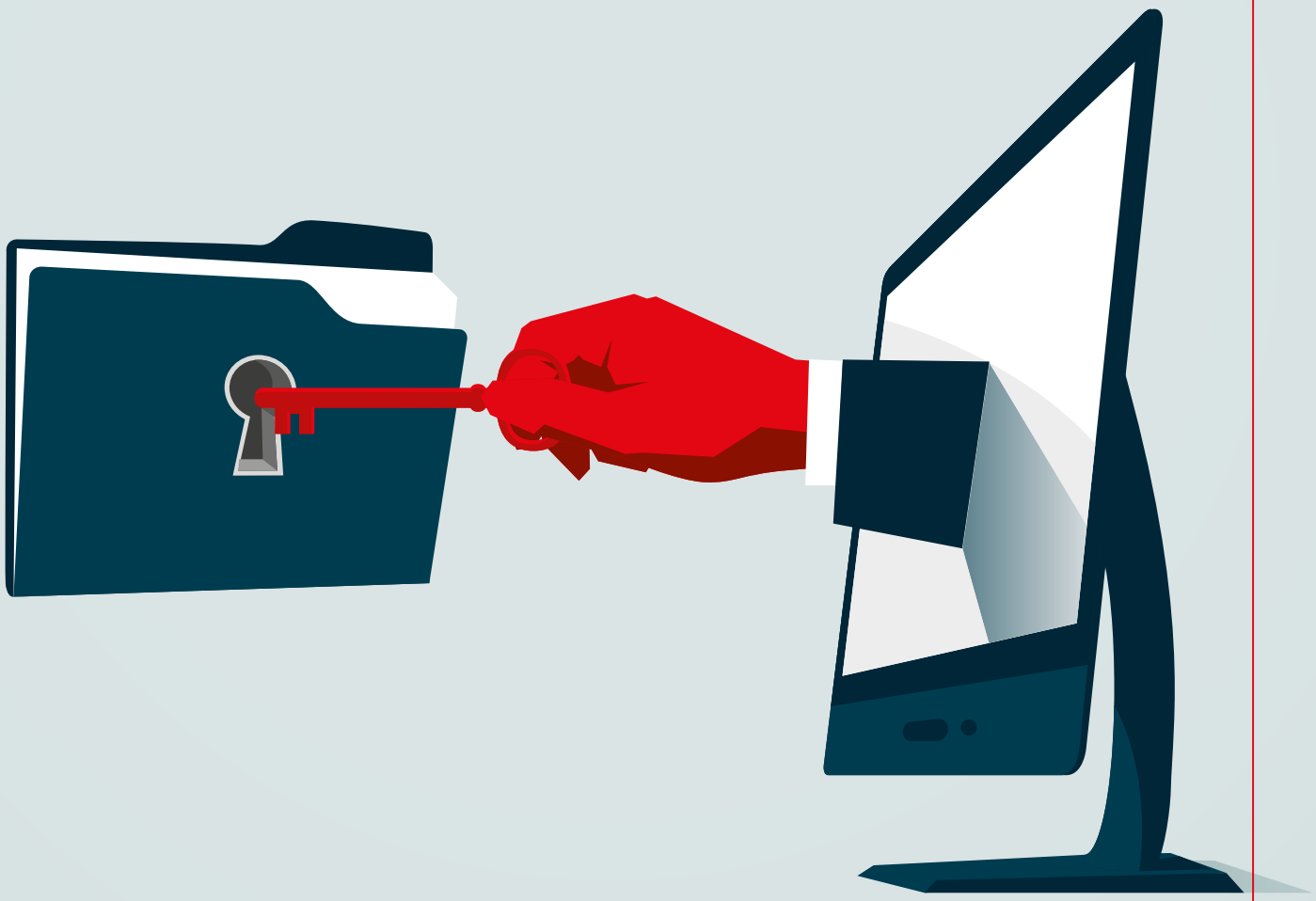
OpSec Alert:

CFO's Top Secret Guide to Cyber Security

(What Bad Looks Like & How to Prepare for It)



Think Ahead

Contents

Primary research taken from ACCA Global's Professional Insight Report:

Cyber and the CFO - in association with Macquarie University and Optus, Chartered Accountants Australia and New Zealand.

May 2019

Executive summary

Without the basics, you don't stand a chance.

Welcome to cyber-bootcamp. You're here because you know something. You also know that what you know is valuable and that by not continuing to learn, you'll destroy your business. Wreck lives. Annihilate the reputation of yourself and those around you. The problem is, what you need to learn is changing every day. Hidden. Morphing. All at once close yet tantalisingly out of reach. And the fact is, you're far from alone in dealing with this truly global issue. When you start to look at the numbers, they're staggering.

One prediction by Cybersecurity Ventures estimates that the cyber-crime economy will be worth $6tn per annum by 2021, representing one of the greatest transfers of wealth in human history. How do you start to count the cost of such a phenomena? In terms of data-loss? Monetary loss? Loss of production? Or maybe it's the cost of clearing up the mess. And if you've got the letters CFO or CEO anywhere near your name, you also happen to be the target-in-chief. Ironically, you're your own worst enemy. Nonetheless, the boardroom are without a doubt looking to you to provide leadership.

So, what are the basics? Well, primarily that assumption and passivity are the main enemies of cyber security. If you think someone else has it covered, you'll fail. If you're the type of person who doesn't double-check that you've locked the door when you leave your office, or look over your shoulder when you enter your PIN, you'll fail. In fact, you'll probably fail anyway. If, but more likely when it happens to you, it's probable it won't even be your fault, at least not directly. You've got to be responsible for everyone and everything associated with your business. Every external contact. Every click. Every memory stick. It's called the Zero Trust model… and that also includes senior management.

And what about the new IT hire who's there to show you the ropes... seems nice enough, right? What's the cost of not properly vetting him or her? How do you create resilience against that kind of internal threat? What's your cyber-insurance premium? What's your governance framework for DDoS? Crypto-jacking? Smart-phishing? Botnets? Malware? Man-in-the-middle attacks? Phone-porting? Regulatory extortion? Artificial intelligence that can imitate your voice? That work phone you unlock with your face… 'deep fake' technology can do the same with pictures or videos of you. Maybe you could just keep your face covered up while trying to prevent copies of it appearing online. That's bound to do wonders for your business.

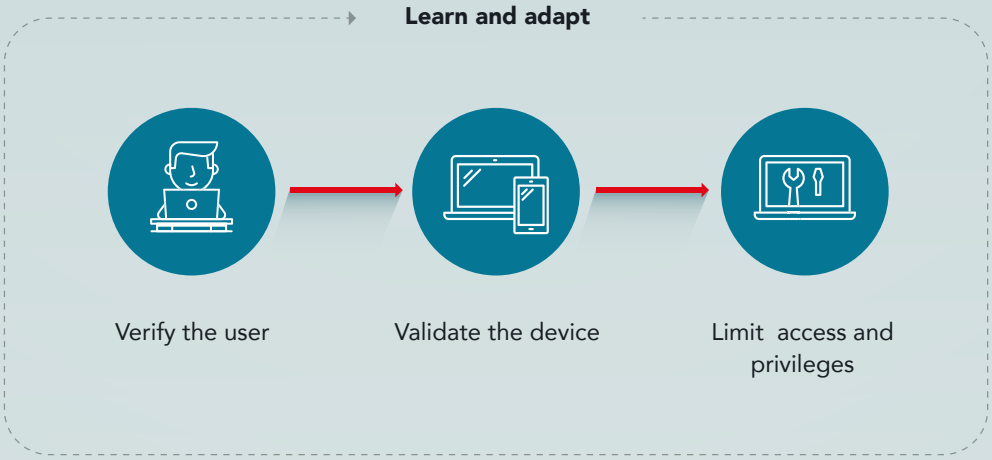
Not knowing everything isn't ignorance. But the scale and types of cyber security threat are growing and evolving at an alarming rate. If you don't **start preparing** it's game over, with no extra lives.

The reality is that you will almost certainly experience a cyber-attack, eventually. Your team needs to be highly aware and trained. That's where the ACCA comes in from both a knowledge-base and resource provision perspective. You need people that can grasp the opportunities that digital finance trends provide, while being able to counterbalance the risks and resource requirements. Indeed, the commercial risk of not engaging with new technology and hiring the staff to manage it seriously increases the likelihood of your company falling behind. Your choice is simple, engage in a meaningful way or fade into obscurity. In this arms race to maintain a competitive edge, it's about having the right people by your side. And we'll always be here, thinking ahead.

Ultimately though, everyone in your organisation is individually responsible to stay up-to-date, despite it being your responsibility to make sure they are. Technicians need to understand financial risk. Financial operatives must learn from the computer guys. Call it awareness or paranoia, but this danger isn't going away. It's no longer about firewalls. It's increasingly about authenticating the user. And if you think running a small business keeps you safe, you're wrong. You're still a target. If anything, you're easy pickings. Regardless of your industry or the size of your market, it's do or die. Your suppliers are under fire, which means you're under fire. 24 hours a day. 7 days a week. The threat never sleeps. And fortunately for the hackers, you do…

Yet fear not, we're here to demonstrate that you still stand a fighting chance. Not only that, you can thrive in this world, it's just a matter of preparing for the worst and even more importantly, knowing what to do when it happens. So, switch off your phone. Air gap your machine. Cover your camera. Get ready to take on some new terminology and analysis, the type of information you're going to want to take back to the board. We're about to deep-dive into the secretive domain of cyber security and the measures your business must take to survive.

The Zero Trust Model



Risks

Know your enemy.

Think about your day so far. How many times have you been put at risk or worse yet, compromised? The fact is, you probably don't know entirely. The number will vary, depending on your definitions. This section will aim to equip you with a broad view of the key risks to your business, covering the typical attack vectors associated with a breach. Think of it as a default operational checklist. With this kind of primer, you will be able to further your own cyber security remit, in order to relay suggestions for immediate change to the key stakeholders on your board and across your wider business network.

The most critical starting point is the data and assets connected to the information systems and computer networks you use, including those connected to your suppliers' and clients' critical systems. Are you questioning where these assets are located? What is the hierarchical importance of different data-types within your organisation? How do your suppliers and clients manage their systems? It might be something appearing useless which is very useful in preparing a cyber-attack. It's also essential to create an inventory of all of your devices and applications. Ensure all relevant security patches are applied, and advise your suppliers and clients to do the same. You're always ready until you're not. Don't use perimeter security as a solution to persistent internal weakness. It's a common problem, but it shouldn't be yours.

That said, it's still necessary to defend against outsiders who are constantly probing, particularly via web application weaknesses. Much of your IT management is likely to be through the cloud, and while that shifts operational duties, it does not transfer financial, reputational or legal responsibility. Outsourced providers' security is part of your own setup and should be subjected to the same degree of due diligence. And that applies to remote workers, too. It's essential to ensure that their mobility doesn't compromise your internal systems. A network, particularly a mobile one, is only as secure as its weakest link.

At a simple level, compromised data can be used directly for financial gain, blackmail or as the basis for social-engineering and phishing. For clarity, these terms imply using psychological trickery in order to garner a specific response, such as clicking of a link by a target user. However, rather than stealing data, criminals will often simply alter data so that it becomes damaging by being inaccurate, misleading or even incriminating. A basic example would be altering supplier payment details or creating inflated bank balances, but could even inflate share values… or crash them. Imagine if your social-media team's Twitter feed got hacked to announce the CEO's death, or some other similarly negative event. How might that affect your market value? What would the value be to someone that had prepared a large buy order, following the inevitable dip?

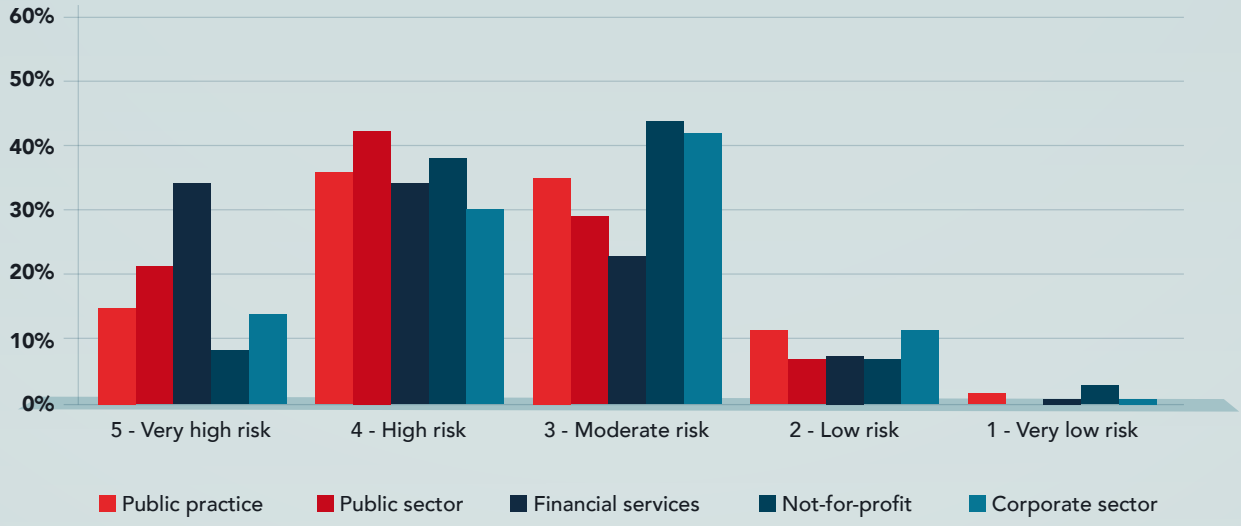
How can you fight an enemy if you don't know which way it's coming from? Only by understanding the risks and **asking the right questions** can you start moving towards a position of readiness.

The risks are manifold. It's no longer just a virus being uploaded to internal systems by some malicious actor. You must be aware of each point of failure and what the fallout might be. And remember, it's as much about your own company data as the 'big data' you hold for your customers. Data protection rules don't apply to anonymised data shared with third parties. However, poorly anonymised data can be 'de-anonymised', particularly when combined with other data, and compromising individuals' privacy carries heavy fines under data protection legislation, such as the EU's General Data Protection Regulation (GDPR).

That takes us briefly into the realm of Open Source Intelligence (OSINT). Telephone directories, electoral registers, company websites and social-media all host a wealth of data to be used as the basis for a cyber-attack, either on its own or combined with other data. Your employees are likely users of sites such as Facebook and LinkedIn, and can therefore post details, like photographs, which compromise security. Be generally wary. Limiting what is shared on those channels, indeed the extent to which those channels should be used for sensitive information sharing, should be qualified and quantified.

Remember, a single breach is all it takes to bring down the whole system. Breaches often result in the loss of login credentials: lists of paired usernames and passwords. Because so many people reuse them on different sites, attackers simply test these lists until they gain access to a critical account. This underlines the need for strong password policies and user awareness. Use long-strings. Different cases. Alphanumerics and symbols. Consequent to this trend, the model is being replaced by multi-factor authentication, which will dynamically ask for different levels of authentication according to who the user is, what they are doing, and how they are connected. With the assistance of properly trained and accredited operatives, it's your duty to enforce these best-practices across the business.

How does cyber security rank as a business risk in your organisation? Analysis by sector.



Errors

Learn from their mistakes.

It's important to look at how others prepare for crisis in order to build resilience for yourself. It's also worth knowing how things go wrong for others, to signal what not to do. Sure, some things are intuitive. You may find yourself reading the following insights and thinking 'we already do that' or 'we'd never let that happen'. But, of course, it's easy when hindsight is 20:20. When you're in a situation, you may find your judgement being clouded by the debris of spontaneous factors outside of your control.

Case-studies ought to become part of your weekly digest of material, as they crystallise human error in a way that is based in translatable narrative, rather than the realm of pure protocol and directives. It's often the emotional trigger of a third-party's failure in a particular situation that allows you to respond at the speed required for a cyber security breach. When things break, it's typically the human response you're likely to remember.

Let's start with the process of protecting revenues through sharing and cooperation. For one airline CFO, cyber security is "right at the top of the risks to the business", with over 90% of bookings coming through the online portal. For the airline industry, revenue is the critical risk, rather than profit and margin. If customers cannot, or rather feel they cannot use the web platform, then revenue will drop significantly. The consequences of a data-breach and loss of credit card details could be worse than a denial of service attack.

Therefore, the organisation spends a lot of time in discussion with MasterCard and Visa to ensure they are meeting the standards of their financial services partners. It takes part in discussions hosted by the International Air and Transport Association (IATA), ensuring they are up-to-date on knowledge sharing events with other members. IATA also supplies education and training to staff, going far beyond what the company could achieve using their own resources. Internally, one IT team member is dedicated to cyber security, supported by consulting and monitoring software firm Darktrace. Cross-departmental reporting ensures that they share issues and provide weekly briefings on cyber security to departmental group-heads.

For this firm, cyber security is an IT issue at the operational level, but quickly escalates to the CFO who has overall responsibility. From the CFO it goes to the Audit Committee, then the Board, who review cyber security on a monthly basis.

There's no point waiting until it happens to learn the lessons. Make time to **actively research** what other companies in your sector are doing, and how they may have responded to previous attacks.

For all of this, the airline suffers an average of two attacks a year, with three occurring in the last year. Company employee activated malware entered the network demanding a ransom to restore access. In each case, the IT team were able to ring-fence the malware and restore the missing files.

Nonetheless, data-breaches and downtime have a domino effect, disrupting engineering and flights, forcing people to revert to manual systems. Recovery is as important as prevention. The Finance department needs to ensure not only that revenue is protected, but that system repairs don't damage its reporting capability. Accountants are now as aware of the need to protect data as they are of their role in processing it. Because finance is always at the frontline of IT attacks, it has generally assumed control of IT to ensure it reflects its security needs. The upshot is investing in staff who know what those needs are, the keyword here being 'investing'.

Of course, there will always be human error. Noting one instance, the global CFO of a public company is concerned that CFOs are too focused on protecting internal financial data and fail to protect against losing money. He gives this example of how one such breach occurred. A third-party professional services firm was tasked with distributing the login details to a critical piece of accounting software to the company in question. In failing to do their jobs correctly, it transpired that they shared it with a much higher volume of staff than was necessary, and unfortunately one of those staff members became the target of a phishing attack. Before the attack was detected, the criminals had changed all of the first payment details for suppliers and employees, and collected all the due owed in the next payment run. Classic theft by stealth. The company only found out about the breach from people who hadn't been paid. Embarrassing in the least, yet reputationally damaging in the extreme. This also highlights the importance of ensuring that supplier processes are as secure as you expect yours to be.

The main takeaway is that all of these breaches were rooted in human error. This means that company-wide policies and procedures have been changed to make practices like using external applications and changing payment details more secure. The companies also outsourced some processes, and therefore data, to specialists who can better protect it, while sharing intelligence with the wider network. In the instance of your company, it will be worth making these types of changes before the inevitable happens, and ensuring you have the best possible personnel on-site to cope when it does.

When was your company last subjected to a cyber-attack? Analysis by all respondents.

Governance

You're only as good as your people.

You need a cyber-governance framework for your organisation. As CFO, you should be able to participate in a robust discussion about cyber security with your board, the wider organisation and outside stakeholders. In 2019, it's a core responsibility to promote these kind of discussions. As we're now discovering, some of these conversations will not be entirely technological. Certain powers need to be delegated to Finance, which will have the skills to oversee audits, inventory, testing and compliance, and which in turn will lead to the assessment of cyber-insurance. In the event of an attack, the CFO and their team will invariably be the first point of call in assessing the damage, leading on internal and external actions, while controlling communication with relevant stakeholders.

But it's not only financial data under siege. Finance personnel will be targeted directly in an attempt to steal and defraud. Therefore, as a key part of these discussions, CFOs must engage with IT to ensure that their own vulnerabilities are understood and addressed. Yet to reiterate, leaving it all to IT is not enough. While IT teams may be part of the solution, they are not the owner of it. It needs to be a cross-organisational activity, not a technical remedy.

Don't be trapped behind a complex subject and remember that education is one of the greatest defence mechanisms you own.

While one might expect IT to be reasonably abreast of the threat landscape, it is unreasonable to expect them to demonstrate an equal understanding of the risk as it pertains to each sector and each part of your business. Unless the business engages with IT and articulates the true nature of the risk, and the organisation's risk appetite, there is a danger that IT will waste resources protecting assets that pose little or no threat.

Also remember that cyber security is a commercial risk. Responsibility for managing it cannot just be outsourced or delegated. Managing cyber-risk means that CFOs need to engage closely with IT professionals to develop a common language, rather than seeing them as 'the geeks around the corner'. While the language of cyber-threats can seem arcane, the consequences are real. Even if they don't become cyber security experts, CFOs must ensure they are not just managing the risks they understand.

Cyber security is not a one person job, and while the responsibility is on you, your first battle is to **relevantly communicate** the importance of the issue to staff and to ensure correct training.

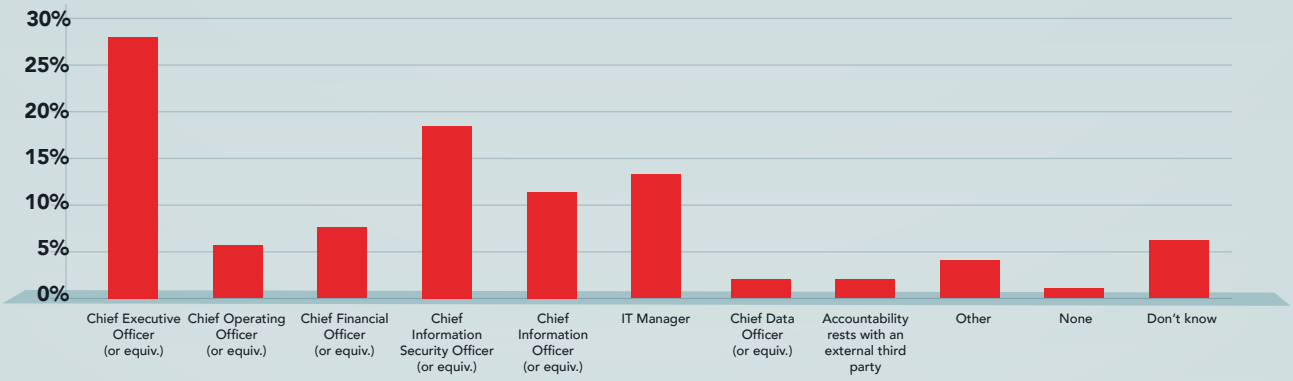
It's clear that for your company at large, cyber security will seem like an inherently daunting topic. The technologies of both defence and attack can be complex and the jargon can be impenetrable. But the threat only exists in a wider context of human behaviour and corporate culture. CFOs don't need to become technical experts, but they will serve their organisations by being aware of the range of threats, and being able to deliver critical insights to relevant teams. It's about thinking carefully about how information is tailored to specific departments, so that non-technical staff don't feel unable to engage.

Therefore you must start asking yourself these types of questions: does the board understand its exposure to cyber-attacks from both inside and outside the business, and the extent of the digital connections that it has with suppliers, customers, and the outside world? What are the vulnerabilities of the organisation to cyber-attacks, and what are the risks of them occurring? What are the likely business outcomes of a breach, including revenue loss, business disruption, crisis management, regulatory and recovery costs?

What is the planned response to a cyber-attack, in terms of technical resolution, business disruption, reputation management and regulatory response, and in mitigating knock-on effects outside the business? What capabilities does the organisation have to manage cyber security risks and deal with incidents? How can the organisation collaborate and share information with regulators, peers, law-enforcement, suppliers, customers, trade bodies and other stakeholders? How often does the organisation's cyber security readiness undergo review and testing? Who does the testing? Who is responsible for reporting on cyber security, both during an incident and on a regular basis? How often should there be board discussion on cyber security?

Once you start answering these types of questions, and formalise that response into an official cyber-governance framework, you will be closer to building the type of resilience required. Being able to share top-level insights with trusted stakeholders will build trust in your own business. They will feel safer in working with you, knowing you are secure in your attitude to this threat. Additionally, the knowledge that your staff are credible enough to deal with any potential scenarios in a sensitive and efficient manner, according to their individual remit, will add to stakeholder confidence and add value across your company.

Who sets the cyber security agenda in your company? Analysis by all respondents.



Insurance

A safety net for the safety net.

How much do you spend on business insurance? If the cyber-insurance trend continues, you could be paying more in the near future. As a bona fide sector, it's been in existence for a little over 10 years, with the US being the strongest market, deploying a third of expenditure. According to Costello, the total market was valued at US$4.52bn in 2017, set to rise to US$17.55bn by 2023. However, despite that growth forecast, it's been a rocky road. The nascent industry is being questioned on its ability to assess cyber-risk, carry out due diligence and provide post-incident support. The desire to limit exposure has led to high premiums, low claim limits, blanket terms and conditions, and a wide range of exclusions. Regulators are concerned insurers don't understand the risks and couldn't withstand losses from a widespread cyber-attack.

In light of this, businesses must question the value being offered and whether it would be remedial or simply a long argument about exclusions and definitions. Organisations must be certain they meet the minimum standards required or the policy could be worthless. Even so, the due diligence required before insurers underwrite a policy is a valuable exercise and any actions taken to reduce premiums will also increase resilience. Cyber-insurance provides a clear opportunity for CFOs to quantify cyber-risk and base security measures on a sound business case. In many ways, it's a lens through which to organise your cyber-governance framework, as described in the previous section.

As cyber-insurance enters the regulatory landscape, firms are being put under increased pressure by clients, customers and shareholders to ensure real protection exists. If you are considering it, organisations that 'self-insure' tend to look at how they would cover the following actions and remedies in a timely and effective manner. As with all things, it's a cost benefit analysis, and one that is hard to quantify until the worst happens. Nonetheless, you'll certainly want to think about business losses from system downtime and business disruption perspectives.

Start by asking yourself, what's your daily revenue? Would an annual insurance premium that covers a day offline be worth it? How about two days? Or a week, which isn't unusual following a major cyber-breach. Where to draw the line on this kind of risk analysis? How about the costs associated with a forensic system examination to isolate the incident and re-mediate vulnerabilities? How complex are your

> It's not enough to rely on generic, underpowered insurance policies to help you. Prevention will always be better than cure. **Be diligent** by establishing your own specific needs and weaknesses.

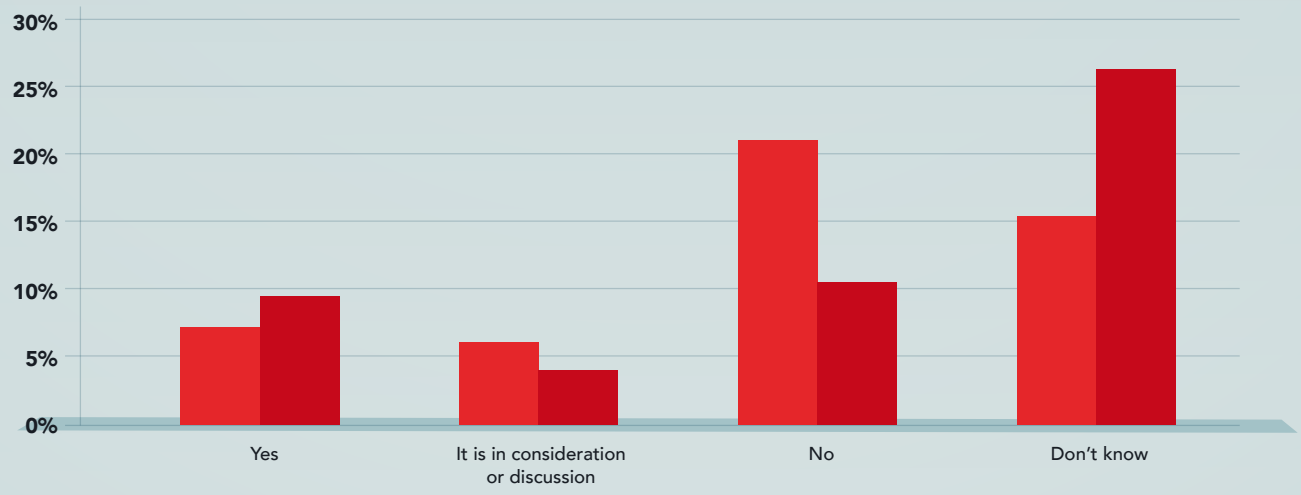
systems? How expensive is that process? Of course if there's theft or fraud, you may need to cover actual material losses. Those kinds of losses might extend to physical systemic damage. How much does all of your company's computer hardware cost? What if your systems simply aren't safe to use following an attack? They've now become a sunk cost. Who covers that?

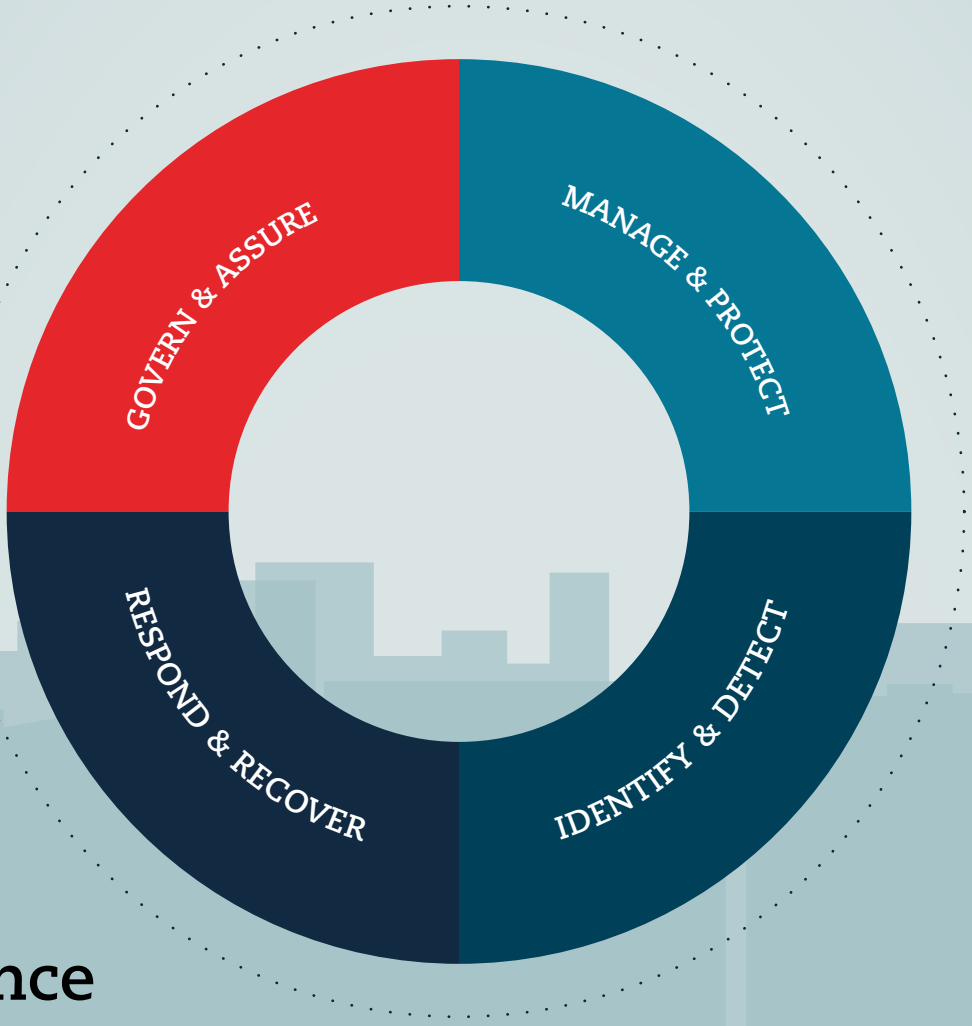
Then moving away from the hardware side of the argument, what about crisis management costs? Who's going to pay for the public relations team that will limit the reputational damage? You'll need to notify your customers and suppliers. That's another cost. Then there's the credit monitoring elements which will be expensive. And the legal team, that can spiral out of control, particularly if we're dealing with a breach of confidential information. No doubt the regulatory fines are going to rack up too, if it doesn't go your way. And the loss of intellectual property, or the ransom you have to pay to get it back. That might be very costly, depending on what goes missing…

With all of that taken into account, maybe covering for the worst isn't a bad idea after all. Maybe it's time to be vigilant and pay the premiums? As with all things, the devil's in the details. You need to know whether the policy covers actions taken by an employee, either maliciously or as a result of social-engineering. Does the policy cover human error and malice? How about third-party service providers and dependant businesses? Or attacks which have already occurred which are yet to materialise? What does the policy say about incidents that occur during the cover period but are detected later? And critically, does it cover future risks as well as known ones? As we know, this space is evolving at lightning pace. Who defines what is currently a threat and how does one qualify its existence?

If you can start to ask these types of questions and analyse how they relate to your business, you may find that cyber-insurance is in fact an important facet of your general resilience strategy, a catalyst to recovery should the worst happen. Of course you may not, given the financial outlay. Nonetheless, its strongly advised that you consider the steps you might take during such a process, as it's all good practice in preparing your firm. Because now, you're thinking like a cyber security savvy CFO, and the next logical step is to think about what cyber-resilience really means for you and those around you.

Does your company have cyber security insurance? Analysis by business size.





Resilience

Go beyond spinning plates.

As CFO, you're starting to feel comfortable in the cyber security space. But there's no room for complacency at this stage. As cyber-threats move from being isolated to more pervasive, so too do your defence strategy requirements. Rather than focusing too much on the prevention of breaches, you need to focus on resilience. That means combining the aspects of traditional disaster recovery planning with business continuity management. Reacting quickly can limit financial and reputational damage. Therefore, resilience is measured by your ability to resume normal business operations as fast as possible. And of course, it must also be delivered cost-effectively.

There are only truly four stages to establishing cyber-resilience, which are as follows: 'manage and protect', 'identify and detect', 'respond and recover', and finally 'govern and assure'. It's the combination of all of these disciplines which creates resilience, but it isn't a sequential list. You should be implementing all of these processes on a consistent and iterative basis, all of which will feed into your long-term cyber-governance framework.

'Manage and protect' focuses on managing the data and assets throughout the information systems and networks under your control. It establishes policies to protect the organisation from cyber-attack, system failures and unauthorised access, which involves establishing defences to cover people, processes and technology. In performing a risk-analysis of your systems, you'll have already started this process. If you've started training your staff on best practice, you're already making strides in the right direction. If you're implementing two-factor and multi-signature login requirements for critical systems, you're well-ahead of the pack. Management and protection is essentially understanding your own ecosystem, how the threat landscape pertains to it, and how you create effective processes to mitigate as much non-technical risk as possible. It's all the things you can do without being required to actually perform any systemic fixes of your own.

Which takes us to 'identify and detect' which requires a much closer relationship with internal and external IT and specialist cyber security teams. This is where you really start looking underneath the hood of your business to perform what is known as 'penetration testing'. This will take on a range of different processes, falling under the broad categories of security tests, vulnerability scans and intrusion detection. It's an always-on process.

There's an art to creating effective defence strategies. **Follow the rules**, and don't try to create efficiencies by skipping any steps. Realise that holistic security is more than the sum of its parts.

You'll employ ethical or 'white-hat' hackers to try and perform the same exploits as would be performed by 'black-hats'. You'll create different scenarios or events in order to run a predictive analysis of what an attack might look like. If you need official standards by which to benchmark, refer to the UK National Cyber Security Centre (NCSC) CHECK standard, or alternatively in the US where the General Services Administration (GSA) publishes Standard 132-45A for similar purposes.

Next, 'respond and recover' which covers all of your business continuity plans and incident response measures. A response and recovery plan includes validating that a cyber-attack is taking place and mobilising the response and recovery team. They will quickly place firewalls and stopgap measures to ensure the threat doesn't spread, quarantining affected applications and networks. This process relies on the penetration testing element previously mentioned. The better prepared you are, the more familiar this will be.

Throughout, timing for alerting authorities and regulators, as well as the firm's external media team, will be deduced in real-time alongside carefully managed public relations.

There can be significant damage to your brand value if you don't get this absolutely right. You will have also planned for unknown situations. If a whole system goes into lockdown, there may be a range of spin-off scenarios you have to deal with, so having auxiliary teams on hand to assist with these is critical to a well managed cyber-response.

And then, there's 'govern and assure', highlighting the importance of regular risk assessment and the need for a continuous improvement programme. You ought to be reviewing your company's compliance with legal and regulatory requirements, not least GDPR in the EU. This is really a meta-process to what is already in place. Educational content should be circulated by your team, and you should be looking to engage with experts like those at the ACCA to better understand every element of the technical, communications, regulatory, legal and governance landscape. Without increasing your knowledge every day, it's easy to become outdated. Of course, in reading this, you're already taking the necessary steps. And the next step is to brace for a breach!

Attack

Code black.

There are a number of stages in a cyber-attack. For the most advanced attacks, a device can be nested inside a network for more than 200 days, on average. This is sufficient time for the perpetrator to gather information that is useful in undertaking the attack itself. Cyber-attacks don't just happen. They are invariably well planned and they often have more than one purpose. Here's a typical scenario to think about.

Stage 1 is Reconnaissance. Hackers will spend months identifying a vulnerable target. It could start on a social network, looking at connections. Rather than targeting the team member directly, they look for vulnerabilities in a supplier. It could be people connected on public LinkedIn and Facebook accounts, implying they're also friends as well as business associates. Perhaps they send public posts to each other on Facebook, humorous memes or some such. It's not a cognitive leap to emulate that content and use it as bait in an email exploit. Your attack surface has been doubled in that one connection alone. There are many similar connections, based on this relationship between business and pleasure.

Stage 2 is Scanning. This is the identification of the weak points that can be exploited. This can be an extended process as the attackers probe for vulnerabilities. It might be that your email filtering system is set to withstand incoming mails from new addresses, but once a contact has been confirmed more than twice, it's allowed through automatically. If there are multiple routes to entry, the attacker might employ click trackers in trojan emails to find out which users are most likely to engage, and which has the most value, before delivering the payload. It's an iterative process, just like the penetration testing you've undertaken.

Stage 3 is Access and Escalate. Once the weak point is identified the attackers gain access and then, by using a privileged access account, move around the network with the objective of taking over. This movement could happen quickly to cause immediate low-level damage, or build over time in an attempt to weaken the system, in turn unlocking greater rewards. It might be that initial access is for the next stage of penetration testing. Advanced security systems can't be disabled all at once. But cyber-criminals have patience, and remember, this is their job. They can afford to take their time...

> Being responsive and adaptable to the varied types of cyber-attack in a real-world situation is be the difference between success and failure. If you don't **think laterally**, you are destined to fail.

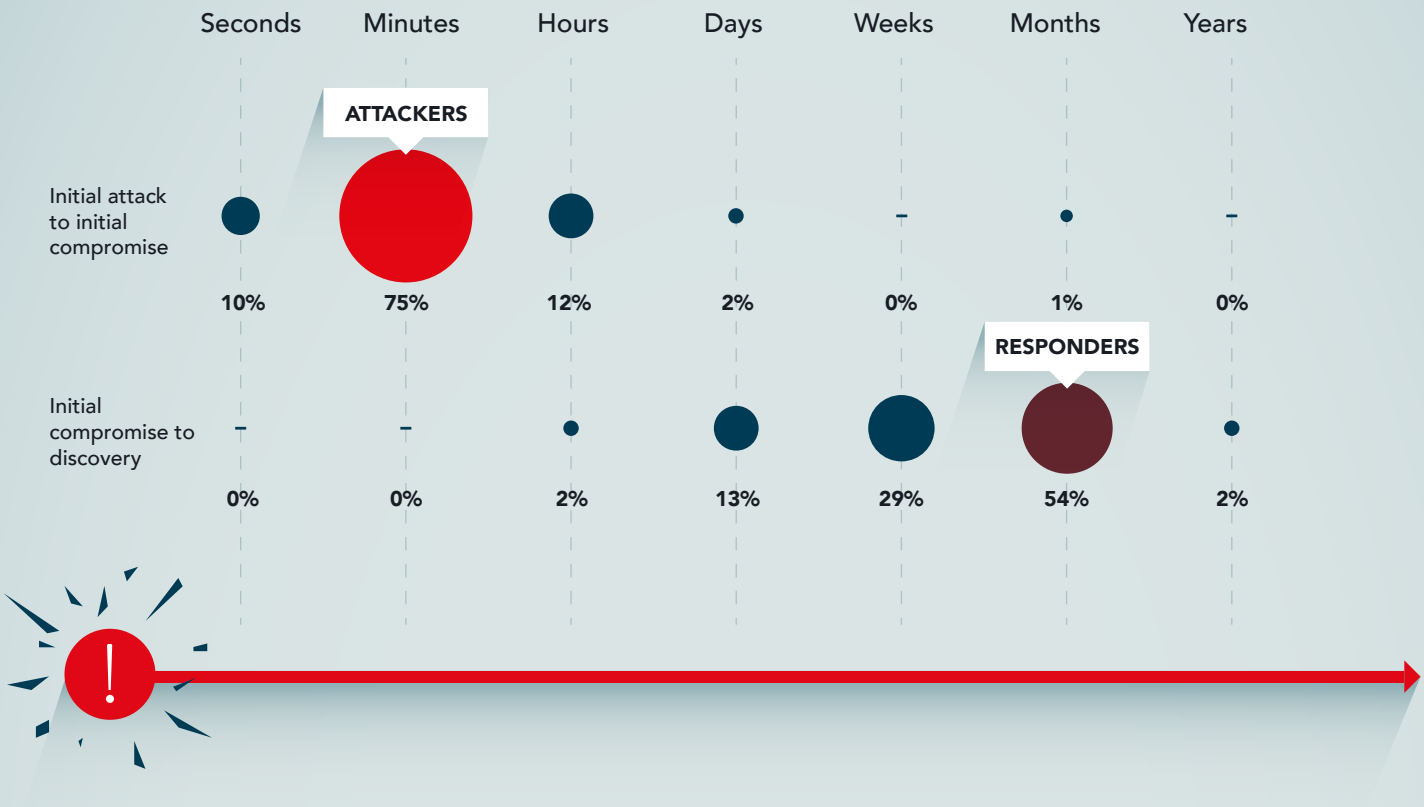
Stage 4 is Exfiltration. Having gained access, hackers can obtain data from your organisation at will. They can change or erase files. At this stage, damage is already being done. If your security team hasn't identified a threat now, it's likely that there will be some fallout. Much will depend on what data is accessed and what they want it for. It could be logins. It could be IP. It could be your private emails with a loved one. It could be your bank details. Each of these would carry with it specific implications. Combined, there could be a range of applications which could be triggered independently to reach a particular goal.

Stage 5 is Sustainment. The hackers are now moving around your network at will. They have multipoint access to critical systems, and are now able to create novel strategies by monitoring activity. What are the usage patterns? What would need to be disabled in what order to create the maximum amount of damage? With this level of access, it's unlikely that even a well-versed IT team would know what was happening. Every move is likely having its tracks automatically covered. The clock is ticking. It's just a matter of time…

Stage 6 is Assault. This stage is not present in all attacks. The hackers may take control of hardware in the organisation or disable it. At this stage, it's generally too late to defend yourself. You will be in a state of resolution, trying to limit the damage as much as possible. You're unlikely to know what really happened yet, it's more about making sure that you can regain as much control as quickly as possible, within the range of commercial sense. Do you unplug completely without backing up your files? It's your choice...

Stage 7 is Obfuscation. In this stage the hackers mask the trail, perhaps after first leaving a 'calling card'. The objective is to confuse those who might be undertaking a forensic examination of the incident at a later stage. Again, this phase is not always carried out, or it could be carried out prior to an assault. It really depends on what the strategy is. Are they sending a message, or are they lulling you into a false sense of security in preparation for the final stage?

Stage 8 is Post-Exploitation and Persistence. Hackers plant additional malware to maintain access even if their initial attack has been detected, systems have been rebooted or patched. This includes, for instance, installing a permanent backdoor on a machine. Ensuring this isn't the case can be very expensive indeed. But then at this stage, you may not have any other choice...



Response

Out of time.

You did your best. But this time, it wasn't enough. IT think it came in through the email system. They were after Marketing. That's where they figured they could spread quickest. You always gave that department a bit more slack. After all, they're moving digital assets in and out of the firm at a much greater volume than everyone else. Too many controls will have stifled progress. After the intern clicked the attachment, it was too late. You all got it. Some of you fell for it immediately, others didn't. You'll need to learn from your mistakes on this one. From here on it's damage and information control...

As we've established, protection is only one part of the cyber security puzzle. A successful attack may be unavoidable, so detection and response will play a vital role in reducing the cyber-threat. If you have an Incident Management Plan in place, a critical part of your general cyber security governance framework, then you should have a head-start. Of course, your skills of improvisation and storytelling will be put to the test now. You need to be decisive and diplomatic in the way that you handle things from here, making sure that things don't get blown out of proportion. Creating the right tone throughout this process is key. The communication fallout can sometimes be worse than the material loss. Remember, what you're working with here is now tantamount to a crime-scene.

Given that an attack is inevitable, organisations need to plan for the scenario. In ACCA's report, The Race for Relevance (2017) Gerry Penfold, a former technology risk partner at KPMG UK commented, "Some companies spend very little time and money on reacting and recovering. They spend 80% of their security budget on defences, and probably less than 10% each on reacting and recovering. Effective planning to manage the response to an attack, including the social-media responses, is essential for organisations to plan for and rehearse." And in a world of hyper-connectivity, that can be extremely difficult.

Roles should be clearly defined in the event of an incident and everyone should know what their role is. This does not just apply to internal actions but external communication. Who talks to the media, who contacts regulators and law enforcement, who informs customers and suppliers, and who deals with the insurers if you have cyber-insurance. If information hits the public in a non-controlled way, it can have all sorts of negative consequences from a regulatory and market perspective. It's essential your company goes into lockdown.

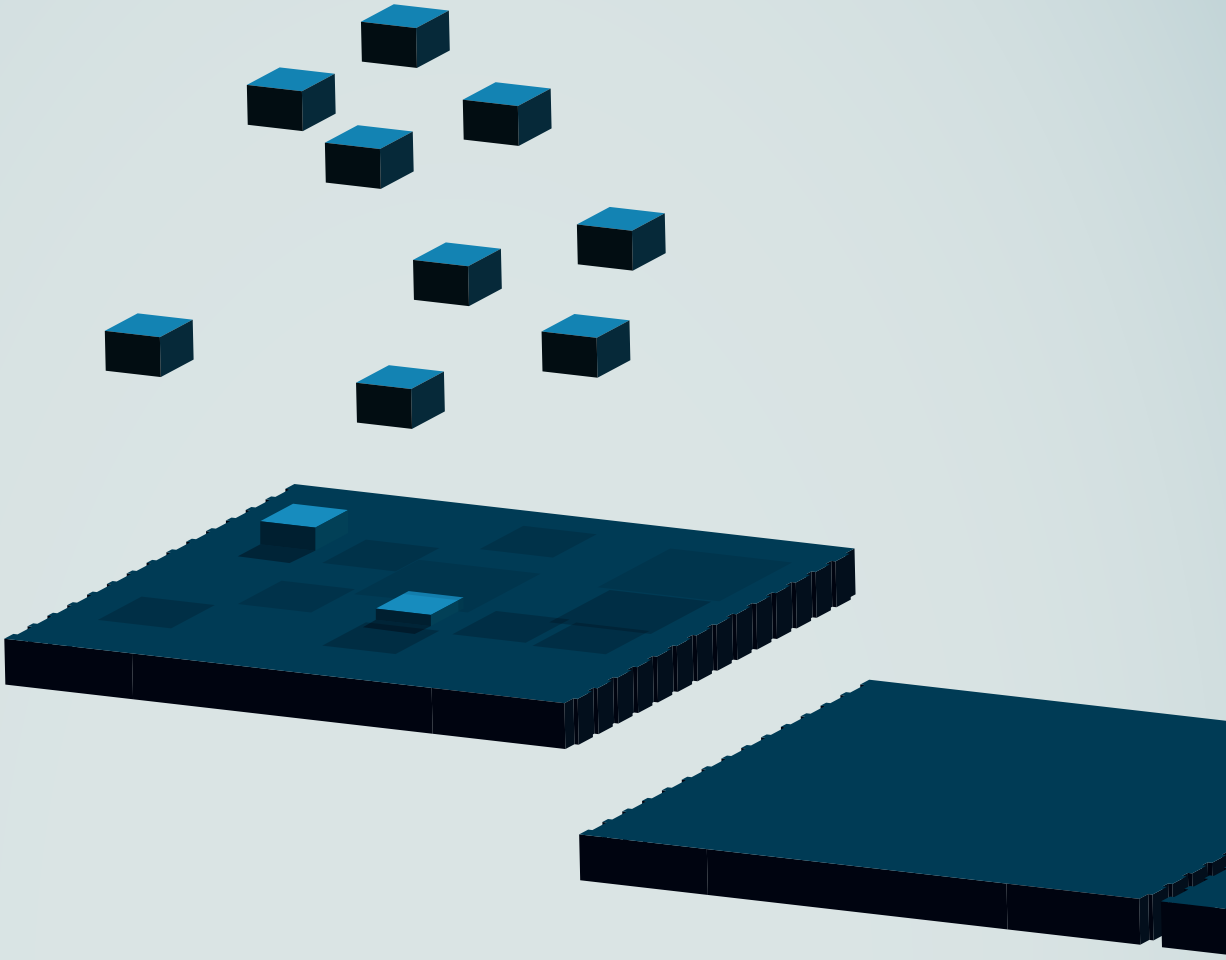
You should **be able to balance** a wide range of commercial and reputational risks in the aftermath of a cyber-attack. How you do this will define the real fallout and your success as a leader.

At this stage, once your IT team has the situation under control, you must move towards orchestrating the restoration and verification of data; helping customers with credit issues and ensuring that you haven't given away all of your trade secrets, or indeed those of your partners. Non-disclosure agreements still apply, whether or not you wish to disclose the information in the first place. You'll be paying compensation as required and attempting to rebuild trust by communicating with stakeholders about the action that has been taken. The process is very much akin to catching water with your hands after a pipe bursts. Far better to have the buckets ready. And be sure not to slip on the wet floor.

A further consideration is the importance of learning your lessons from the attack. What were the vulnerabilities that were exploited? What was the timeline of events? Remember, at this stage the attackers are potentially still in your system. The re-mediation process could be long and expensive, but it needs to be thorough. There's always the risk of post-exploitation and persistence. A relapse of this incident is the last thing you can afford. You should be picking through the crime-scene alongside your IT personnel looking for any evidence you can and using everything you find to update your cyber security governance framework. As the old saying goes, what doesn't kill you makes you stronger...

Having survived your first cyber-attack, it's important to treat the cause, not the symptoms. Attacks are random but may not be repetitious. Some elements which caught you off-guard this time, and which were a critical part of this attack-strategy, may be far less important the next time round. The key here is to start thinking about how the whole attack was conducted. How did it get in? How did it move so quickly? Were the staff involved equipped to manage the threat? How did they respond when everything was made official? Were you able to communicate effectively with each department involved?

The learning here is that, despite being an inherently technical issue, the real dynamics of a cyber-attack are distinctly human. As CFO, you'll be away from spreadsheets and accounting software and directly in charge of information control, a process that requires a unique degree of emotional intelligence. How you respond to this challenge in a structured way defines your success in surviving the attack and increasing your company's resilience.



Future

The Internet of Everything.

As we've covered in this report, the scale of the cyber security issue is growing exponentially. Consequently, the demands on personnel equipped to deal with it are growing too. However, the supply of new professionals into the space is not in tune with the demands from the wider industry. Some estimates see the shortfall as high as 3.5 million roles in the global cyber security sector by 2021. And naturally, being human, there's only so much of that work that can be covered by humans alone.

Given the state of cyber security today, the implementation of Artificial Intelligence (AI) and Machine Learning (ML) systems may serve as a solution, bringing with them many benefits in helping to prepare the cyber security workforce of tomorrow. Cyber security techniques that rely on AI/ML use previous attacks as a template with which to respond to emerging yet somewhat similar risks. Currently, the technology's ability is simple, yet is still of great benefit, in that human staff are freed up to focus on more complex threats, with the AI/ML shield in place to deal with the high volume of more low-level attacks.

In the race to detect low-level penetration risks before they evolve into a more widespread issue, these tools are critical. In the future, they are likely to re-mediate situations autonomously. Of course, the attack technology will evolve in tandem, so ultimately you'll have software autonomously fighting software, with white-hat and black-hat operatives' main role being the curation of their creations. Indeed, the cyber security space is set to be one major battleground which powers the evolution of AI/ML, securing its place in our society. Inevitably, it will be a machine world, and we'll just live in it.

Which leads to the Internet of Things (IoT), potentially a game changer for entire industries, even for organisations that have no direct interest in it. As the proliferation of smart devices creates greater opportunities for attack, increased connectivity means these attacks can themselves be more coordinated and disruptive. Even organisations that do not possess IoT devices themselves potentially face cyber-attacks from 'botnets', armies of corrupted and controlled devices. This issue once again highlights the endemic importance of ensuring your supply-chain's security is as tight as your internal approach. A problem for your supplier is a problem for you. As many such devices are essentially consumer items, these will likely be used by your employees and those of

> To be at your most resilient as an organisation, you must be able to **anticipate changes** in the market and have your finger on the pulse of technological trends before they become mainstream.

your partners, and as such may have been developed with minimal security that can be easily breached by hackers. Your suppliers' IT assets and networks should really be thought of as your own, and any IoT sensor networks they use are truly a critical target for hackers.

When such devices are connected to networks, even in a peripheral way as they are to yours, they immediately open up vulnerabilities, which means they must be considered in any cyber security governance framework that you create for your company. The current media narrative around 5G security across the UK's communication infrastructure, and how governments around the world are anticipating the technology, is a testament to its importance and the severity of the threat. On the one hand, IoT and 5G has the potential to provide a wide range of benefits on both a business and consumer level, however the security risk will increase exponentially as a result.

Underpinning these types of next-generation communication applications will be blockchain technology, with blockchain-based identity and access management systems being leveraged to inherently strengthen IoT security. Such systems are already in use to securely store information about identity, credentials, and digital rights. As a result, it's likely that we will see smart IoT devices carrying out autonomous processes via blockchain powered 'smart-contracts', which will be particularly prevalent in the finance sector.

Indeed, it is a technology that is set to disrupt a wide range of industries, including but not limited to supply-chains and logistics, data-storage and transport. For further details and a more in-depth exploration of the technology, be sure to check out the ACCA website which hosts a range of resource and various reports on the subject. As a CFO, it's absolutely critical subject matter. Yet, with all of the hype surrounding such technology, it's not without its flaws. Despite being immutable, blockchains and Distributed Ledger Technology (DLT) are still open to DDoS and Sybil attacks, in which the consensus mechanisms that power them are overwhelmed by raw compute power. As Moore's law plays out, and more novel computing systems are introduced, the implications of this risk remain to be seen.

One such risk involves the evolution of quantum computing, as cryptography powers many of today's security and communications systems, including that of blockchain technology. The nature of quantum computing means that cryptography based on factoring numbers, and the security powered by this type of technology, will become effectively useless. 'Brute force' attacks will take on a whole new meaning. Traditional passwords will cease to exist and the move to 'authenticate the user' will be absolute. Inevitably, with the threat will appear more experimental, quantum defence mechanisms, too. As CFO, it's your role to anticipate these technologies and build them into your overall cyber-governance framework as we move into the 2020s and beyond.

Conclusion

Focus and take stock.

We've come a long way. The expectation is you've now primed yourself to understand some of the key terminology and governance strategies required in the cyber security space, and it's clear that as a cross-organisational activity this will involve engagement across the whole business. You've also thought on a top-level basis about the future of the threat and how that may affect your cyber security strategy. So, let's briefly recap on some of the practical actions you'll want to make at different levels moving forward.

At board level, you'll properly establish and quantify the risk. You need to take the position that it's not a matter of if you'll be attacked, but when it will happen, and how you intend to respond. You must ensure that cyber-risk assessments are made on a regular basis and you'll want to allocate sufficient funds dedicated to cyber-risk prevention, including skilled professionals in-house who are capable of ensuring you are protected.

You'll also want to run cyber security drills, as you would a fire drill, and ensure that the outcomes from these exercises are reviewed at board level. This process will involve a consistent analysis of your prevention measures, which you will review alongside all data-elements and reviews of system inventories, looking for such aspects as outdated operating systems. You'll also interrogate what the future support for your systems looks like, and how that affects your commercial relationship with suppliers and customers.

Finally, you'll ensure that appropriate resilience and recovery programmes are in place to deal with a real-world scenario and that you fully learn the lessons from any successful attack, logging everything that may be of use and continuing to invest appropriately to counteract future breaches. This may well involve the hiring of third-parties to perform penetration testing procedures, in addition to using this as the basis for further conversations around your use of cyber-insurance.

For you and your department, it's much more about recognising that cyber security is an operational risk, and therefore cannot be delegated entirely to the IT department. The CTO, CIO and CEO should all be having regular conversations with the CFO around cyber-governance and risk management. You'll also want your specific team to start understanding more about the implications of reputational damage and brand management, which will involve having more conversations with the CMO too.

> Begin to think about how you educate your teams, apply standard methodologies, become adaptable to crisis and anticipate change. **Never assume** someone else will do your job for you.

As discussed, it's your duty to stay abreast of the threat landscape, recognising that it's constantly evolving and there are unknown threats which are yet to emerge. Further to this, you should always be thinking about supply-chain risk, which will involve educating your partners around these issues and as a network seeking out as much support as you can from regulatory and technical bodies in this space. Remember, knowledge is power. You're only as good as the information you have, which in turn can be disseminated to your firm. With that in mind, it's essential that training for employees is prioritised to ensure that they understand the criticality of information systems and how they may be targeted. Start to use identity-management systems to control how different data is accessed, and ensure that these practices are not undermined by users on public platforms.

On a more technical level, you must use firewalls, anti-malware and intrusion detection to protect your environment, if you don't already. Employ data-encryption to protect sensitive data in transit and at rest. Monitor and control devices connected to the corporate network, especially smart devices. As mentioned right from the start, deploy security patches as soon as possible to reduce vulnerability, and comply with the data privacy (personally identifiable information) regulations for the jurisdictions in which you operate and where your data is stored. It's all work and will come with relatively high upfront cost, but these actions are essential to maintaining your security and credibility. But of course, for all of these sophisticated fixes, there's no substitute for simplicity. Nine out of ten times, it's something embarrassingly obvious that granted your adversary access and created much wider issues.

Top-level, remember the basics. They're as important as the ultra-technical elements, as it's these that hackers will look to exploit first. The easiest and fastest route into a system will always be preferred, which is why it's essential to ensure these are on lockdown. As CFO, you and your teams are the target. It only takes one lapse in judgement to cause a widespread security breach. Do not click on suspicious emails from unknown senders. Always verify the address and be careful to check thoroughly, as often rogue names and addresses including site URLs, will look almost undetectably similar to the genuine article.

Start thinking seriously about taking a new approach to the essential function of accessing your accounts - offline password storage, two-factor authentication and other types of identity hashing software are all available and provide an additional layer of security and peace-of-mind. Use public wi-fi with caution as it may be more vulnerable. Vary passwords between websites or services to prevent a compromised account opening up access to others. Use credit monitoring services to deal with suspicious activity. These are the standards by which you and your organisation should operate, and it's your role to lead by example...

So with that, you've graduated from cyber-bootcamp. We wish you all the best in tackling this threat, in an increasingly uncertain business arena. Be sure to share as much information as possible with your board and do check out the ACCA website for further information on this subject. We look forward to working with you soon.

Think Ahead

About ACCA

ACCA (the Association of Chartered Certified Accountants) is the global body for professional accountants, offering business-relevant, first-choice qualifications to people of application, ability and ambition around the world who seek a rewarding career in accountancy, finance and management

ACCA supports its **208,000** members and **503,000** students in **179** countries, helping them to develop successful careers in accounting and business, with the skills required by employers. ACCA works through a network of **104** offices and centres and more than 7,300 Approved Employers worldwide, who provide high standards of employee learning and development. Through its public interest remit, ACCA promotes appropriate regulation of accounting and conducts relevant research to ensure accountancy continues to grow in reputation and influence.

ACCA has introduced major innovations to its flagship qualification to ensure its members and future members continue to be the most valued, up to date and sought-after accountancy professionals globally.

Founded in 1904, ACCA has consistently held unique core values: opportunity, diversity, innovation, integrity and accountability. More information is here:

www.accaglobal.com

OpSec Alert: CFO's Top Secret Guide to Cyber Security

To discover our latest research visit our Professional Insights page: accaglobal.com/insights

ACCA The Adelphi 1/11, John Adam Street, London WC2N 6AU, United Kingdom

+44 (0)20 7059 5000 / www.accaglobal.com