Grant Thornton

An instinct for growth™

Cyber security: the board report

How boards can reduce the impact of cyber-attacks on business

2019

Contents

Section	Page
Why now?	5
The growing threat: who's affected?	6
How vulnerable are you?	14
Board leadership makes the difference	18
Taking control of cyber risk in your organisation	22
About the research	25
Our cyber capability	26

Video No. 5243

Why now?

Just like business and technology, the cyber threat never stands still. It's always evolving and will always be with us. Criminal groups capitalise on new technologies to identify targets and launch attacks on an industrial scale. If your business has not experienced a cyber-attack in the past year, you are in the minority.

Two thirds of mid-market/ large businesses have identified at least one breach or attack in the past 12 months, according to official statistics[1].

73% of companies surveyed reported losses of up to 25% of revenue following a cyber breach.

Mid-market[2] companies are particularly vulnerable. They're less likely to implement best-in-class cyber security than larger companies or to require their suppliers to do the same. Nevertheless, they have a level of resources that makes them an attractive target for criminals looking to extract a ransom, and a network of offices that makes fraud easier.

What a difference the board makes...

Any other scenario with the potential to disrupt operations, damage reputation and generate costs to this degree would be identified and managed as an important business risk. Despite this, most boards don't pay much attention to cyber security. In our survey, which was undertaken as part of Grant Thornton's International Business Report:

- one in three mid-market companies reviews cyber risk and management at board level or has a board member with specific responsibility
- around six in ten do not have a cyber incident response plan in place.

This needs to change – and there's a great opportunity for boards to make a real difference. According to the 2018 Cost of a Data Breach Study: Global Overview[3], the average cost per record lost in a data breach is $148. However, for every record lost, it was found that $13 would be saved, on average, through effective engagement by the board with cyber risk management, and the appointment of a chief information security officer.

This means that if a business loses 50,000 records during a data breach, board responsibility can save approximately $650,000 per breach. In our experience, breaches of over 500 million are becoming increasingly common. Effective leadership from the board helps ensure appropriate investment and focus on this important business risk.

Time for action

Now must be the time for boards to take action on cyber security. In this report we:

- explore the scale and nature of the threat
- examine the potential impact and cost of a successful attack
- look at where businesses are most likely to be vulnerable and how well they understand their vulnerabilities
- identify what action to take as a board to manage the risk and minimise losses
- assess which board member is best placed to take responsibility.

Cyber risk management, across people, processes and technology, is now a fundamental for every business striving to grow and prosper in a connected, digital world. No business – whatever its size or sector – is immune. Boards have a key role to play in ensuring an effective strategy is in place. This report explains why and how.

1 Cyber Security Breaches Survey 2018: Medium/large business findings, Department for Digital, Culture, Media & Sport, 2018
2 Companies with a revenue between £15m and £1bn.
3 2018 Cost of a Data Breach Study: Global Overview, Ponemon Institute, 2018

The growing threat: who's affected?

The changing scale and nature of cyber crime means every business is now a potential target. With 73% of companies surveyed suffering losses of up to 25% of revenue following an attack, no board can afford to ignore the threat.

A new era of cyber crime

It's easy to imagine that cyber criminals are all highly skilled tech professionals. This idea couldn't be more wrong. Today, unnerving as it may sound, anyone can become a cyber criminal. Online videos providing detailed instructions on how to prepare an attack are only a click away for anyone looking to become part of the new cyber crime wave. With many of the technical and knowledge barriers to planning and executing a cyber-attack all but gone, cyber crime is happening on an industrial scale.

Meanwhile, vulnerability identification software has made criminal groups more dangerous than ever. The software enables groups to trawl IP addresses and identify unsecured systems with ease. "It's the equivalent of thieves driving down a street to see who's left their door open," explains our head of cyber consulting, James Arthur. "Criminals exploit the vulnerable networks they identify or sell the list of promising targets on to others interested in exploiting the opportunity. If your defences are not up to scratch, your business could already be on a list."

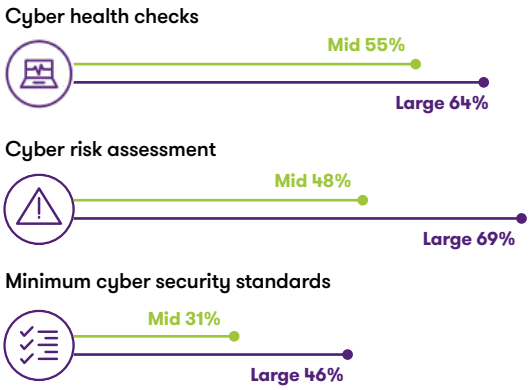
Cyber crime now represents a serious threat for every UK business. According to government figures[4], two-thirds of mid-market and large businesses experienced at least one breach or attack in the previous year. Our experience working with our clients is consistent with this.

"Whatever your sector, whatever type of business you are, assume that you are being targeted all the time. With the levels of volume cyber crime we are seeing now, you almost certainly are."

James Arthur, Partner and Head of Cyber Consulting, Grant Thornton

4 Cyber Security Breaches Survey 2018: Medium/large business findings, Department for Digital, Culture, Media & Sport, 2018

Figure 1. Mid-market versus large companies



Why every business is a target

Many businesses still believe they are below the criminals' radar. In truth, with the growth in cyber crime enabled by automatic vulnerability identification, every business is a target every day. It's not the nature of a business that attracts the interest of cyber crime groups. It's weak defences and the opportunity these present to mount a successful attack.

While the threat is real across sectors and for businesses of every size, mid-market companies are particularly vulnerable as shown in figure 1. Government figures[5] show they are less likely than large companies to carry out regular cyber health checks and are less likely to have conducted a cyber risk assessment. In addition, they are less likely to require their suppliers, whose networks can be a source of risk, to have minimum cyber security standards in place.

These figures show why criminal groups often prefer to target mid-market companies. While large businesses may have deep pockets from which to extract ransom payments, they also have the resources required to establish the strongest defences. By contrast, mid-market companies are still wealthy enough to be attractive targets but do not have the same level of resources to invest in defence.

How cyber criminals make money from your business

Ransomware

Attackers install software to shut down business systems or take the business offline. A ransom must be paid before the 'ransomware' is removed or deactivated. In a variation, attackers threaten to corrupt data and make it unusable if no ransom is paid.

Data theft

Attackers steal customer data and sell this on to other criminals to enable identity theft. Alternatively, they ask for a payment to release the data back to the business in a usable form.

CEO fraud

Online reconnaissance of publicly available data enables criminals to impersonate the CEO or finance director. Criminals can then request changes to payment details on invoices and divert payment to their own accounts. Government figures show impersonation is currently the second most common type of attack[6].

Bitcoin mining

A relatively new but increasingly common form of cyber crime. Attackers install software on the company's IT estate and hijack processing power to generate crypto-currency. Business systems slow down or grind to a halt.

IP theft

Espionage isn't limited to state actors. Industrial espionage is a real threat, with ambitious companies targeting competitors' systems to uncover and steal IP.

5 Cyber Security Breaches Survey 2019: Medium and large business findings, Department for Digital, Culture, Media & Sport, 2019
6 Cyber Security Breaches Survey 2019, Department for Digital, Culture, Media & Sport, 2019

Counting the cost

The financial impact of a cyber-attack can be huge. More than half of the companies from our survey reported losses equivalent to 3–10% of revenue following a cyber breach. As seen in figure 2, for businesses impacted most severely, losses were up to 25% of revenue – or £250 million for the largest companies covered by our research.

Businesses identify reputational loss, clean-up costs and management time as the three areas where they most expect to feel the impact as shown in figure 3. In addition, direct loss of turnover, customer loss or churn and customer behaviour change are all mentioned by more than one in three of the businesses we surveyed. Clients we have worked with post-attack often haven't predicted the time and cost impact to their business following an attack.

Reputational loss – how will customers react?

In a highly connected world, reputations built over time can be dashed in minutes when a cyber breach happens. Social media provides customers with a very public way to vent their disappointment and anger. Even if your business has insurance to protect against the cost impact of reputational damage, you must still face the reality that you have suffered a very public fall and face a steep climb back to being trusted by your customers.

Figure 2. What impact did this cyber-attack have in terms of revenue loss for your business?

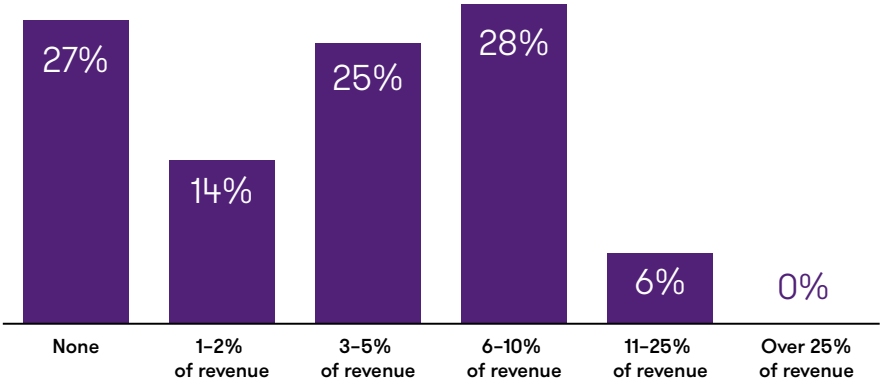
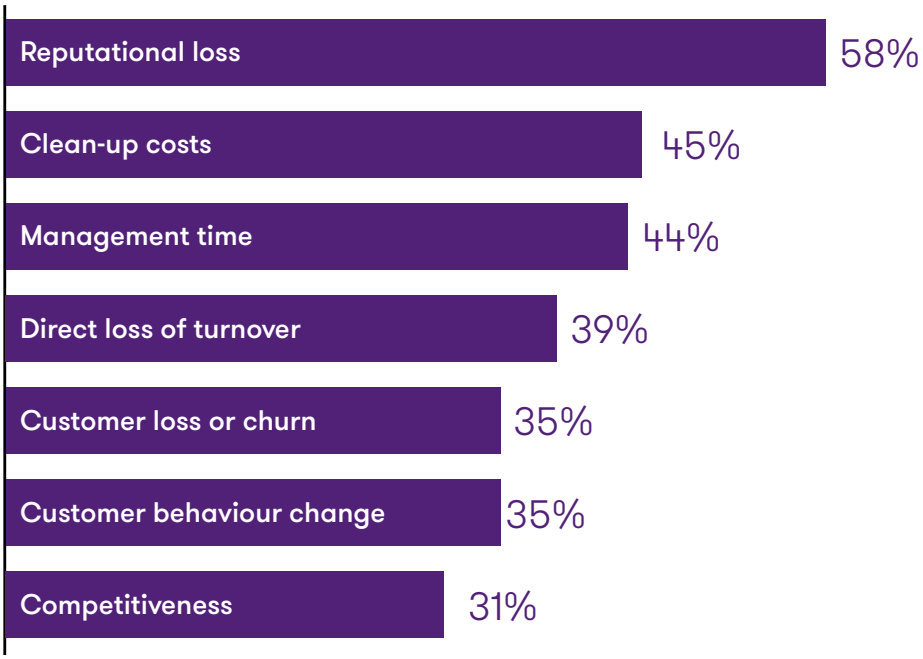


Figure 3. Most likely impact of cyber-attack



"The way we do business has evolved rapidly in the last 15 years. Although organisations have kept up to speed with the technological changes and customer requirements, cyber security controls often play catch-up."

Manu Sharma, Partner and Head of Cyber Assurance, Grant Thornton

The impact of reputational loss on customer behaviour is real, with customers often switching to competitor brands following cyber breaches. In the B2B space, the fall-out from a breach may not be quite so public, but is no less real. "When businesses cannot fulfil their contractual obligations because of a cyber breach, customers lose confidence and are likely to move to alternative suppliers," confirms our head of digital forensic investigations, Vijay Rathour. "Ultimately, this loss of confidence has a real and measurable impact on company value."

Clean-up costs

The cost of cleaning up after a cyber-attack is a huge incentive to invest in an effective cyber security infrastructure. Dealing with the fall-out from a data breach, for example, demands a range of expertise on a scale that most mid-market companies do not have in-house. This includes digital forensics (to locate, assess and repair the breach), law (to advise on regulatory exposure, contractual breach and liability) and PR management (to limit reputational damage). In the case of a data breach, a notification service to manage contact with customers whose records are affected, is essential.

We estimate that in the last 12 months, the total cost of cyber security breaches to UK mid-market businesses has reached at least £30 billion.[7]

These figures don't even take account of regulatory fines. Regulators are making organisations more accountable for the customer data they hold. New regulations such as GDPR and the Senior Managers Regime enforce significant fines when businesses are careless. "If a business cannot demonstrate that a good cyber security framework and controls have been implemented, the regulators will impose large fines to demonstrate that this is a serious failing and to set an example", says our head of cyber assurance, Manu Sharma.

A growing number of businesses are taking out cyber insurance to mitigate direct losses incurred as a result of a cyber-attack. Some policies also provide a team of professional consultants to support the business through the cyber breach.

Management time

The impact of a successful cyber-attack goes beyond the costs and reputational damage from business interruption. It also places a huge burden on the senior team, who will have designated roles in the incident response plan. During serious incidents, we typically see the CFO, the CIO and General Counsel committing 100% of their time until the crisis is resolved, and the CEO around 50%. Response activity may last for weeks, not days. The knock-on impact is considerable. Decisions are delayed and plans are put on hold as senior leaders' attention is diverted away from their day jobs. We see the effect spreading across the organisation, with employees losing confidence in the leadership team and pride in the organisation.

7 Estimates for the loss of revenue were generated by taking the total revenue of the mid-market in the UK (EIU) and Grant Thornton's survey data on the percentage of mid-market companies that faced cyber-attacks in the last 12 months and the average losses from these attacks.

Almost 70% of our respondents agreed ransomware demands are best handled by outsiders, and almost 65% think legislation would help.

Ransom demands: to pay or not to pay?

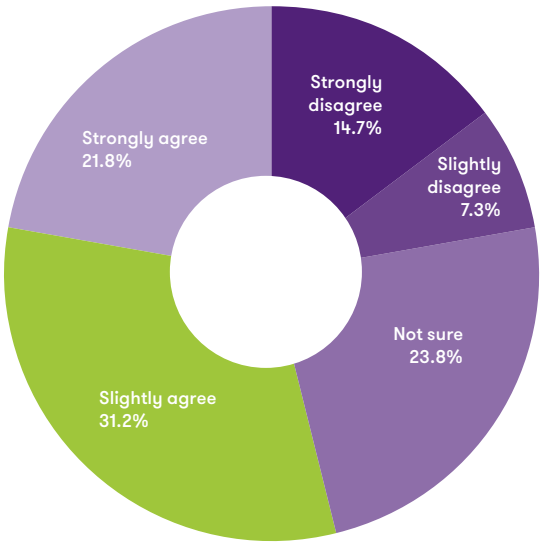
In 2018, ransomware attacks were the fourth most common type of cyber-attack on businesses[8]. In our survey, more than half of respondents told us they would consider making a ransom payment to get their data back.

The problem is that making a ransom payment marks a business out as a promising target for future extortion. In addition, there is no guarantee that, once a payment is made, data will be returned in a usable state. This is a difficult challenge for businesses.

As a result, there is a debate as to whether ransom payments should be handled by outside experts or government. Could putting demands for payment in the hands of experts improve the balance of power between hackers and targets? Could requiring businesses to report ransomware attacks by law help stop the volume of attacks snowballing?

Most businesses believe these two strategies could help. Almost 70% of our respondents agreed ransomware demands are best handled by outsiders, and almost 65% think legislation would help.

Figure 4. We would consider making a ransom payment in the event of the encryption or theft of company information

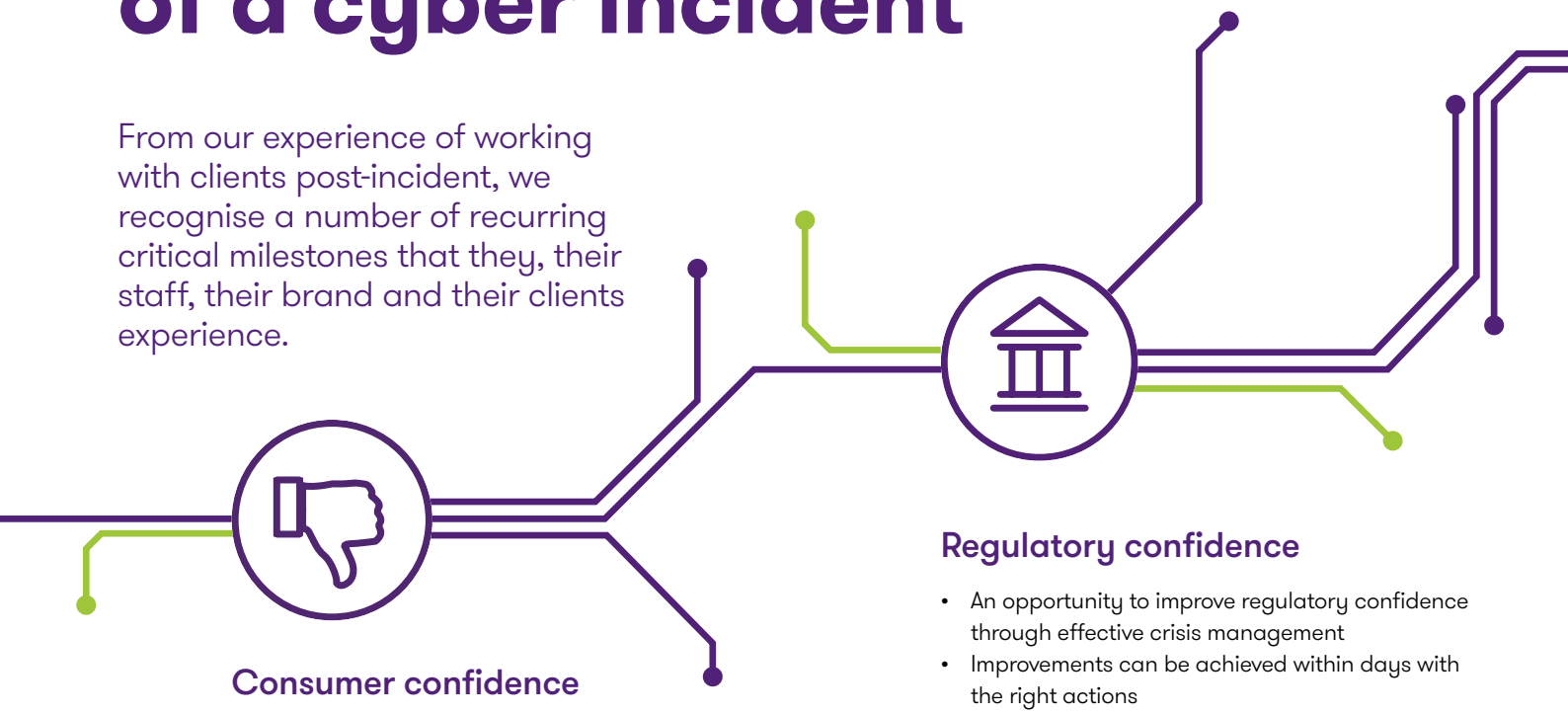


8 Cyber Security Breaches Survey 2019, Department for Digital, Culture, Media & Sport, 2019


Innovation
Branding
Solution
Marketing
Analysis
Ideas
Success
Management
Technology
Innovation
SYSTEM
Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec
Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec
Innovation
Branding
Solution
Marketing
Analysis
Ideas
Success
Management

Critical milestones of a cyber incident

From our experience of working with clients post-incident, we recognise a number of recurring critical milestones that they, their staff, their brand and their clients experience.



Consumer confidence

- Immediate change in behaviours as consumers switch to alternative providers
- Takes years to rebuild to pre-crisis levels

Regulatory confidence

- An opportunity to improve regulatory confidence through effective crisis management
- Improvements can be achieved within days with the right actions

Reducing the cyber threat: getting radical

With entire societies now dependent on connected technologies, some countries are taking radical action to reduce the cyber threat. Russia, for example, recently disconnected briefly from the global internet to test its ability to function if international sanctions are introduced that isolate the country online. Meanwhile, Uganda has imposed a social media tax of around 4p a day. This has reduced the number of internet subscribers by 2.5 million and, as a result, the number of people at risk of a cyber-attack. In China, the government uses a firewall to isolate the country's internet from the rest of the world, and so protect the network from the possibility of external cyber-attack.

In reality, there are often other motives for these measures. The Russian government's longer-term aim is to increase control over internet traffic by getting all domestic data passing through government routing points. In China, the firewall enables the government to prevent people from connecting to websites or services it disapproves of. Meanwhile, Uganda's social media tax was an attempt to raise revenue for public service. However, it has also been branded an attack on free speech and there are calls for it to be revoked.

Internal confidence

- Short-term damage to staff morale must be rebuilt over months and years
- Recriminations among senior team can damage strength of leadership longer term

Cyber risk capabilities

- Capabilities fall dramatically directly after a crisis
- Incident creates a chance to build steady improvements within weeks

Business and operational capabilities

- Decision-making typically paralysed in the short term
- Recovery to pre-crisis capabilities may take many months

"Every crisis provides an opportunity to prevent the same type of attack succeeding again. It's not enough just to fix the breach and get back to business as usual. There are lessons to learn and a chance to become stronger and better prepared in future."

Vijay Rathour, Partner, Head of Digital Forensic Investigations, Grant Thornton

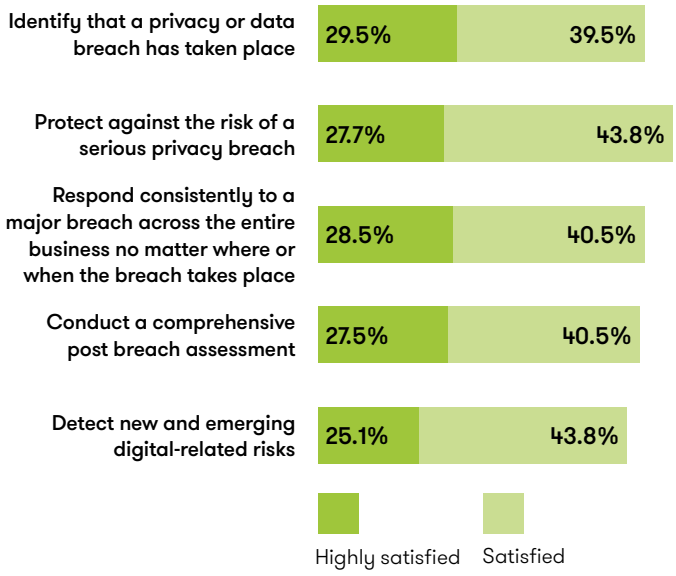
How vulnerable are you?

Businesses need to understand where their cyber security weak points are in order to counter the threat effectively. Our research reveals perceived and actual vulnerabilities don't always match up.

How good are your cyber management capabilities?

If you are confident in your cyber management capabilities, you share this confidence with most other mid-market companies. In our research, around seven in ten businesses said they were confident in their ability to protect against the risk of a serious privacy breach and to identify when a data breach has taken place. In many cases, however, this confidence is misplaced.

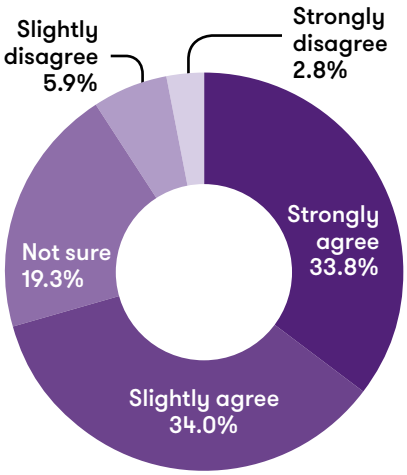
Figure 5. How satisfied are you with your organisation's ability to do the following?



Over two-thirds of respondents told us they could mount a consistent response across the organisation. Yet to do this requires having a comprehensive, up-to-date and regularly rehearsed cyber incident response plan in place. According to our research, only four in ten companies have such a plan.

Similarly, 68% of respondents told us they could detect new and emerging digital-related risks as shown in figure 5. Yet the same proportion don't believe their employees' security information is available for purchase on the dark web as shown in figure 6. These businesses have misread or are simply unaware of the danger from this growing digital risk. Our cyber security health check and ongoing monitoring of the dark web on behalf of clients typically indicates that four out of five organisations have sensitive data available for criminals to buy on the dark web.

Figure 6. I don't believe any of our staff login details are currently available to purchase on the dark web



Where are you most vulnerable?

Often, companies make themselves vulnerable to attack simply by failing to get the basics right – from changing passwords regularly to following protocols to keep sensitive information secure as it is moved between work and home devices. In addition, many companies are slow off the mark in responding to the fast-growing threat from volume cyber crime. Every business should be thinking about how their defences look from the outside, and running the same automated tools that criminals use to identify vulnerabilities in security. Our clients have seen huge benefits when we have undertaken this exercise.

The three areas that businesses themselves identify as key vulnerabilities are the supply chain, over-reliance on software to manage cyber risks and a lack of clear understanding among employees on which risks they are responsible for.

Is your supply chain a weak link?

Businesses underestimate their supply chain as a source of cyber risk. Among businesses that have not faced a cyber-attack in the past 12 months, only 33% mention it as a key vulnerability. But this view changes for businesses that have faced a cyber-attack in the past year, with 45% highlighting the supply chain as a source of weakness.

All businesses are required to know who has access to their systems for the normal purpose of data exchange, and must ensure that all partners and suppliers have effective controls in place. Partners and suppliers must always be required to follow normal security protocols before accessing the business's network. They must also be able to demonstrate that they have secured all cloud and internet-facing data stores, perhaps through the use of penetration tests and cyber health checks.

This type of risk is brought into sharp focus by the massive cyber-attack suffered by US retailer Target. Hackers found a way into Target's systems using security details stolen from a third-party vendor. As a result, they were able to acquire the payment card account details of more than 41 million Target customers.

Figure 7. When managing cyber and privacy-related risks, where are your key weak points?

Do you rely too much on software?

One in three businesses identified employees' over-reliance on software as a key vulnerability as seen in figure 7, with the proportion more or less the same among companies that have and haven't experienced an attack. They are right to identify this as an area of weakness. Security software, however expensive, is only effective when it is correctly configured, running on the right data and updated to cover the latest threats. There must always be someone in the loop – a trained responder – able to respond to alerts when they are triggered and there must also be a clear process for what should happen when alerts occur. On its own, software can never provide the best protection. This sounds like common sense yet 65% of businesses in our survey believe most of the work required to protect a company's data can be performed by a technology solution.

Do your employees understand their role?

The other area where businesses underestimate their vulnerability is in the role employees play in helping prevent a successful attack. For those businesses that had not suffered an attack in the past 12 months, less than 25% mentioned employees as one of their top three vulnerabilities, however this rose to approximately 40% for those businesses that had suffered an attack.

People are an essential component of an effective cyber security strategy and are often the weak link. Wherever it feels as if cyber security procedures are getting in the way and slowing things down, it's a natural instinct for employees to find a work-around. In many cases, they are unaware just how significant the cyber threat now is and, equally, unaware of how key their role is in helping the business stay protected.

Training to raise employee awareness has a hugely positive impact on cyber security, but changing behaviours is difficult and the threat is always evolving. This means training needs to be regular and ongoing. Despite this, more than six in ten businesses told us they had not provided all members of staff with cyber security training in the last 12 months.


WORD

Board leadership makes the difference

Putting cyber risk onto the board agenda is one of the most effective ways to minimise the chances of a successful attack and reduce the financial impact if a breach occurs.

The neglected business risk

The growing threat, combined with the significant potential losses from a breach, makes cyber crime an important business risk. But many boards are ignoring the danger. More than six in ten of the companies we surveyed say no board member has specific responsibility for cyber security. And in roughly the same proportion of companies, the board does not undertake a regular formal review of cyber security risks and management.

Why are so many boards ignoring this risk? In some cases, it is because board members are not fully aware of the severity of the threat from the current wave of industrial-scale cyber crime. This lack of understanding may go hand in hand with the lack of confidence many business leaders have in their ability to address the challenge. The temptation is to file cyber security as a technical issue and trust someone else is picking it up. This approach leaves the business exposed just as organised crime groups are ratcheting the risk up to a new level.

Figure 8. Which of the following statements are applicable for your organisation?

41.1%

We have a cyber incident response plan

37.3%

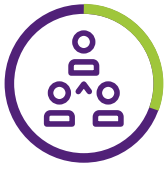
The board formally review cyber security risks and management

37.1%

There is a board member with specific responsibility for cyber security

35.6%

We have provided all members of staff with cyber security training within the last 12 months



30.6%

Within the board, there are individuals with prior experience of overseeing cyber security in a similar organisation

"Cyber risk needs to be considered just like any other business risk. What are the chances of it happening? What will the impact be? And how can we mitigate against it?"

James Arthur, Partner and Head of Cyber Consulting, Grant Thornton

Reducing the impact of cyber crime

We know from experience that boards can make a real impact on reducing the likelihood of a successful cyber-attack and in minimising the reputational and financial impact when a successful attack occurs. Our research is consistent with this, showing three distinct areas where action by the board changes outcomes for the better.

Review cyber security risks and management at board level

Prepare an incident response plan

Make cyber security the responsibility of a specific board member

Review cyber security risks and management at board level

Scheduling a regular and formal review at board level puts cyber security on the board agenda and ensures the issue receives the focus and investment it requires. Companies that do this suffer lower financial losses in the event of a successful attack.

Among the 38% of companies that do review cyber security risks and management at board level, the frequency of these reviews varies. In one third of companies, formal board review takes place twice a year, while in just over a quarter it takes place four times a year. One in five boards complete a review three times a year.

Prepare an incident response plan

In responding to a cyber incident, a well-rehearsed plan of action can help business leaders act to manage a highly stressful situation quickly and more effectively, minimising business interruption and negative impact. According to the 2018 Cost of a Data Breach Study: Global Overview[9], having an incident response team in place was the factor found to most decrease the per capita cost of a data breach, saving $14 per compromised record. Time is important. When an organisation is haemorrhaging data or customers are providing a running commentary on service failure on social media, minutes and even seconds count.

9 2018 Cost of a Data Breach Study: Global Overview, Ponemon Institute, 2018

Our research shows that companies that have an incident response plan in place experience lower financial and reputational losses in the event of a successful attack than those that don't. Despite this, almost six in ten companies don't have an incident response plan.

An incident response plan should cover the full life-cycle of a data breach – from discovery, to resumption of business as usual, to lessons learned. Our recommendation is that it should be rehearsed with a full simulated cyber attack twice a year.

"A serious breach creates a level of psychological stress that it's almost impossible to prepare for. A pre-prepared incident response plan allows the business to do the right thing as fast as possible when every second counts."

Vijay Rathour, Partner, Head of Digital Forensic Investigations, Grant Thornton

Make cyber security the responsibility of a specific board member

Making cyber security the responsibility of a specific board member helps to stop cyber risk management slipping through the net. Our research shows that companies that appoint a specific board member suffer lower average losses in the event of successful attack than those that don't.

Figure 9. You said you have a board member with specific responsibility for cyber security. What is their position?

31.2%
Chief Information Officer (CIO)

23.3%
Chief Technical Officer (CTO)

15.9%
Chief Executive Officer (CEO)

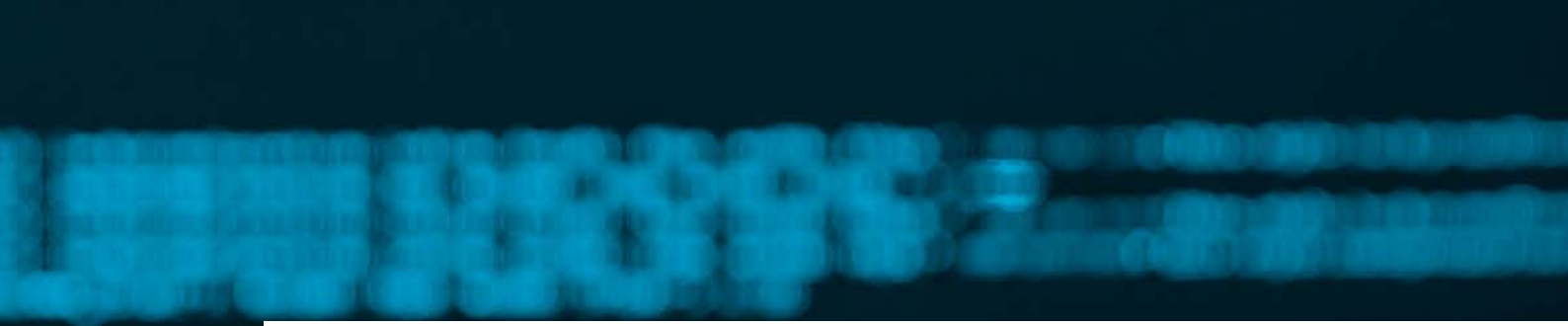
15.3%
Chief Financial Officer (CFO)

8.5%
Chief Strategy Officer (CSO)

3.2%
MD/Chairperson

Companies most frequently choose the Chief Information Officer or Chief Technical Officer to fulfil the role. Yet, in our view, it's worth considering a different board member, without any particular technology specialism. The Chief Financial Officer would be a good choice. In most mid-market companies, it is the CFO who is typically responsible for risk. Making cyber security their responsibility underlines the fact that cyber risk is a business risk, like any other, that needs to be managed.

There is a further advantage. In business, there is often a natural tension between operational targets and cyber security targets. Should the priority be to minimise interruption to operational systems (and therefore limit or delay software updates)? Or should maximum security be the priority, even if frequent updating means users cannot access business systems for hours or sometimes days? A board member who is neither the COO or CIO has the benefit of a degree of distance on the debate and is perhaps positioned to find a better balance.



"Your staff will know what to do if they discover a fire, but do they know what to do if they discover malware in their application? Emergency response principles apply – raise the alarm and remove the danger. When was the last time this drill was practised in your organisation?"

Manu Sharma, Partner and Head of Cyber Assurance, Grant Thornton

Achieving operational resilience

Resilience is the ability to absorb shock and bounce back. Effective cyber security enables your business to do just this, establishing an operational capability to manage inherent risks (absorb shock) and respond in the event of a residual risk event occurring (bounce back).

The process is one of continual improvement, focused on reducing cyber risk to an acceptable level, whether through policy, procedure, hardware, software, training or culture change. Once the top ten inherent risks have been mitigated, the next tranche can be addressed.

How to bounce back

Bouncing back begins with your incident response plan. This defines the sequence of actions that should be followed in the event of a cyber or data breach. At their most basic, these are: raise the alarm, contain the threat, secure the site, escalate the response. Anyone involved should proceed under the guiding principle, 'don't put yourself or others at risk'.

Once the alarm has been raised (ideally within seconds of an event), the crisis management phase begins. The first hour is the 'golden hour' when effective action can dramatically reduce the damaging impact of the event. The crisis management team convenes and uses command, control and communications to stabilise the situation. Only then should business continuity be invoked for critical business functions, and IT disaster recovery launched to continue or recover critical applications.

Taking control of cyber risk in your organisation

At a time when business is more connected and more digital than ever before, cyber crime is an integral feature of the risk landscape. The significant financial and reputational impact of a successful attack means every board must step up to address the threat. Mid-market companies are more at risk than the largest players.

Reviewing cyber security risks at board level and appointing a board member with specific cyber responsibility are key actions your business can take to reduce losses from any future breach. Once these arrangements are in place, where should you focus? Here are some questions you may want covered on the agenda of your next board meeting.

Incident response plan

Your incident response plan should allow you to respond effectively to a range of scenarios, such as an internal breach, external attack, accidental data sharing and loss or theft of a physical device.

- Do you have an incident response plan in place?
- Who will lead the incident response team?
- What will happen in the first 24 hours after a breach?
- Have you allocated enough resources to ensure an effective response?
- What external partners will you use to manage elements such as forensic investigation, public relations, legal affairs and the notification process in the event of a data breach?

Rehearsals

Practice makes perfect so your business should be rehearsing the incident response plan regularly. Using scenarios is a highly effective way to enable different levels of responders to practise, from individual staff members and end users up to multinational teams affected by the same cyber event or data breach.

- When did your business last carry out a scenario-based rehearsal?
- What were the key recommendations in the follow-up report?
- Have the recommendations been acted on to improve security? How?
- When is the next rehearsal?
- Will it incorporate and elaborate on the lessons learned from last time?

Supply chain

Press coverage of major data breaches resulting from suppliers' inadequate cyber security is not hard to come by and makes for a sobering read. Check your business has this source of risk covered.

- Who has access to your systems and where is this information recorded?
- What controls do your suppliers/partners have in place? Are their controls weaker than your own?
- What security protocols must suppliers/partners follow before accessing your network? How can you be confident they are doing this?
- Can suppliers/partners demonstrate they have secured all cloud and internet-facing data?

Insurance

While insurance will not cover the fact that you've suffered a very public fall - it can limit financial losses and support you during an attack.

- Does your business have insurance against cyber losses?
- Does your insurance cover all the potential sources of loss?
- Are your calculations on potential losses realistic?
- Does your policy include provision for expert support through a breach?

Staff training

Investing in training and raising staff awareness of the cyber threat often delivers a significant uplift in security. But the challenge of making lasting change to behaviours means training must be ongoing.

- What staff training has taken place in the past 12 months?
- What proportion of staff have received training in the past 12 months?
- Have you tested staff to check the impact of training?

Establish a baseline

Understanding what 'normal' looks like for your business, in terms of application usage, network traffic and external connections, and being able to recognise unfamiliar patterns, such as an increase in activity for specific protocols, provides a valuable head-start in responding to an attack.

- Does your organisation monitor normal activity to detect any changes?
- Have you invested adequately in up-to-date monitoring tools?
- Who is monitoring the alerts triggered by these tools?
- Who is responsible for responding to the alerts triggered by these tools?

About the research

This report is primarily based on over 500 interviews with UK business leaders during October and November 2018. All of these businesses had revenue between £15m and £1bn and came from a variety of industry sectors. The research was undertaken as part of Grant Thornton's International Business Report, which surveys around 10,000 businesses annually across more than 30 economies. Fieldwork is undertaken on a biannual basis, and online and telephone interviews are conducted with board and senior leaders, not limited to but including: chief executive officers, managing directors and chief financial officers.

Our cyber capability

We offer an integrated suite of cyber security services, supporting end-to-end cyber consultancy, design, pre-emption and protection. Our services include:

Service	Overview
Cyber risk and resilience	Provision of expert consultancy advice to identify and manage cyber risks in a clear and understandable way and improve clients' cyber resilience across people, processes and technology.
Cyber health checks	Provision of cyber health checks ranging from combining both empirical evidence and guided assessments against UK Government best practice through to ISO27001 readiness assessments.
Cyber security design	Provision of expert cyber security advice to plan specific improvements to cyber security defences, this could range from security policy advice to complete security and network architecture redesign.
Cyber security implementation	Implementing improvements to cyber defences for clients, this could range from improving existing systems to full new defences incorporating improvements to people, processes and technology.
Cyber awareness and training	Provision of tailored cyber awareness and training ranging from bespoke C-suite training, apprenticeship levy funded internal cyber talent identification and development and companywide training.
Cyber risk monitoring	We offer a range of cyber risk monitoring solutions for our clients ranging from regular external vulnerability scans, dark web monitoring through to active monitoring of our clients' networks for proactive identification of attacks.
Threat hunting	A focused investigation on the client's networks to identify if they have any active malware or other evidence of ongoing cyber security breaches using forensic investigation approaches.
Incident response and remediation	Working with our clients to contain and eliminate active cyber-attacks on their systems and networks and to return them to live operations as soon as possible.
Digital forensics and investigation	Forensic acquisition of data post-breach and detailed investigation of incidents to identify the source of infections, including reverse engineering of malware and attribution of attacks where possible.
Cyber standards assessment	Assisting our clients to assess their level of conformance with a range of international standards such as ISF, ISO27001, NIST and identifying improvement plans if required.
Penetration testing	Human-led penetration test of a client's networks and ICT infrastructure that is designed to simulate the Tools, Techniques and Procedures (TTPs) used by current hackers.
Supply chain monitoring	Monitoring the cyber security posture and threat level of organisations involved in our clients' supply chains. Options range from external only monitoring through to regular internal scans and regular confirmatory testing.

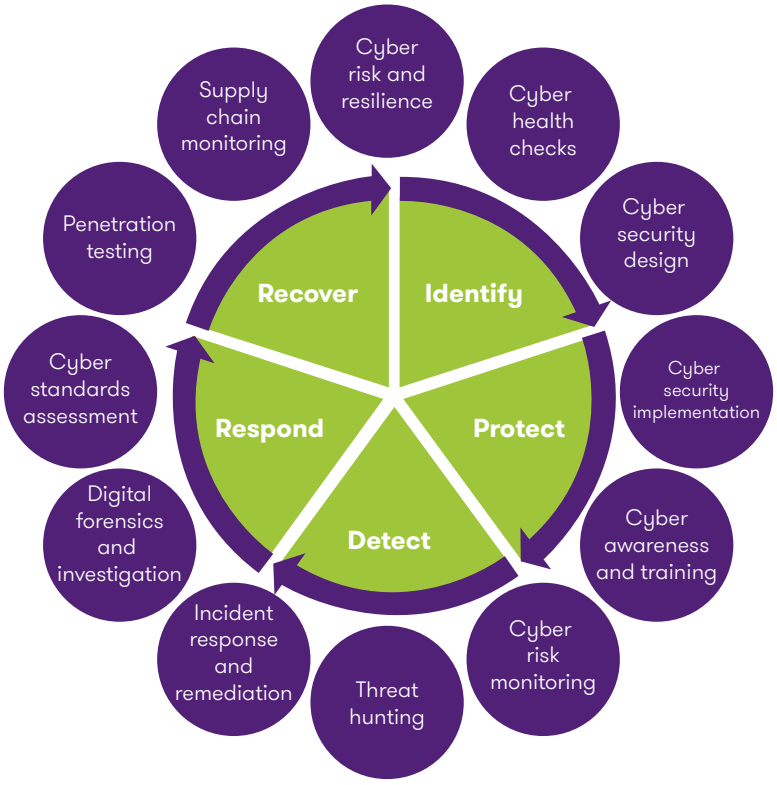
Our services

We support clients across all industries and sectors with their cyber risk. From assurance, to incident response management to full scale design and implementation of cyber security processes.

We can assist you to identify potential risk. We can provide you with the information you need to make informed commercial decisions to either maintain or improve your cyber security and allow you to manage your organisation with confidence.

Our team have years of experience in providing pragmatic cyber solutions having worked on projects ranging from helping a 17 person business address their highest priority weaknesses through to designing, installing and operating national scale cyber defences to secure entire countries.

Visit our cyber hub to read our latest insights and to find out more about our services
grantthornton.co.uk/cyber-security



Contact us

James Arthur
Partner, Head of Cyber Consulting
T +44 (0)20 7865 2969
E james.ag.arthur@uk.gt.com

Vijay Rathour
Partner, Head of Digital Forensic Investigations
T +44 (0)20 7184 4684
E vijay.rathour@uk.gt.com

Manu Sharma
Partner, Head of Cyber Security Assurance
T +44 (0)20 7865 2406
E manu.sharma@uk.gt.com

Grant Thornton

An instinct for growth™

grantthornton.co.uk

DS746