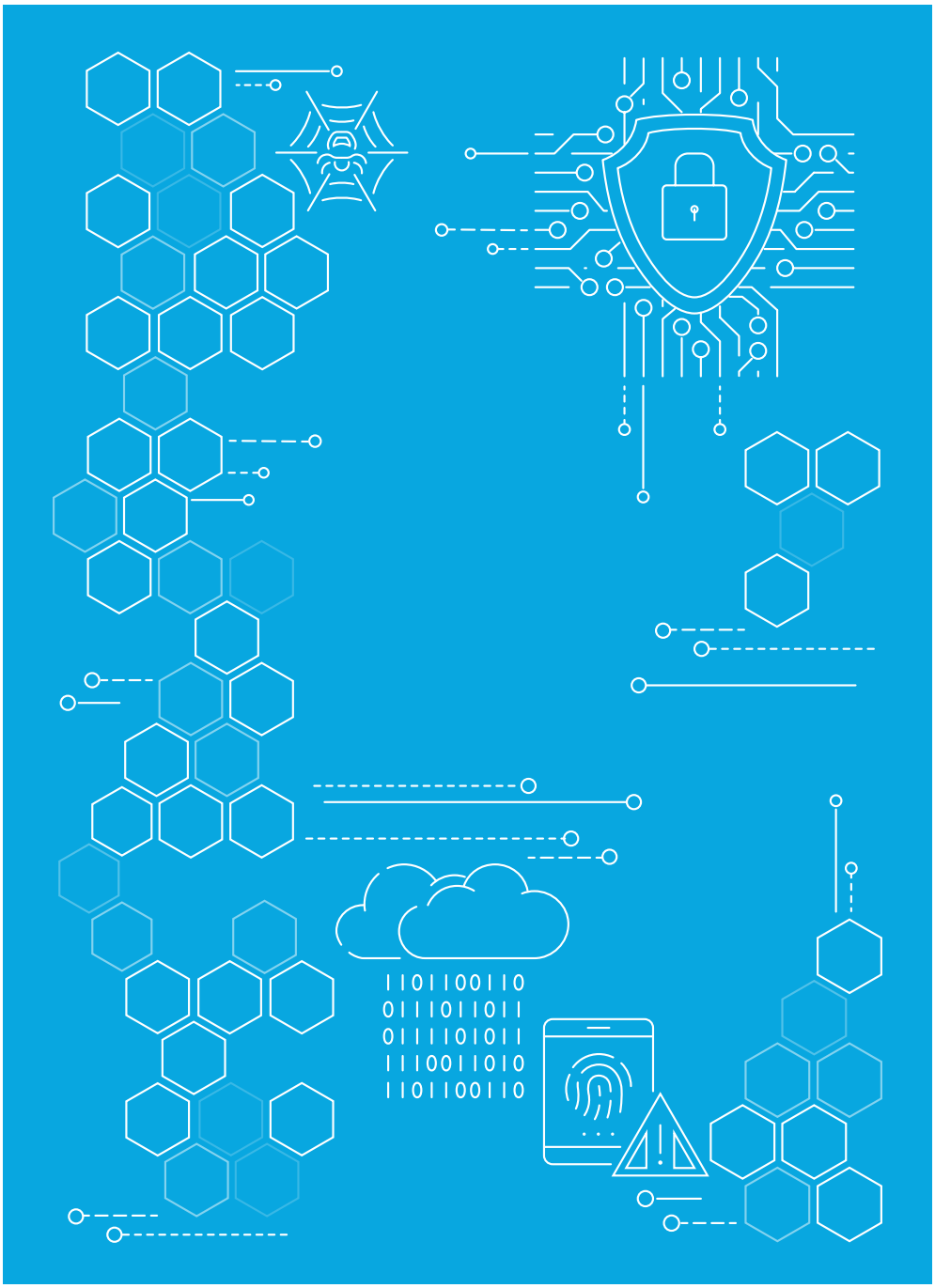
CATCH–22:
DIGITAL TRANSFORMATION AND ITS IMPACT ON CYBERSECURITY



THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING

RSM

EXECUTIVE SUMMARY

Regardless of their digital footprint, any business with a reliance on technology is at risk of cybercrime. In today's digitised economy where threats to cybersecurity are continuously increasing, protecting data, infrastructure, customers, business partners, clients and third-parties against a breach is one of the biggest challenges that European businesses face. The financial and practical challenges that technology brings mean we are more interconnected globally thereby increasing the opportunity for cybercrime hence, the Catch-22 business leaders face. If a business doesn't go through a digital transformation there is a risk it may get left behind, and if it does there is an inherent and increased risk of cybercrime.

An in-depth survey of successful companies across Europe has been undertaken for RSM International by the European Business Awards, in order to understand levels of industry awareness of these cyber risks, the actions being taken to combat them, as well as the reaction to breaches taking place. The ultimate purpose, given the findings, is to raise awareness to C-suite and senior management, of the urgent need for establishing a formal cybersecurity strategy, planning to combat and react to a cyber event and the action required to secure their organisation's most valuable asset: data.

RSM's '**Catch 22: Digital transformation and its impact on cybersecurity**' report comprises responses to a range of questions posed to 597 companies in 33 European countries, spanning multiple industries and sizes, with recorded turnovers varying from less than €30 million to over €300 million. 56% of the respondents are on the management board with a further 31% reporting directly to the board. *

Although 80% of leading European businesses say digital transformation is a current strategic priority for their business, a significant number of organisations are not adequately protecting themselves against cybercrime. So, while businesses are alive to the threat of a breach, a large majority believe they are at risk of suffering a cyber attack. A significant number of businesses do not have a formal cyber security strategy in place; and amongst those that do, display a lack of faith in these strategies to protect them.

Additionally, most European businesses think it is possible that their company has been hacked without their knowledge, leaving them in a vulnerable position to further cyberattacks.

The survey also reveals that at board and senior management level, there is a gap in awareness and perceived accountability, which may be one of the key internal drivers behind this vulnerability. Not only is there a lack of discussion around the risks at board level regarding cyber security but there is also ambiguity over who is responsible for leading on this within the organisation.

However, the study offers reasons for hope and signposts key solutions. Largely thanks to the EU's General Data Protection Regulation (GDPR), much of the groundwork has been laid, and most businesses who responded to the survey have taken the first steps to securing data.

Finally, the section of data examining the direct actions of those businesses who have already experienced a security breach shows positive actions and reactions from European businesses to the crime and raises compelling questions around transparency and a continuous need for employee training.

** Results between size and seniority of role did not significantly change the main findings and the views and issues raised were similar across the whole of the middle market.*

ABOUT THE AUTHORS

SHEILA PANCHOLI, RSM UK

Sheila is a national partner responsible for leading the Technology Risk Assurance practice across RSM UK. She has undertaken Head of IA and Risk roles as well as leading successful co-sourced and outsourced IT Audit teams across a diverse range of clients over her 26+ year career in practice. She is a cyber security and data privacy specialist and has provided assurance and advisory support to a wide range of organisations to help clients manage all aspects of technology risks including cyber security, data privacy and operational resilience. Sheila has led SOX compliance and third-party assurance engagements across a broad client base including Financial Services, Utilities, FMCG, Media & Entertainment, Retail & Hospitality, Technology, Telecommunications, and Manufacturing. She is an IT risk and controls specialist and has significant experience in delivering global SAP ERP system implementations and leading project and programme assurance engagements, including major change programmes and systems implementations, data centre relocations and outsourced IT service provision.

GREGOR STROBL, RSM GERMANY

Gregor is a national partner responsible for leading the Technology and Cyber Risk Assurance practice across RSM Germany. He has considerable experience with the implementation and ongoing monitoring of risk management and internal control (SOX) projects for middle-market companies and international corporations based on the universally known and accepted COSO frameworks (COSO I and COSO II / ERM) as well as on ISO standards for risk management. With extensive experience, he is a specialist in serving clients in the field of IT risk management services, IT audit services as well as other special services (e.g. IT migration projects, Process Mining and Mass Data Analytics, GDPR, Forensic Services and Business Resilience with regards to cyber threats). For over 10 years, Gregor has provided risk advisory and cyber security services to customers in the private sector as well as to non-profit organisations and educational institutions based on their individual business needs.

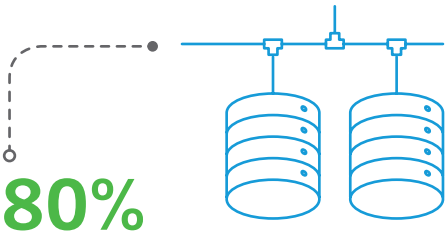

We exist to empower our clients to move forward with confidence.

INCREASED DIGITAL TRANSFORMATION INCREASES THE NEED FOR CYBERSECURITY AND ACTION

OVERVIEW

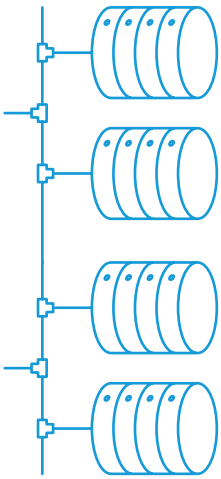
In today's fast-changing digitally-led economy, most businesses are currently going through some form of digital transformation, either to improve their offering or to streamline their operations, with many already seeing the benefits of financial investments made. The Catch-22 is that with this increased use of technology and collection of personal data, the need for protection increases. But not all businesses are actively protecting themselves against cybercrime.

KEY FINDINGS



80%

of leading European businesses say digital transformation is a current strategic priority for their business



Digital transformation is happening across multiple areas of business, not just operations and customer service.

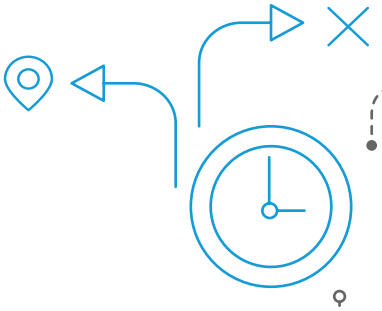
- Sales
- Business development
- Finance
- Logistics
- Marketing and HR

21%

of leading European businesses do not have a cybersecurity strategy in place despite having invested in digital technologies

"A hacker attack happens every 39 seconds"

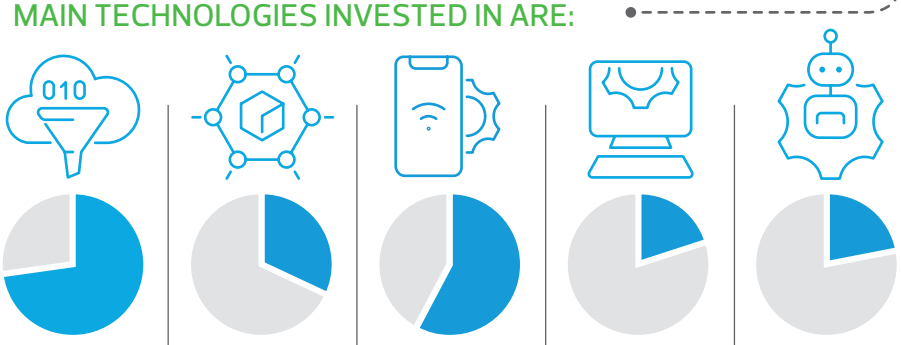
Clark School study at the University of Maryland



29%

of businesses have experienced an increase in revenue from digital transformation

MAIN TECHNOLOGIES INVESTED IN ARE:



73% CLOUD

32% INTERNET OF THINGS

58% AUTOMATION

20% MACHINE LEARNING

22% AI

THE MAIN PURPOSES OF THE TECHNOLOGIES INVESTED IN ARE:

MULTIPLE CHOICE ANSWER	RESPONSES
To integrate, activate and utilise data across functions to enhance business performance	67%
To update obsolete systems	51%
To reinvent and evolve business processes	51%
To secure sensitive data at risk of breach	34%

ATTITUDES:

- 78% of businesses agree that digital transformation is the only way to thrive in the current and future economy
- 64% of businesses agree that it is inevitable that digital technologies will replace lower skilled jobs
- 12% of businesses strongly agree and 38% agree that the more technology you implement, the more at risk you are of a cyber attack if adequate controls are not implemented

INSIGHTS FROM RSM

It is no surprise to see that the majority of companies are embracing digital technology and recognising its importance and future role. Any business looking for growth, longevity and a competitive edge is now using digital technologies, in multiple business areas to drive efficiency revenue and sales.

But the key to success is having a strategic approach. Risk management, security and good project management of any investment in digital transformation must be properly considered if the benefits are to be realised.

Effective digital transformation isn't just about changing your systems; businesses must change their culture and their working habits. They must understand that these new processes bring different ways of working, new training requirements, and crucially, new risks. And it is here we see a major problem emerging.

When it came to reasons for adopting new technologies, the lowest driver is 'to secure sensitive data at risk of breach' and it is the first indication of an issue. This suggests that the need for more security tools and skilled resources to protect against the risk of a breach (as more firms become digitised) is not being recognised.

Further, there are two alarming findings that underpin this. Only 12% of businesses strongly agree that the more digital technology you implement the more at risk you are of a cyberattack, while 21% of European businesses do not have a cyber security strategy in place despite having invested in digital technologies. This means one in five European businesses have no coordinated way of tackling cybercrime.

It seems that many European businesses haven't yet made the link that the more digital you become, the more connections and access points you have, making you more vulnerable to cybercrime and therefore more likely to have a breach.

It is clear: if you adopt digital technologies, you need a cyber security strategy. Security and operational resilience must be a key factor in the strategy for businesses as they move forward in this digital transformation.

Quite simply, robust cybersecurity strategies make firms more resilient. A strategy is your starting point: it gives you an overarching framework that sets out goals, determines what you are looking to invest in, assesses risk appetite, spots weaknesses and threats, identifies areas in the businesses that are reliant on third-parties — a huge risk area for cybersecurity — and details how you would recognise and contain a breach.

If a business hasn't gone through that process then not only is the risk of a cyberattack much greater, the degree of damage a potential breach could have becomes immeasurable.

Additional or supporting data

Data Breach Investigations Report (2018) https://enterprise.verizon.com/resources/reports/DBIR_2018_Report_execsummary.pdf
DLA Piper GDPR Data Breach Survey: Feb 2019 https://www.dlapiper.com/en/uk/

HOW TO PREPARE AND MITIGATE INEVITABLE CYBERCRIME

OVERVIEW

The majority of European businesses understand they are at risk from a cyberattack and many even believe they could have been the victim of a breach without knowing. However, coupled with this, is a lack of confidence in their ability to protect themselves and a sense of inevitability and resignation to an attack, with many believing hackers will always outwit preventative software.

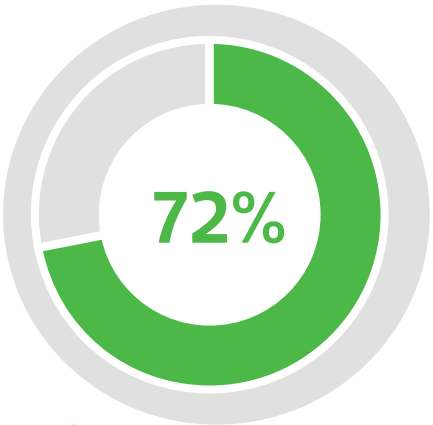
KEY FINDINGS

OF THE BUSINESSES THAT HAVE A CYBER SECURITY STRATEGY

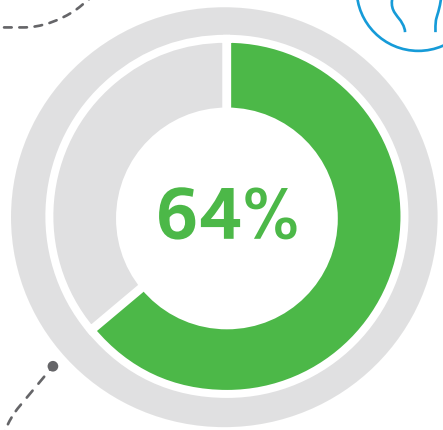
29% don't believe it will prevent a cyberattack

23% of businesses are unsure it will prevent a cyber attack

48% believe the company's security strategy will protect them



of businesses believe they are at risk from cybercrime



of leading European businesses think it is possible that their company has been hacked without them knowing

"There are two types of companies: those who have been hacked, and those who don't yet know they have been hacked"

John Chambers, former CEO, Cisco

INSIGHTS FROM RSM

When it comes to cybersecurity, the lack of confidence from businesses is understandable because the reality today is that the threats are greater than protection – the hacker is always two steps ahead.

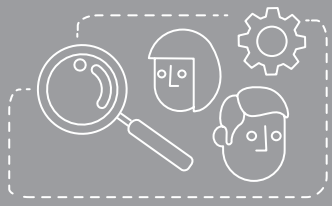
Not only are there more hackers, but we have seen a move towards syndicates where criminal organisations across the globe are joining forces – often working together via the dark web quite often geopolitically – making the threat stronger.

Doing nothing is not an option. The first step to protection is understanding that investing in security tools and technology will not necessarily prevent an attack, but with strong user education and awareness, it may help you to monitor, detect early, and quickly deal with a breach should one occur.

A strong incident management process will also be crucial to containment. The more equipped you are to contain a potential breach, the less you are you going to be impacted from it – whether that be reputationally or financially.

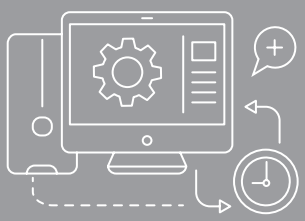
Controls to prevent, detect, contain and build reliance can be the difference between little impact and a public scandal with significant financial loss.

EFFECTIVE INCIDENT MANAGEMENT INCLUDE



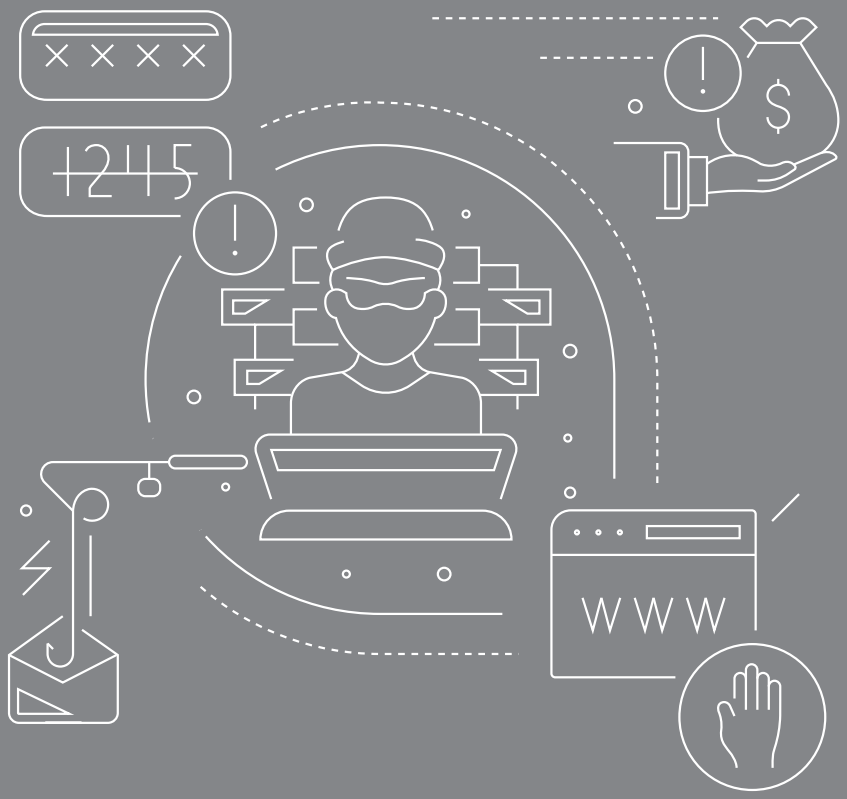
Training users to identify a potential attack and knowing who to inform

Having tools and technology in place to identify and prevent malware



Having regular monitoring in place over systems and infrastructure

Having a formal tested process for dealing with incidents, to contain the incident and resolve it as quickly as possible



If you want to keep pace with the developments in technology, you need to keep pace with the developments in cybersecurity – the two must go hand in hand.

The 64% who believe they have unknowingly been breached is a major concern given the implications and this indicates the psychological stronghold business leaders are under by cyber attackers.

We have seen instances where, via phishing, an attacker has dropped malware into the back of an email inbox and over time all email traffic to and from that email address was redirected to an email inbox abroad, and this went on for months without being detected. An investment in monitoring tools could have detected this but as with many of the clients we see, the damage had been done before they came to us for advice.

Cybersecurity needs to be a priority before the breach as well as during the breach, as mitigation work whilst the breach is occurring can make a huge difference on the potentially damaging effects. Prioritising cybersecurity after breach is, by definition, too late.

CASE STUDY

DATA BREACH IN THE UK

The work we carried out

Our client had suffered a data breach on the back of a phishing attack which had resulted in the compromise of personal and commercially sensitive data via the email account of an IT team member. Given the client is regulated by the UK's Financial Conduct Authority, they were keen for our specialist Technology Risk Assurance specialists to undertake a formal investigation following the data breach. We undertook a post-incident investigation which included looking at the controls in place to prevent the breach ('prevention'), the controls in place to identify the breach ('detection') and the approach taken by the business when the breach was detected ('containment').

The outcome

We identified from our initial investigation that there were underlying weaknesses in the IT control environment, no formal process to effectively manage a data breach or cyber incident; and a lack of awareness amongst staff of cyber threats and risks across the organisation.

As a 'phase 2' engagement, we developed an end-to-end incident management process for the organisation, scenario tested it with key stakeholders and the Board; and conducted cyber training for all staff across the organisation (over 120 people) including the Senior Executive team. We have also provided detailed advice and practical guidance as to how the business can ensure robust controls exist across their IT infrastructure.

BOARD AND SENIOR MANAGEMENT MUST BE RESPONSIBLE FOR CYBERSECURITY

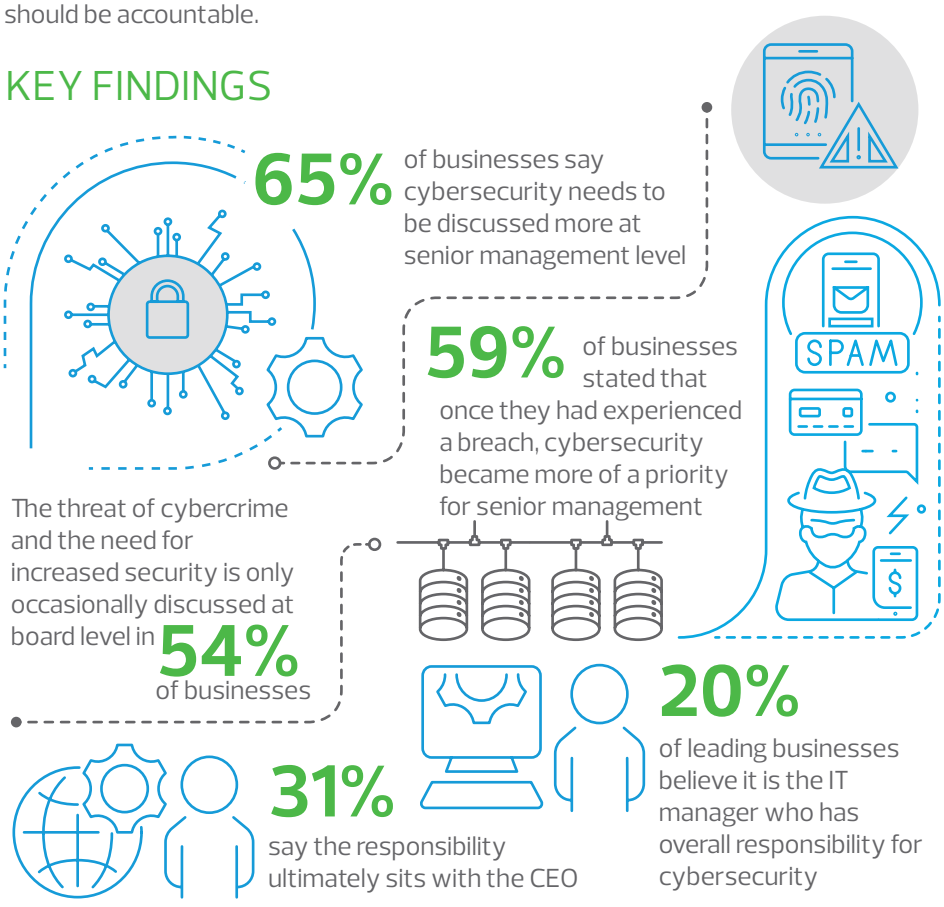
"Corporate governance specialists are increasingly concerned that senior management and board directors across the world are ill-prepared for potential data breaches and other technology problems"

Attracta Mooney and Jennifer Thompson, The Financial Times

OVERVIEW

There is a gap in senior management's engagement and prioritisation of cybersecurity that needs to be addressed. Not only is there a lack of discussion around the risks at board level but there is also ambiguity over who is responsible for cybersecurity in the organisation. Ideally, the senior executives themselves should be accountable.

KEY FINDINGS



For businesses, there are multiple requirements to tackle the threat to cybersecurity:

INSIGHTS FROM RSM

Cyber risk management needs to be owned at board level and it is encouraging to see 60% of the management board of businesses agreeing that it should be discussed more often. Certainly, we have seen a clear shift towards this over the last few years, with RSM training and raising education and awareness levels of the threats and solutions of cybercrime to an increasing number of C-suite, executives and non-executive directors.

However, it is still concerning to note that only 38% of board members see the CEO as the person ultimately responsible for cybersecurity within their business. Cybercrime is a senior executive responsibility. It's important to remember that when a data protection breach or attack takes place, it is the CEO who is liable.

It is still common for senior level management to become involved only after a breach and not before. Indeed, 59% of businesses stated that once they had experienced a breach, cybersecurity became more of a priority for senior management.

All too often senior management don't see the need for investment in cybersecurity, holding on to the dangerous belief that since they have yet to experience a breach (as far as they are aware) it won't ever happen.

Many CEOs are ignoring the problem and only want to invest in cybersecurity when they see that something will happen or can happen. This is a particular problem for small companies with limited budgets where there is no CIO or IT Director in place and the CEO has a limited knowledge of cybercrime.

This will change as the number of breaches and public fines increase, but we are actively encouraging senior executives to understand the risks associated with cybercrime, how it affects the organisations they're responsible for, and advising where specialist support is required to protect the business against cyberthreats.

Additionally, once senior management make combating cybercrime and protecting their business a greater priority, then many of the key requirements identified by businesses to tackle the threat are more likely to be delivered.

CASE STUDY

GDPR COMPLIANCE – A GLOBAL ORGANISATION

The work we carried out

In 2017/18 we worked with an organisation to support their readiness for GDPR coming into force. This highlighted a number of weaknesses in their underlying IT infrastructure and systems controls which resulted in a programme of work to assess each business unit across four different geographic locations against the NIST (National Institute of Standards and Technology) cyber maturity matrix. In doing this, our cyber security specialists worked closely with senior stakeholders across the business to determine the level of cyber risk and threat posed by the business against the organisation's risk appetite.

The outcome

The business has a documented maturity model to determine the level of control they want to implement across the various business units and cyber security domains to safeguard the business from data loss, financial and reputational damage. This allows senior management and the Executive team to make informed decisions on future investment in cyber security and where risks will be accepted.

Senior management have determined the level of investment they need to make in safeguarding the business from cyber threats and have a clear understanding of the risks and controls being managed across each business unit globally. There is a clear directive on which cyber related risks will be accepted by the business and which risks need to be managed. Where control weaknesses or gaps have been identified we continue to work closely with the IT function to determine practical solutions to address these weaknesses.

Clients trust me to help them unlock opportunity by putting risk in the spotlight.

THE POSITIVE AND NEGATIVE CONSEQUENCES OF GDPR

OVERVIEW

The EU's General Data Protection Regulation (GDPR), which came into force in May 2018, is identified as the key driver to businesses taking the first steps in cybersecurity. More than one year on from the implementation of GDPR, the legislation is justifiably seen as a champion of security, but there have been some unintended consequences.

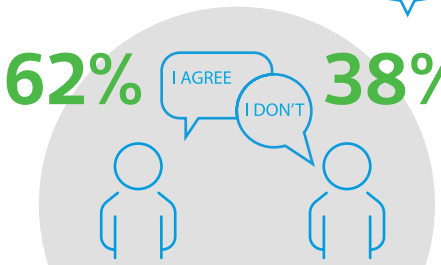
KEY FINDINGS

REASON FOR INVESTING IN CYBERSECURITY:

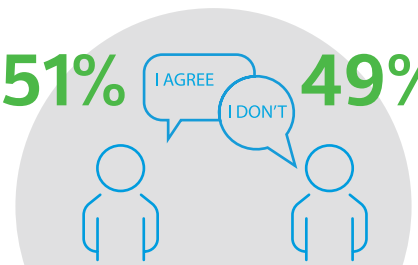
68% the GDPR requirements

55% holding increasing amounts of customer data

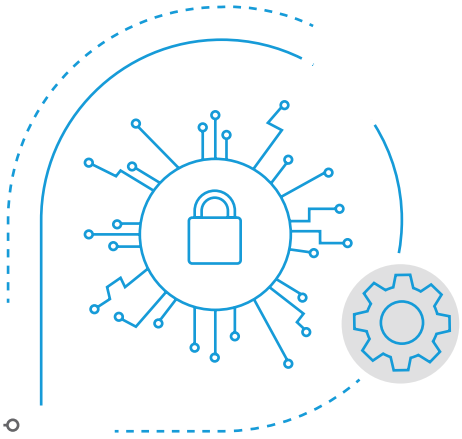
26% of businesses don't believe their business is fully compliant one year on from GDPR



GDPR compliance has resulted in more investment in cybersecurity



GDPR compliance has made our business safer from cybercrime



"Our qualitative findings suggest that GDPR has encouraged and compelled some organisations over the past 12 months to engage formally with cyber security for the first time, and others to strengthen their existing policies and processes. However, the qualitative findings also highlight that GDPR has had some unintended consequences"

UK Government report 2019

INSIGHTS FROM RSM

It is no surprise that the GDPR is the key driver for cybersecurity. It has significantly raised the level of awareness among European businesses of data breaches resulting from cybercrime and the need for protection. GDPR has given cybersecurity weight through giving cybercrime more tangible consequences.

More specifically, from our work with businesses across Europe, we see that it is the threat of financial penalties behind GDPR and the resultant reputational damage that has spurred action.

The fear of significant financial penalties has changed the way organisations are thinking about data protection and security. Many businesses have taken a closer look at their data footprint and data privacy controls and made an investment in protecting data assets.

GDPR has succeeded in forcing action that was long overdue.

However, there has also been a downside to this. With so much pressure on organisations to meet the complex requirements we have seen GDPR fatigue; overwhelmed by information and demands on what they had to do from the press, industry bodies and stakeholders, many organisations just gave up and reverted back to previous working practices. This may have also resulted in many businesses (especially those in unregulated industries) taking a more 'tick box' approach to getting the job done resulting in less effective protection and a false sense of security.

A further issue with the GDPR was it took a one-size-fits-all approach. This meant many requirements were left open and too broad, which as another unintended consequence, has left businesses more vulnerable.

Our research has highlighted the gap: while 62% of businesses invested more in cybersecurity in preparation for the GDPR, 49% do not believe it has made their business safer and 26% don't believe that a year on from the GDPR deadline, their business is fully compliant.

There is clearly still a lot of work to be done and pressure is needed. As soon as audits are carried out, there will be fines, press coverage and needless to say, action.

We would urge firms to be proactive rather than reactive and take positive steps to take the time to review what has been put in place as a matter of priority. Cybersecurity controls should not be just about meeting the GDPR requirements but about protecting your key business assets on a wider basis.

CASE STUDY

GERMAN RANSOMWARE ATTACK

The work we carried out

A partner of a marketing communications business received an email from someone known to them expressing a potential business interest. The partner opened the email and an attachment, unaware that it contained anything suspicious. He began having difficulties finding files for his clients, and it was only when the partner found and tried to open a file that he received a pop-up message informing him that his files had been encrypted and he would have to pay money in order to regain access to the files. The partner alerted the IT department, who quarantined the partner's files, so they were no longer in contact with the server.

RSM's Risk Advisory Services cybersecurity and IT specialists were contacted by the marketing communications agency to assist them with identifying the issue, recovering the files and securing the data for the future. RSM's team ran tests to identify which files had been blocked and if any other computers had been affected and confirmed that the attack had only affected the one partner and associated client files. The partner's computer was wiped, removing anything suspicious. The team reviewed the back-ups and set it to the point in time when a large number of files were accessed simultaneously, so the back-up could recognise suspicious activity and developed an ongoing policy to minimise loss in the event of another ransomware attack.

The outcome

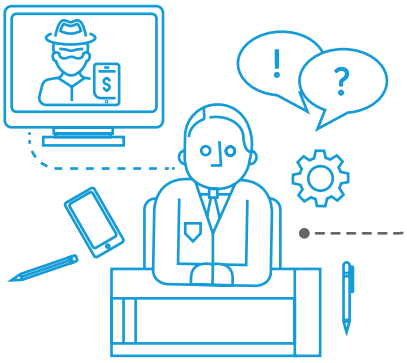
The RSM team were able to minimise the impact, recovering everything except 17 minutes' worth of data. Normally ransomware can only impact files with direct access. The objective of this type of hacker is to affect as many files as possible to ensure they are paid the ransom money. Due to the help of RSM in advance of the attack, the company had sound policies and procedures in place and had conducted appropriate levels of training, however in this case human error was the root cause. The impact of this attack could have been substantial if the partner had clicked on the suspicious email in the evening giving the system more time to infect files without being detected, or if the business had been a production environment and not service based. Ransomware can only access the files that you also have access to, therefore it is important to restrict access to files and have authorisation policies in place, otherwise all files could be infected.

THE PSYCHOLOGY OF CYBERCRIME AND VULNERABILITY OF EMPLOYEES

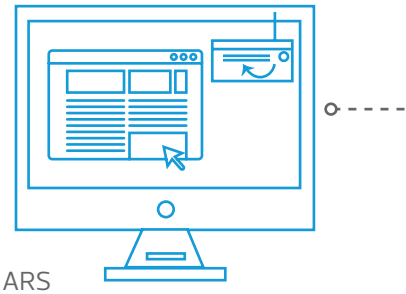
OVERVIEW

When it comes to threats now and in the future, most businesses see human error as the core area of vulnerability with targeted attacks on staff via phishing, whaling and ransomware attacks being the most sensitive touchpoint. This assertion is consistently supported by all of the findings on data breaches that have already occurred.

KEY FINDINGS



64% of businesses cited 'ensuring staff company-wide are appropriately trained to prevent human error' as the key challenge they face



THE GREATEST CYBERSECURITY THREAT TO EUROPEAN BUSINESSES OVER THE NEXT TWO YEARS

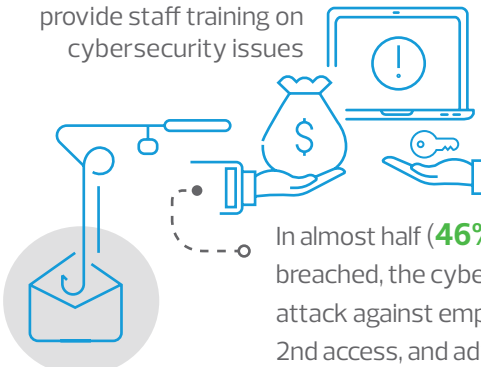
44% targeted attacks against employees via email

22% of businesses don't provide staff training on cybersecurity issues

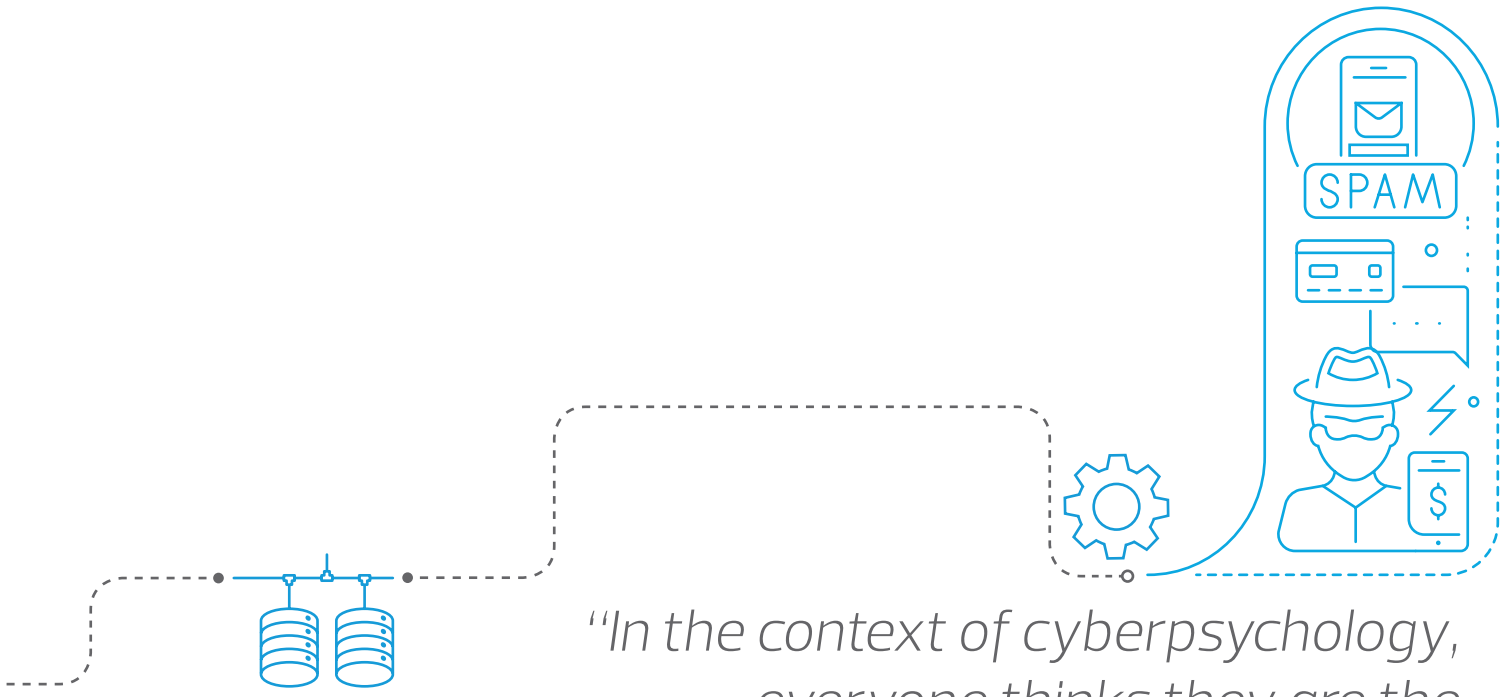
24% advanced persistent threats /advanced malware

18% ransomware

13% third-party administration



In almost half (**46%**) of cases where a company had been breached, the cybercriminal gained access through a targeted attack against employees via email, with ransomware (**25%**) 2nd access, and advanced malware (**24%**) and third-party administration (**9%**) following



"In the context of cyberpsychology, everyone thinks they are the equivalent of a cyber genius. In a study conducted at Friedrich-Alexander University, Germany, 78% of participants stated in a questionnaire that they were aware of the risks of clicking on unknown links, and yet, when sent a mock phishing email, 45% clicked the malicious link anyway"

The Huffington Post

INSIGHTS FROM RSM

Psychology plays a vital role within cybercrime. The cynical hacker's success comes from a detailed study of human behaviour through the use of social engineering to understand what will trigger action and take advantage of our curiosity and propensity to trust. Ultimately, using social engineering, the hacker's goal is to manipulate and deceive people into performing actions or divulging information such as passwords, bank account information, sensitive personal or commercial data, and they can even install malware on your computer.

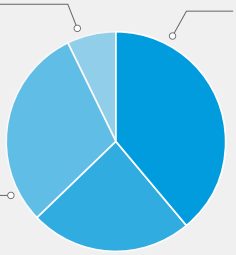
It is vitally important staff are aware of the threats of cybercrime and know how to recognise a potential phishing, whaling or ransomware attack. We are seeing an increase in all of these methods of cyberattacks – which can result in significant operational disruption, financial loss and reputational damage.

The threat of human error is a key challenge for all businesses. The most important solution is ongoing user education and continually raising awareness.


Thinking ahead
and responding
rapidly.

REPORTING CYBERCRIME TO INCREASE AWARENESS AND FIND SOLUTIONS

When directly asked if they knew if their company has ever had a **security breach**:

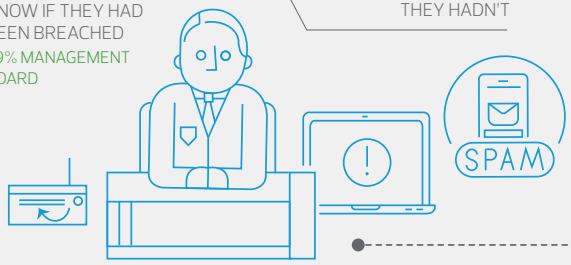


7% BELIEVED IT WAS NOT THEIR POSITION TO KNOW

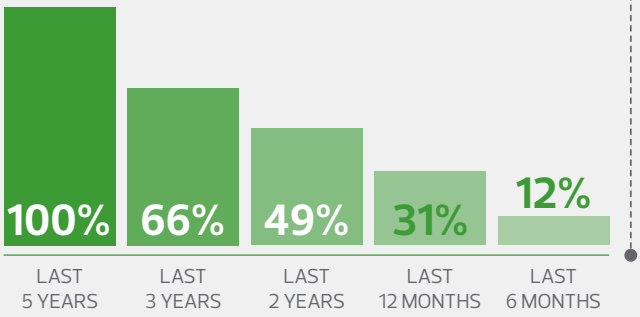
39% OF BUSINESSES SAID THEY KNEW THEY HAD
40% MANAGEMENT BOARD

30% SAID THEY DIDN'T KNOW IF THEY HAD BEEN BREACHED
29% MANAGEMENT BOARD

24% SAID THEY KNEW THEY HADN'T



Details of the businesses admitting a breach. The breach took place in:



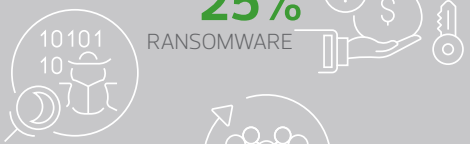
77% of the breaches were identified by an internal member of staff

9% come from the hacker (ransom demand)

7% were alerted by an external client or customer

CYBERCRIMINAL GAINED ACCESS THROUGH:

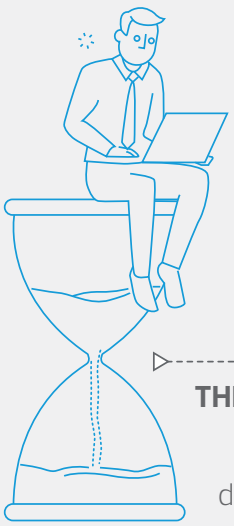
46% AN EMAIL TO AN EMPLOYEE



25% RANSOMWARE

24% ADVANCED MALWARE

9% 3RD PARTY ADMINISTRATION



In **50%** of cases the company was made aware of the breach within the **first 2 hours** of the attack, **28%** were alerted **within 24 hours**, **9%** within **less than a week** and **3% in 1–2 weeks**

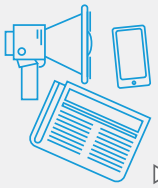
THE KEY IMPACT

54% data loss/leakage or system damage

19% didn't know

OVERVIEW

A significant number of companies in the survey admitted a security breach and gave details about how they had dealt with it and its impact. The findings confirm the critical role of the employee with most attacks identified by them and/or access gained through them. Positive direct action after the event is seen with investment in software, training and much needed IT security reviews. However, one key issue highlighted is the lack of transparency of the breach with 75% of breaches not becoming public knowledge.



In **75%** of the businesses the breach **DID NOT** become **public knowledge** (in only **19%** of businesses **it did**)

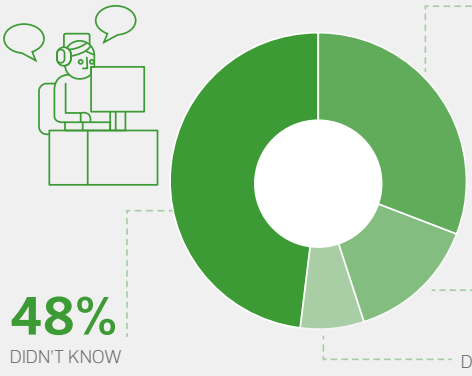
When asked if they fully understood in what circumstances, or level of data breach, they should inform the Data Protection Authority when a potential breach of personal data has been detected

34% said **'NO'**

SHORT TERM RESPONSE OF BUSINESSES:

- **23%** INFORMED THE REGULATOR
- **21%** INFORMED CUSTOMERS
- **66%** INTRODUCED IMMEDIATE COMMUNICATION TO STAFF
- **4%** PAID A RANSOM

THE OVERALL EFFECT OF THE DATA BREACH ON THE COMPANY



- **31%** THE IMPACT ON INTERNAL MORALE
- **14%** RESULTED IN LOSS OF REVENUE
- **7%** DAMAGE TO THE BRAND
- **48%** DIDN'T KNOW

In **10%** of businesses, cybersecurity did not become more of a priority for senior management even after the breach

LONG TERM RESPONSE OF BUSINESSES:

- **61%** invested in new security technology
- **51%** invested in staff training
- **37%** sought help from external specialists
- **27%** searched for and found further vulnerabilities in defences
- **26%** developed/updated crisis planning to include security
- **16%** invested in insurance
- **15%** reviewed third-party suppliers
- **8%** still reviewing the issue
- **5%** invested in rebuilding trust with customers
- **4%** reduced data

The most positive outcomes cited from the breach by businesses was an **increased awareness of threats company-wide** (**60%**) and a **necessary review of systems** (**49%**)

INSIGHTS FROM RSM

Firstly, the data highlights the importance of the role of the employee and the need for cybersecurity training throughout organisations. The greatest risk within an organisation comes from the inside as most breaches come via employees. Therefore, internal morale in a business takes the biggest hit after a breach. Having a culture which encourages staff to report data breaches is key to ensuring that the real scale of the threat can be determined, and importantly, so that root cause analysis can be undertaken to help prevent future attacks.

We also see a confirmation of 'action after the event' with the majority of firms investing in software and training in the long-term. However, given the volume of ongoing cyberattacks, the findings also ring some alarm bells. Only 27% of businesses searched for and found further vulnerabilities in defences post-breach, and only 26% developed or updated crisis planning to include security. That leaves the majority of organisations in the same place they were before the breach occurred.

Worryingly, only 15% of businesses reviewed third-party suppliers. As businesses are increasingly reliant on third-party service providers, it is vital to ensure that these third-parties have effective security, controls and processes in place to maintain the security and resilience of their operations. Independently assessing third-party operations can give senior executives and the board the assurance required over these outsourced providers.

When we address the finding that in 75% of the businesses, the breach did not become public knowledge, there is one key question – did it need to? Arguably, yes. If firms are keeping breaches under the radar (for fear of financial or reputational damage for example) then we have a harder task of making businesses understand the risks. If you are continually told something will happen but don't see evidence of it, you will be less likely to believe it or be inclined to take action against it. If those 75% talked about the issues and problems, there would be movement in the market, more awareness at CEO level, increased software solutions and better protected organisations. Reporting breaches would be a great help to the industry.

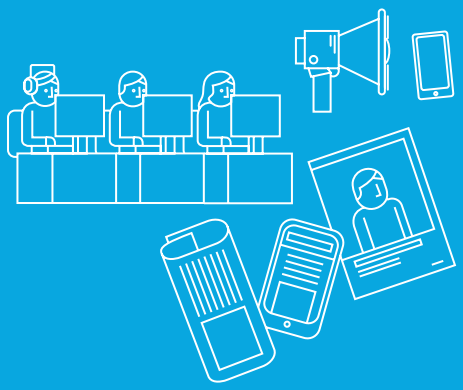
However, there is a balance to be found when it comes to reporting a breach. There are factors to be considered: what is the regulatory requirement? Is the data that was breached personal information that could cause distress to an individual? Has a high volume of data been breached? If not, do we actually need to know? Most businesses will be subject to a large number of attempted attacks, but they may not result in significant damage.

What the regulator is required to know causes much confusion. 34% of businesses have admitted they do not fully understand in what circumstances, or in which level of breach, the regulator should be informed. Clarity is needed. At the moment this will only take place as more breaches and fines occur.

Overall, we need to see a broader reporting requirement across every industry. Not only would increased transparency drive greater protection but the fact that there are businesses outside of regulation that don't need to report anything at all shows a lack of balance.

We would advise a sensible approach while understanding the duty of care and governance requirement to all stakeholders.

RSM'S **CYBERSECURITY** TOP TIPS

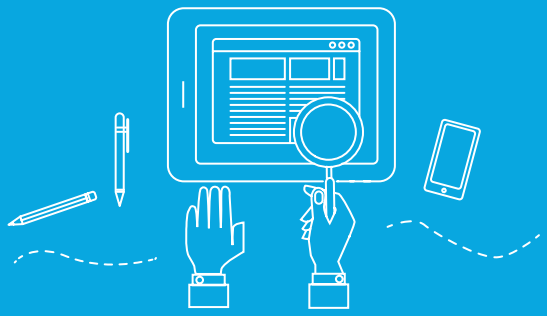


MAKE THIS A BOARD LEVEL ISSUE

- Consider all of your risks – data, people and third-party
- Review your policies and procedures
- Provide rolling education and training e.g. on the use of social media

STAFF RESPONSIBILITIES

- Read policies and procedures
- Keep up-to-date with education and training
- Be aware of unusual phone calls, e-mails or texts
- Verify contacts
- Accept all security updates to your PC/laptop as soon as possible
- Don't click on links – type in the URLs

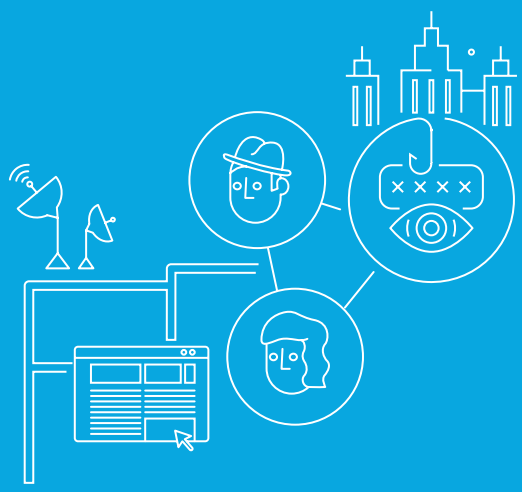


CYBER RISK MANAGEMENT

- Report anything suspicious to IT immediately
- Be careful on social media
- Change your passwords regularly
- Have strong and different passwords for different accounts
- Be careful with portable media
- Check security certificates, especially for payment websites

WHAT DOES BEST PRACTICE LOOK LIKE?

- Keep your firewalls, operating systems, virus engines up-to-date
- Password protect the Wi-Fi
- Consider data scrubbing
- Implement good IT general controls in depth
- Have a formal Incident Management plan for when the worst happens
- Consider compliance with Cyber Essentials Plus, or similar good practice
- Consider cyber insurance
- Check physical site controls
- Review controls against social engineering generally
- Conduct penetration testing



CONCLUSION

RSM's 'Catch 22: Digital transformation and its impact on cybersecurity' report clearly shows that organisations must do much more to protect themselves. Businesses should not wait for a breach to occur before investing. A breach is inevitable and choosing to react rather than protect could create untold damage to an organisation.

The main responsibility for cybersecurity lies with the CEO and change will happen if senior management step up, become aware of the dangers, and take charge. To combat the Catch-22, CEOs must match tech spend with cyber spend to effectively protect their company, invest in continual training for employees (a firm's most vulnerable and capricious access point) and be honest when a breach has occurred.

An industry shift around cyber risks, threats and breaches is needed and transparency is at its heart. Open discussion, best practice and fair regulation will drive better solutions and ultimately lead to a more protected world.

NOTES

- Not all figures for every question add up to 100%, as some questions required multiple answers (e.g. top 3)
- Not every question was answered by every business surveyed but all statistics are a percent of the number that answered each individual question

THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING