your business communicate with customers if attacked? What are your critical services that must stay running at all times? What would be shut down or taken offline?

2. Defend – what is most important to the business? What do you need to protect first if attacked? Is it loss of data? Your reputation and brand? Your revenue? Where are the potential vulnerabilities and systems that could impact this?

3. Detect – do you have the best monitoring systems in place based on your business assets and what you are looking to protect? How will you capture any data that helps with identifying and diagnosing any problems? What is the escalation process if an issue is detected?

4. Respond – if a threat is detected, what's the chain of response? How are problems escalated and to whom?

5. Recover – how is data recovered? Make sure you have detailed checklists in place. Test and test again.

By asking the difficult questions, having a plan in place and ensuring that the entire business is involved in cyber security at all levels, TalkTalk is working to ensure its ready as it can be for any attack.

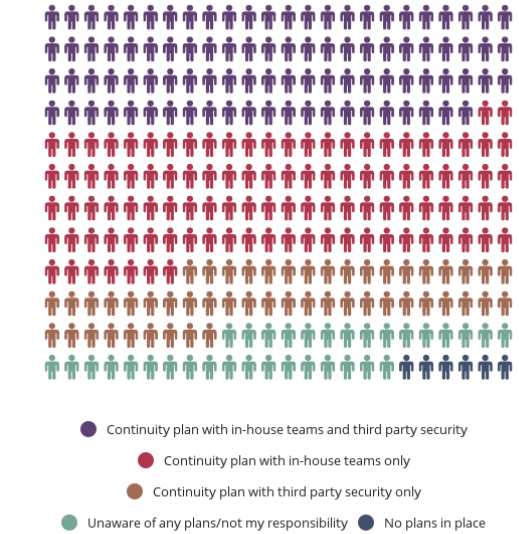
1.4.4 Cyber Attack Response

Given the increasingly connected and online nature of business, the question surrounding cyber security becomes ‘when will we have a data breach?’ not ‘will we have one?’. Nearly 90% of respondents reported having a plan in place for when a data breach occurs, most of which involve in-house action.

- On average, businesses undertake more than 3 actions to mitigate the impact of cyber attacks. The most usual of these is having secure practice guidelines, but even this was reported by less than half the respondents.

While the vast majority of businesses have plans in place, only 45% conduct crisis exercises or penetration testing to assess the ability of systems and staff to withstand a cyber attack.

Figure 8: Continuity Plans in the Event of a Data Breach

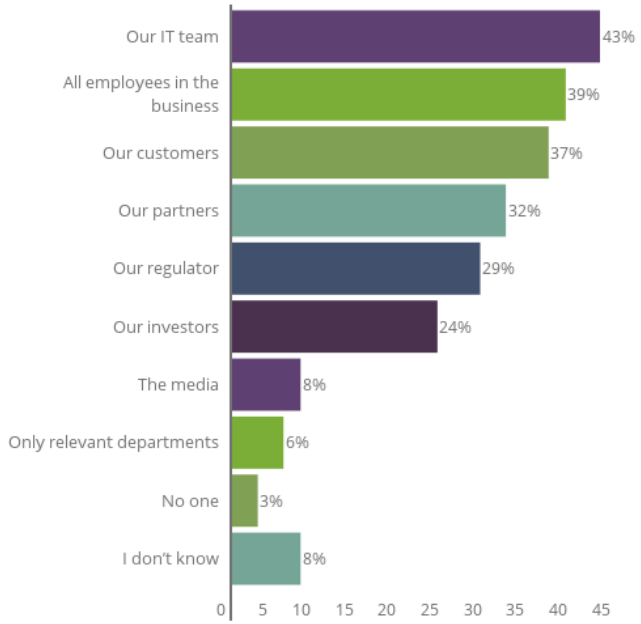


1.4.5 Tell Anyone, It Doesn't Matter Who…

Alongside having a contingency plan for a data breach, most respondents feel they are obliged to inform multiple entities about the breach. Less than 10% of respondents consider it 'need to know-only' information and on average respondents will tell more than 2 entities.

- However, as with dealing with data breaches overall, there is no clear set of practices that emerges from our survey. No single place gets more than half of responses, another indicator that responses to data breaches differ hugely between organisations.
- While the overall figure of less than 30% of respondents informing their regulator seems low, it should be borne in mind that not all industries have a formal regulatory body.
    - However, less than half of financial services institutions consider that they have an obligation to inform either their regulator (the Financial Services Authority) or their customers in the event of a data breach. This indicates a desire for this sector, which trades on its image of security, to appear secure at all costs.
- There is a negative correlation between the amount of businesses which value their reputation and the amount which tell their employees about the breach. This is accompanied by a positive correlation in concern for their reputation and likelihood of informing investors and the media. This indicates that these companies are concerned to 'control the story' around the breach and want the story to reach outside channels through the company, rather than word of mouth and other unofficial leaks.

Figure 9: Who Does the Business Have an Obligation to Inform in the Event of a Data Breach?



JUNIPER RESEARCH

Respondents who would contact another person on noticing a breach tend to think of them as problems to be solved and be done with, rather than something that should concern the company in the first instance. Around 60% would inform the IT team first, while less than 30% would take it to someone higher up in the company on discovery.

- Less than 7% of respondents would notify the CEO directly on discovery. This runs directly counter to a government recommendation that crisis response should be CEO-led.[xi]

Figure 10: Who is the First Person You would Contact on Discovering a Data Breach?

JUNIPER RESEARCH

- While respondents are most likely to inform their IT team about a data breach, respondents who consider the IT department directly responsible for cyber security are no more likely to tell the IT department than those who do not.

1.4.6 … But Not at the Same Time

- While more than half of respondents would contact someone immediately in the event they discovered a data breach or vulnerability outside of working hours, 18% would wait until the next working day if they did not consider it a 'big problem', including 38% of founders and 27% of all board-level respondents.
- This level of non-concern from those in management means that delays in response are highly likely, particularly if targeted for implementation around times when key personnel are absent from work.
    - This is something that needs to be made particularly clear among larger organisations, where a third of respondents would not contact another person immediately on discovering a vulnerability or evidence of a cyber attack outside of working hours.
- The tendency to wait is particularly high among those working in IT and finance, possibly because these industries are used to dealing with sensitive data as a matter of course, so particular vulnerabilities may not stand out. However, it also means that incidents in these kinds of companies are more likely to be left unattended and 'blow up' before they are dealt with.

1.5 Recommendations

- While 86% of the businesses we surveyed believed that they were doing enough to prevent a cyber attack, a significant minority of those had suffered a data breach. Furthermore, of the 27% of SMEs who believed that they were secure because they were 'too small' to be of interest to cyber attackers, more than half (59%) had been the victim of an attack. There is thus a significant disconnect between perception and reality regarding cyber attacks. **We would stress to all businesses that they are now targets for a cyber attack and they need to have policies in place to minimise risk.**

- Furthermore, our survey suggests that many enterprises are complacent about both the scale of cyber attacks and their inability to deal with them. 51% of businesses are either 'not aware' of any attacks or do not think that they have been attacked. **It is incumbent upon senior executives to ensure that they keep abreast of security issues so they are in the best position to assess the threat of cyber attacks and to modify (and disseminate) plans and procedures accordingly.**

- **We would recommend as a matter of urgency that businesses review their IT policies** to ensure that the plans they have in place are robust enough to face the challenge; **that** these plans are **updated regularly in response to the evolving threats;** and, that they are **communicated to all employees** across the enterprise.

    - It is essential for businesses to **ensure that all employees are made aware that security is an enterprise-wide issue and one which is not exclusively the preserve of the IT department**. In many cases this may require a cultural shift within an organisation, with all departments assuming responsibility.

- While most of our respondents had security plans in place, we would argue that enterprises will only achieve optimal levels of security by ensuring that these plans are communicated and regularly reiterated to employees. **Employees and departments need to be made aware of their individual and collective responsibilities, both on a day-to-day basis (to minimise the scale of risk) and in the event of a breach (to minimise disruption for them and the enterprise as a whole).**

- It is not sufficient for enterprises simply to provide individuals with a copy of corporate data protection rules and practices. **Enterprises should ensure that there are regular cross-company training sessions to emphasise both the scale of the threat and the actions which individuals should take**. These could and should include exercises designed to simulate attacks to gauge their potential impact and to develop and refine corporate responses in the event of an actual breach.

- **It is also essential that documentation is updated on a regular basis to reflect any attacks which may have occurred against the company,** together with any pertinent information on the evolution of techniques being used for enterprise fraud.

1.6 Methodological Appendix

This whitepaper was based on a survey of 200 managers, directors or company owners across UK businesses. The fieldwork was conducted between 10th and 17th June 2016 by Vanson Bourne through an online platform.

Quotas were set for the organisation size, with 100 respondents from businesses with over 250 employees and 100 respondents with 250 employees or fewer. Results are unweighted, and have an estimated confidence interval of ±6.93% at the 95% confidence level.

Endnotes

[i] From https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/412017/BIS-15-147-small-businesses-cyber-guide-March-2015.pdf: “The average cost of the worst security breach is between £65,000 and £115,000”.

[ii] https://www.ipsos-mori.com/Assets/Docs/Publications/sri-csbs-2016-main-report.pdf

[iii] Significant at the 90% level in a two-sample z-test between businesses with 20-250 employees and those with more.

[iv] Significant at the 95% level in a two-sample t-test between businesses with 20-250 employees and those with more.

[v] Two-sample z-test between businesses with 20-250 employees and 250+ employees showed no significant differences.

[vi] Significant at the 95% level in two-sample z-tests between businesses with 20-250 employees and those with more.

[vii] Significant at the 95% level in two-sample z-tests between businesses with 20-250 employees and those with more.

[viii] Significant at the 90% level in a two-sample z-test between businesses who increased cyber security spend and those who did not.

[ix] Weak positive correlation (Pearson’s $r = 0.15$) between likelihood of having secure practice guidelines and the number of insecure practice respondents’ departments and businesses engage in. At this level of correlation, there is likely to be no relation between the two results, indicating that having secure practice guidelines does not have an impact on the amount of insecure practices engaged in by respondents’ companies.

[x] Significant at the 95% level in a z-test between founders, board-level respondents and directors who consider they are doing enough to mitigate the impact of cyber attacks and those who think they have the right policies in place to make their businesses secure.

[xi] http://www.publications.parliament.uk/pa/cm201617/cmselect/cmcumeds/148/14805.htm#_idTextAnchor010