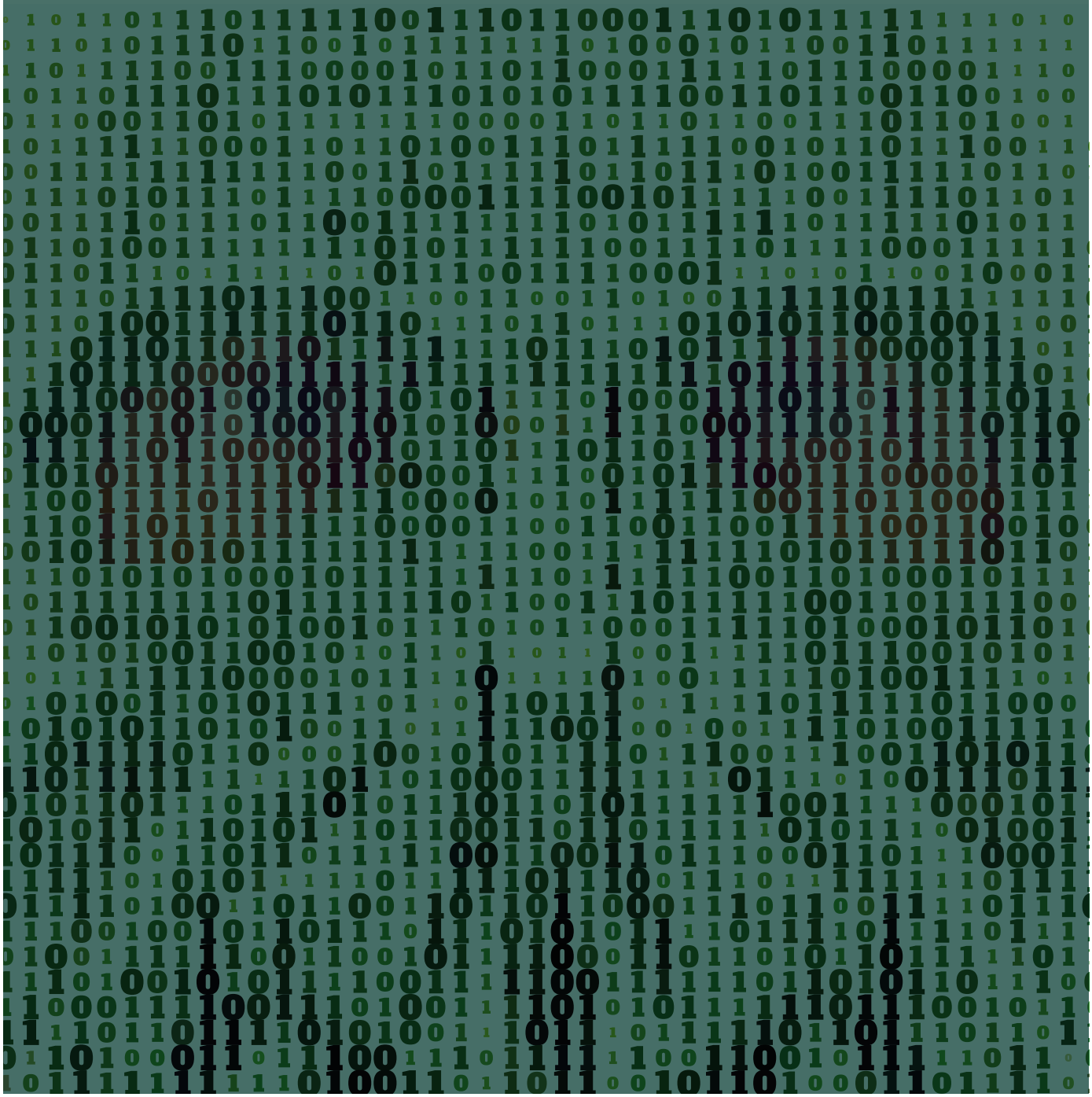
StrategicRISK

GUIDE TO: CYBER RISKS



Sponsored by: Swiss Re Corporate Solutions

Thoroughly modern theft

Cyber crime used to be a rarity, with physical break-ins par for the course, but the new breed of highly sophisticated criminal makes the swiping of data tapes seem quaint

The rapid migration of business and personal information into the digital stratosphere has largely taken the world by surprise. Global interconnected technology platforms have created a base not only for businesses to bound into previously untapped markets at the touch of a button, but also given criminals a new and arguably easier way to operate. The amalgamation of both has exposed the vulnerability of large companies such as Ashley Madison in the US and TalkTalk and Carphone Warehouse in the UK to costly, high-profile cyber attacks.

Experts say the challenges facing firms in 2016 are very different from the TJX and Heartland hacks that put data breaches on the map 10 years ago.

"We have gone from essentially the first and largest data breaches to now, where it is a daily event that we have data breaches and cyber events," says Swiss Re Corporate Solutions claims expert Catherine Lyle.

Airmic board member Tracey Skinner says: "Eight years ago, you would have considered cyber to be a remote risk for businesses. You would have considered it to be particularly impacting those who are working around the technology and telecommunications area – in other words, the service providers in those areas. You would not really have thought much about the risk exposure of cyber in most other organisations."

"Before," says Lyle, "you actually had physical theft, where someone had to actually break into a room and steal a data tape or a filing cabinet, or you had the opportunistic theft, where someone saw material and simply took it. That physical theft was immediately noticed. That's very different from today, where a criminal can enter a system for months and be undetected, and can exfiltrate large amounts of data – and it can be gone without ever being noticed."

As a new breed of highly sophisticated cyber criminal emerges, simple data theft is starting to look like old news. "It has become far more organised," says Fifth Step chief executive Darren Wray. "Yes, there are still the opportunistic individuals or opportunities out there that people take advantage of, but it is now all about organised cyber crime. One of the big challenges that's taken place in the last five years is the rise of the hacktivists – hackers with a political or social agenda – as opposed to those who are just hacking for sport or for the opportunity to hack into a large organisation."

Another challenge for risk managers stems from the basic principle of the internet, which is to be an open playing field that anyone can use. Given the sheer volume of sensitive data digitised and stored on cloud-based systems, security is by no means guaranteed.

Lockton cyber risk practice leader Ben Beeson says, "This risk is driven by technology. If there was no internet, there'd be no cyber risk, but the internet was never built to be secure. It was built to be open. Since then, we have had to retrofit security and do patching. Technology drives the risk, and it's getting riskier because certain industries are now digitalising, such as the healthcare industry. Patient records are being digitalised and stored online. That creates more technology-driven risk." ●

> **IF THERE WAS NO INTERNET, THERE'D BE NO CYBER RISK, BUT THE INTERNET WAS NEVER BUILT TO BE SECURE. IT WAS BUILT TO BE OPEN**
> BEN BEESON, LOCKTON

A brave new world

Hooked on high technology, our society has never been more vulnerable to cyber attacks. With the 'age of Big Data' upon us, ransomware and hacktivism pose a disturbing threat

Highly visible data breaches are growing with such frightening regularity, it is easy to understand why business leaders would fear they are losing the battle with cyber attackers. The biggest shift in this space in the past 10 years, and the one that is of most concern to risk managers, is that cyber criminals no longer discriminate between multinationals and small, high street businesses or between a telecommunications giant in Singapore and a tiny textiles factory in York.

DAC Beachcroft partner Hans Allnutt, who leads its cyber risk and breach response team, says we are in the 'age of Big Data'. He adds: "There are three Vs in Big Data. One is variety, another volume and then velocity. We've never before had such a variety of data being held on individuals. It used to be that if you buy something in a supermarket, the supermarket knows that someone bought certain goods at a particular time and spent X amount of money. Now the supermarkets know who it was, what they're doing, what period of time, where they came from, what they did, what they're missing in their fridge, what their preferences are and other activities.

"In addition, the volume of that data is enormous. Naturally, that data was always there, but the capacity for companies now to capture it and store it is unprecedented. Then the velocity to transfer that data around the world and use it at speed. That really all builds up to the fact that data has been monetised, so personal data and our privacy is now a commodity. That means it needs protecting, >

which is a huge issue for risk managers in today's world."

Airmic board member Tracey Skinner says new technology has changed the cyber risk landscape in another way, in that the majority of business functions now rely on it. "The volume of business done on the internet in this space versus 10 years ago is completely unrecognisable. Every organisation's reliance on technology is so much greater. Therefore the likely impact of a cyber attack on any organisation is far greater than it was. The two combined together, coupled with the greater sophistication of the hacker, has created a much greater risk for businesses. Also, there are now hackers with different agendas who are targeting particular organisations for a particular reason, as opposed to 10 years ago when it may have been somebody who just wants to do something for fun or for a little badge of honour. These days, it's far more serious than that."

Allnutt says an operational change has altered the risk landscape. "Most people now are paperless. When you are so dependent on electronic systems, that becomes a significant risk for businesses. Technology hasn't really changed cyber risk. I think it has created it by definition. Modern life is governed by electronic systems. If we can't have them, if we don't have access to them, we cannot function. Technology is always going to be new and always developing, but our reliance on those systems is unprecedented. Cyber risk has always been there, but it's here now at the forefront because of our reliance on those electronic systems."

Skinner agrees. "Our reliance on IT systems and technology has changed dramatically all across the [Airmic] membership, therefore the risk becomes one for all of us," she notes.

"Having said that, I believe there is still more of a brand and reputational risk for those delivering services in the technology and telecommunications industry, so they are still at the high end of the exposure. But I don't really think any organisation, unless they're completely without any technology, can escape."

IT IS SAFE TO SAY THAT 2016 IS THE YEAR OF RANSOMWARE. THIS IS A QUICK AND EASY WAY FOR A CRIMINAL TO MAKE MONEY. THEY FREEZE THE SYSTEM AND SAY 'PAY US'
CATHERINE LYLE, SWISS RE CORPORATE SOLUTIONS

SECURITY BY DESIGN

One of the key issues for risk managers is that when adopting new technology solutions, there will always be a trade-off between functionality and security. New technology gives a firm the ability to differentiate and gain a competitive advantage. But while there is a temptation to promote the firm's new functionality above all else, the flipside is there will always be a catch-up on the security side, according to experts.

"The answer is to have a principle of security by design," says Allnutt. "That is, whenever you're building anything new or developing anything new, you design security and integrity into that system or project from the start. Of course, the big challenge for risk managers is that this comes with a cost and time burden."

Another significant development in the cyber risk space is where responsibility lies. Once, it sat squarely with a business's IT function. These days, however, it is a concern for every employee from the board down.

The difficulty for risk managers is not only understanding the risk in the organisation, but also getting all staff to actively engage in the protection of data.

Skinner says: "The challenge for risk managers is truly understanding the risk in the organisation end to end, which means understanding a lot about IT, being engaged with the CIO and really understanding the organisation's unique weak points and therefore, any possible issues. The challenge doesn't stop there, because once you get to understand it, you then have to communicate it to your senior management, which again can be an area, depending on the type of business, that they may not have touched on to any great extent before.

"For a board or an operating committee that hasn't really touched on this space, it's quite a difficult conversation. Time is always tight and it's about getting airplay. The usual 'five slides and you're out' approach can sometimes be a challenge when you're talking about things that they don't really understand and haven't really got a handle on."

Even with buy-in from the board, risk managers must justify the enormous costs of managing cyber risk. "The greatest difficulty is quantifying exposure, justifying expense and assessing the risk," says Allnutt. "Just as technology changes, so is the law, almost as rapidly at the moment. Putting numbers into what that risk looks like in order to justify expenditure on risk management, be that control, software, systems or insurance, is a real challenge because we're going into uncharted territory."

One thing all the experts agree on is that ransomware is the biggest new cyber threat facing businesses.

Swiss Re Corporate Solutions claims expert Catherine Lyle says: "It is safe to say that 2016 is the year of ransomware. This is a quick and easy way for a criminal to make money. They freeze the system and say: 'Pay us or you won't be able to do business.'

"We're also seeing a lot more hacktivism, where a person or a group may disagree with how the company is doing business and will hack in and cause either financial harm or embarrassment to a company because of the position that that company takes."

She adds: "Criminals stay one step ahead and all we can do is try to keep our technology ahead of the crimes and our response moving faster, so that we can shut down and narrow down the timeframe of a cyber event."

Scott Stransky, manager and principal scientist at risk modelling firm AIR Worldwide, says it is important to remember that where there are challenges, there are also opportunities for savvy businesses.

"I think there are all sorts of challenges around this risk, but that also leads to big opportunities. There is a challenge in figuring out where the next breach will come from. I don't think anybody could predict what the next big event will be. The challenge is managing for any type of breach, any type of eventuality. We believe that by understanding what would happen if a cloud goes down or if a payment processor goes down, companies again could become more resilient to those types of events." ●

TOP FIVE CYBER CRIMES

Workplace complacency continues to be a major contributing factor to the vulnerability of a business to cyber attack. Experts say although employees are aware of the risk, they do not comprehend the full scale of the impact that even a minor breach will have. One issue for risk managers is the misconception perpetuated by C-suites and employees that their business is not large or important enough to be hacked.

Darren Wray, chief executive of IT services firm Fifth Step, says cyber criminals are not concerned about economies of scale. "One of the crazy things we hear all the time is, 'We're too small to be of interest to the hackers' or 'We've got nothing interesting that the hackers want' or 'We're too big to be of interest to the hackers because we're too protected.' That is just absolute nonsense. Many organisations are hacked because they have a piece of the jigsaw. It may be that your organisation holds the last five digits of the credit and that's actually all the hacker needs in this instance. That's where the complacency comes in."

Here, then, are the top five cyber crimes businesses must be aware of.

1

Internal crime

This form of cyber attack will take place over a period of time, usually undetected, and involves a rogue employee gaining access to vital confidential information or taking control of part or all of the technology infrastructure. A ransom is usually demanded in exchange for surrendering control.

• Average detection costs for hiring forensic IT experts: $610,000 (Source: IBM/Ponemon Institute)
• Average lost business cost: $3.72m (Source: IBM/Ponemon Institute)

2

Organised cyber crimes targeting large multinationals, competitors and chief executives

Increasingly, spear phishing is being used by cyber criminals to gain access to a particular high-level employee in order to gain control of IT or accounting systems. Examples include an invoice attached to an email which, once downloaded, will contain a virus or malware that will take control of the firm's systems. This form of attack is particularly dangerous because, due to its sophisticated nature, the employee may not be aware for a period of time that control has been lost.

• In 2015, spear phishing was responsible for 38% of cyber attacks on large enterprises (Source: Vanson Bourne survey)
• Average business cost of a spear phishing incident: $1.6m (Source: Vanson Bourne survey)

ONLY 25% OF RESPONDENTS THAT BUY LIMITS ARE CONFIDENT THAT THEY COMPLY WITH INTERNATIONAL BEST PRACTICES AND STANDARDS FOR INFORMATION SECURITY GOVERNANCE

AON GLOBAL RISK CONSULTING CAPTIVE CYBER SURVEY 2016

3

Ransomware and terror threats

A ransomware attack can create a two-pronged problem for businesses: pay the ransom to have the files unlocked or spend days rebooting systems from back-ups, which are likely to be out of date. In both scenarios, businesses are likely to face exhorbitant costs of business interruption, data recovery, lost sales or contracts, dissatisfied customers and traumatised employees.
In early 2015, the FBI issued an urgent alert to businesses globally about cryptographic ransomware – a particularly malicious type of malware that encrypts company data and demands payment for the decryption key.

• CryptoWall ransomware cost US businesses more than $18m in 2015
• 72% of infected business users were unable to access their files for at least two days following a ransomware attack.

4

Data theft, privacy and hacking

The aim of 'hacktivism', usually performed by social or political 'hacktivists', is to gain access to a firm's sensitive records such as credit card data, social security information or medical records. Hacktivists usually pierce the firewalls and release the information publicly as a way of crippling the firm. They are mainly motivated by social or political justice, rather than monetary gain.

• Average cost per record breached: $230 (Source: IBM/ Ponemon Institute)
• Cost of malicious attack per capita rose from $159 in 2014 to $170 in 2015 (Source: IBM/ Ponemon Institute)
• Average post-breach costs: $1.64m (Source: IBM/Ponemon Institute)

5

Fraud

Fraud-motivated cyber attacks come in many forms. Unsecured databases mean employees or hackers, via social engineering methods, are able to gain access to businesses' internal systems and use them for undetected fraudulent invoicing, bank transfers and incremental syphoning. This type of fraud can be particularly damaging to the reputation of a business because lax security instils a sense of fear in clients and can lead to legal action against the firm for failing to prevent unauthorised access to electronic data containing others' confidential information.

• Average customer notification costs: $560,000 (Source: IBM/ Ponemon Institute)
• Average legal defence costs: $698,000 (Source: IBM/Ponemon Institute)

Now's the moment to step up to the plate

Businesses need to maximise their defences and stop treating cyber threats as an emerging risk, says Swiss Re Corporate Solutions' François Brisson

The digital revolution is transforming the way in which businesses operate. Thanks to technological advancements of the past decade, the advent of smart and WiFi-enabled technologies, and the birth of the Internet of Things, economies and industries across the world are operating faster and more efficiently than ever before. But with this advancement comes a major risk, one that is changing at a pace few businesses are able to keep up with. That risk is the growth and increasing complexity of cyber-related attacks.

In this new, hyper-connected digital world, cyber threats can no longer be treated as an emerging risk that sits on the horizon. It's a very real concern and authorities are getting ready and the implications for companies will be quite considerable. For example, the new EU General Data Protection Regulation will become effective locally in 2018, making notification of cyber incidents mandatory. This means that corporations need to start now to get ready.

Cyber threats are, then, a reality for businesses of all shapes and sizes. And even more worrying is the fact that attacks are inevitable, with the potential to cause global losses for multinationals.

This does not mean, however, that managing the risk is a futile pursuit. In fact, there is a lot that businesses can do to maximise their defence against cyber risks.

First, businesses must refrain from treating cyber threats as an IT problem. It is, without doubt, a risk management issue and managing the threat calls for an enterprise-wide risk management approach, where the risk and IT departments work together and in tandem. This is not an easy task. The two departments speak completely different languages and will often have opposing views on how to manage the threat.

But with a risk that spans costly data breaches to ominous cyber espionage, it is absolutely crucial that the two departments put an end to silo working and collaborate on taking a risk-based approach that puts business resilience at the heart of their cyber prevention strategy.

To get to this point, risk managers need to step up to the plate and work with IT professionals to establish the right security culture. This begins with a risk assessment that looks specifically at a company's exposure to cyber-related vulnerabilities.

In this process, risk managers must identify their company's data assets and intellectual property and classify them into groups. This will provide a clear overview of the assets that need to be protected. The next step is to determine the value of each group of assets in monetary terms before drawing up a map of threats that could harm these assets. This will give a clear picture of the depth and breadth of losses a company could suffer should an attack take place.

Through stringent risk assessment, businesses can then build an effective resilience programme that plugs any security gaps they may have, and ultimately save the company hundreds of thousands of dollars.

With a collaborative, risk- and IT-focused prevention plan, the board of directors is more likely to sit up and take notice. Risk managers can then get involved in strategic conversations about why and how they can align cyber risk prevention with the company's objectives, how a preventative strategy could save the company significant amounts of money, and how the business can measure the effectiveness of its new cyber security programme.

Cyber risk is not just a risk management problem. Insurance is a valued tool in a risk manager's toolbox and insurers can ease the burden when it comes to cyber risk. Cyber risk poses challenges for insurers too. We have to work harder and move faster so that we can improve our insurance offerings and keep pace with the fast-evolving cyber risk landscape.

François Brisson, head of Swiss Re Corporate Solutions' cyber & technology team

Ask naughty questions

Helle Friberg, group insurance manager at Hempel

The cyber risk landscape has become extremely vicious. It is no longer an emerging risk, it is a known risk and it is here to stay. The risk is exacerbated by the launch of new technologies, which are growing in sophistication and complexity and more and more businesses are becoming reliant on them to do business efficiently.

At the same time, the cyber risk landscape is constantly shifting, so it is difficult for risk managers to get to grips with and fully understand it. One of the main challenges for me is that as a non-IT-technical person – which most risk/insurance managers are – it is difficult to understand both the nuances of new technologies and cyber risk itself. For this reason, it can be challenging to support mitigation processes and I believe that the majority of risk managers do not have the right preventative and post-incident response plans in place.

It is therefore vital that risk managers engage with and work collaboratively with the IT department. They should ask IT personnel 'naughty' questions, challenge the IT processes and procedures and systems. This will, undoubtedly, help them gain a better understanding of the risk. In addition, they should seek knowledge, learning and information from their risk manager peers and external groups so that they are in a better position to challenge and take action.

The ultimate destroyer

Maurizio Micale, corporate ERM & insurance management director, STMicroelectronics

In the last three to five years, the cyber risk landscape has changed dramatically. Cyber risk is now a very imminent threat, which could ultimately destroy the image and the reputation of all businesses. No one business sector can be retained not vulnerable by cyber threats because of the combination of the pervasiveness of microelectronics and internet and the interconnectivity of any devices throughout wireless and mobile applications.

A good risk manager will do their best to raise awareness and try to develop cyber risk loss prevention and risk control, with the constant involvement of internal and external specialists. As cyber risk is constantly changing, the systematic risk identification and evaluation processes are critical and will help establish adequate and effective preventive and post-event recovery plans. Prevention and control measures should also be monitored, evaluated and upgraded regularly.

Cyber insurance is currently and definitely not the complete solution for cyber risks.

Cyber risk scenarios are constantly evolving and can stem from traditional IT infrastructures, which are the primary targets, to any kind of products or devices interconnected via internet to servers and mainframes.

Recently, car-makers have experienced cyber-attacks to their last-generation vehicles. In the future, third-party liability claims will increase, possibly resulting in insurance litigations.

Safety first

Drawing up a cyber risk management plan frequently leads to IT and the C-suite butting heads. The dangers of being unprepared, however, hardly bear thinking about

The most crucial aspect of a cyber risk management plan is that is it needs to be created ahead of time, before a business has experienced a cyber event. Swiss Re Corporate Solutions claims expert Catherine Lyle says: "You must perform penetration testing, which is something that's part of the IBM – Swiss Re Corporate Solutions agreement to offer advanced cyber risk protection. After that, the risk manager will go back and work with IT on lessons learned."

The human risk is an important factor when it comes to creating a secure cyber risk management plan, according to IBM Security Europe associate partner, Serdar Cabuk.

"When you get a risk management plan down, it is a full stance of security around technology. Your risk management should not just rely on tools and typically, one typical mistake is to start throwing technology at the cyber risk, which doesn't really work," he said.

"What you end up with is a lot of patchy solutions or point solutions that are not effectively used and that actually gives you a bit of an over reliance on technology and a bit of a false sense of security if you only use technology to start to try to fix your cyber risk issues. Start with the human risk but use technology the right way, in an integrative way, in a cognitive way, to manage your cyber risk," he added.

According to experts, risk managers have a unique role to play when it comes to cyber risk because they often act as an intermediary between two groups that do not always communicate well with each other and can have opposing desires. "On the one hand, you have the members of the C-suite who are focused on costs and the bottom line. In other words, the health and wealth of the corporation. On the other hand, you have IT, which is focused on the systems and prevention of a cyber event. Sometimes the views of those two groups don't correlate; they don't coincide," adds Lyle.

BALANCED VIEWPOINT

A risk manager must create a team that can balance each point of view effectively, according to Lyle.

"Once you have those grouped, I think the best way to do this is then to create a team with members from each of these stakeholder groups and have them assist in the creation of the cyber response plan. It's basically having buy-in before you need the plan to be in place. This all must be done before an event occurs."

Company-wide cyber risk assessments are a vital part of any prevention plan.

Kevin Kalinich, global practice leader for cyber/network risk at Aon Risk Solutions, says: "Given the evolving nature and complexity of cyber exposures, we found that the use of cyber risk assessments is surprisingly low."

He adds: "Conducting such an assessment is a useful tool for improving risk understanding and maturity, as well as for helping organisations better prepare for potential business interruption during or after a breach." ●

OF THOSE THAT DO, 68% OF COMPANIES SURVEYED BUY CYBER FOR BALANCE SHEET PROTECTION, CLOSELY FOLLOWED BY ENSURING DUE DILIGENCE COMFORT FOR THE BOARD

AON GLOBAL RISK CONSULTING CAPTIVE CYBER SURVEY 2016

Aon recommends the following three steps for a cyber risk assessment:

Scenario analysis:
Benchmark the existing cyber risk profile and work with business stakeholders to prioritise cyber risk scenarios.

Financial modelling:
Leverage advanced financial simulation tools using deterministic modelling to quantify first and third-party costs of select cyber scenarios. Consider performing an analysis on non-damage business interruption scenarios using forensic accounting capabilities.

Insurability risk review:
Test the adequacy of limits against the assessed cyber risk and review the optimisation of the proposed insurance programme.

Once a plan is being executed, the next stage of successful cyber risk mitigation is to remember that "people are the perimeter", says Fifth Step chief executive Darren Wray. "Make sure that your people have awareness of the landscape, of the environment that we live in. It's synonymous with when we teach children how to cross the road. We assume everyone knows how to use a computer today and how to stay safe online, but they really don't." Wray adds that cyber criminals are using tactics that can snare even the most tech-savvy employee. "We need to help people. We need to help employees and staff understand how to keep themselves safe, both for their personal safety and for the benefit of the organisation's safety."

Importantly, cyber risk management plans must be under constant scrutiny. Airmic board member Tracey Skinner says there is no such thing as a 'job done' moment when it comes to the creation of a cyber risk management plan. "It's very much an ongoing process because all of the pieces are constantly changing. Your use of technology within your organisation is changing daily. Your cyber criminal is changing daily. The impact on your business will be changing, so all of those things need to be monitored."

The nature of the business means people resources are not static and require a higher degree of flexibility, she adds. "Teams change, so you can have people around a table and give them training so they understand what the issues are. They understand how they're going to be dealing with the situation. All of these issues are kind of scoped out and three months later, somebody that was at that table may not be at that table any more. You need to identify that risk. You need to make sure all the players are fully up to speed as to what their roles are and what they'll be doing on the day. Then, test it and test it again."

Eye on the ball

A company's first response to a cyber attack, hopefully fine-tuned in advance, is critical to its reputation – but as the dust settles, legal considerations and incident reviews loom large

What to do when the worst happens is a vital part of any risk management plan. Despite the best efforts of risk managers, the likelihood of an attack is ever-increasing, so it is important for businesses to be ready when one does happen. "The important aspect of this is that you have to be prepared for attack," says Fifth Step chief executive Darren Wray. "Most organisations will suffer a data loss, a data breach or a hacking incident. Therefore you need to have an incident response plan."

Experts agree that a firm's immediate response to a cyber attack is what will minimise the damage to both brand and reputation. Airmic board member Tracey Skinner agrees: "I think this is probably one of the most important points in the whole issue in terms of what happens next. This is where there will be clear differences between organisations who have placed cyber risk high up on the agenda. They have gone through exercises and have a full, detailed contingency plan in place which has all the operational pieces – IT, HR, communications, C-suites – clicked in together with a plan. The organisations that have not placed cyber high on the risk agenda are those who may attempt to deal with a breach as a traditional risk. From those companies, you may not see so much connectivity to other parts of the group and there could be delays in communication which will impact the company as as a result."

IMMEDIATE ACTION

"You've got to have a good incident response plan," says Wray. "You've got be able to shut down that access as quickly as possible. You've got to be able to have a good communication plan in place to keep stakeholders informed. They may be internal stakeholders. They may be shareholders or individual investors. They may be clients and customers that you need to identify and inform. You've got to have a good communication plan in there so that the right information is released. Preparing an incident report plan right now, before you know you need to use it, is absolutely imperative for all organisations because you never know when one of these attacks is going to strike."

As well as saying the right thing when a breach occurs, it is important to know when to address an issue publicly. DAC Beachcroft partner Hans Allnutt says: "There is an argument to say if you have these incidents, you don't need to tell anyone about it. That is changing. People are voluntarily notifying now, which they didn't before. No longer can you stick your head in the sand. As a legal obligation, we're having to tell regulators and affected people of serious breaches."

It isn't simply about financial penalties, which could be claimed on insurance. Future insurance

policies could also be affected by changes in the law regarding unnecessary data. Allnutt says: "A big thing that firms miss in terms of the legal aspects of cyber risk is businesses think it's all about security and getting fines, penalties and being sued when you lose data. Absolutely, that is a key aspect of it – but actually, the liabilities and the questions in the years to come will be about what the company was doing with the data and whether they were holding it lawfully.

"Security breaches are now often highlighting these questions which need to be answered. People are purely focusing on securing data and not losing it, but the question now is once you've secured it or take the steps to secure it, at the same time you've got to be making sure you are holding the data lawfully."

Swiss Re Corporate Solutions claims expert Catherine Lyle says businesses can never take their eye off the ball. "Criminals are forever changing and they're forever evolving. They're staying one step ahead. You also have to keep in mind that a response plan is just that, a response plan. It is meant to respond to an event. It is created with the expectation of its use. So it is not a prevention plan or a wall. Following a cyber event or each quarter moving forward, risk managers should review the incidents that they're seeing and make changes where changes should occur with the input of each of the stakeholders. As these criminal hackers evolve, so should a company's response plan."

95% OF COMPANIES SURVEYED STATE CLEAR POLICY WORDING AS THE MOST IMPORTANT ISSUE IN THE CYBER RISK MARKET, AND 75% OF LARGE COMPANIES EXPRESS CONCERNS ABOUT THE LOSS-ADJUSTMENT PROCESS

AON GLOBAL RISK CONSULTING CAPTIVE CYBER SURVEY 2016


Swiss Re
Corporate Solutions
Our
cyber insurance
+
IBM
security expertise
=
Two industry
leaders
joining forces
Help protect your company. Use the Swiss Re and IBM® cyber security solution.
swissre.com/cybersolutions
We're smarter together
Swiss Re Corporate Solutions offers the above products through carriers that are allowed to operate in the relevant type of insurance or reinsurance in individual jurisdictions. Availability of products varies by jurisdiction and products may not be available in all U.S. States, Brazil or Colombia. Products underwritten by member carriers including North American Specialty Insurance Company in the U.S., Swiss Re Corporate Solutions Brasil Seguros S.A. in Brazil, and Confianza S.A. in Colombia. This communication is not intended as a solicitation to purchase (re)insurance. IBM is a trademark of International Business Machines Corp. registered in many jurisdictions worldwide.