IDPP

International journal for the
Data Protection Officer
Privacy Officer
Privacy Counsel

JOURNAL ADDRESSES

Personal data | Privacy | Data protection | Law, regulation and caselaw | The new DPO profession | Compliance | Independence and conflict | Resources | Records | GDPR | Ethics | Security incidents and notifications | Breach notification | Pre-problem solving | PbD/DPbD | Audits and assessment | Education, training and programmes | Solutions and systems | Resource update review |

ISSUE INCLUDES

2018 VOLUME 2 ISSUE 4

NOT ALL

BURGLARS

WEAR BALACLAVAS.

You are over 40% more likely to be a victim of cyber crime than a burglary. If you do fall victim, Hiscox will get you back up and running fast.

Specialist business insurance.

HISCOX
EVER ONWARDS

International journal for the
Data Protection Officer
Privacy Officer
Privacy Counsel

Contents

Insurance and Data Breaches

Subscriptions
Subscriptions are available by contacting: lex@mydistillex.com.

Submissions
Submissions are invited and should be sent to lex@mydistillex.com.

Advertising
Advertising opportunities are available and requests should be sent to lex@mydistillex.com.

Disclaimer
The views expressed in the content submitted are those of the authors and do not necessarily reflect the views of the IDPP, its editors or publishers. Contributions and views contained in the journal are not intended as, and do not constitute, legal advice and are not a substitute for same.

Contact
IDPP, 7 Dunbo Hill, Howth, D13, Ireland. Contact: lex@mydistillex.com

KLARA MILETIČ ▲ Partner, Wolf Theiss, Ljubljana

South Africa
DANIE STRACHAN ▲ Adams and Adams, Pretoria

Spain
JOSÉ M BAÑO FOS ▲ Baño Leon Abogados, Madrid

Taiwan
VINCENT HUANG ▲ Deknow Technology Services, Taipei

Tanzania
ALEX B. MAKULILO ▲ Faculty of Law, Open University of Tanzania, Dar es Salaam

UAE
SHAHAB AHMED ▲ JD, MBA, Managing Counsel, Lead Group Privacy Counsel, Etihad Airways, Dubai
BRIAN MEENAGH ▲ *OMAR M. ELSAYED* ▲ Partner, Latham & Watkins, Riyadh

UK
SUSAN SINGLETON ▲ Singletons, Solicitors, London

Uruguay
FEDERICO FLORIN ▲ Guyer & Regules, Montevideo

US
VICTORIA L. SCHWARTZ JD ▲ Professor of Law, Co-Director, LLM and Certificate Programs in Entertainment, Media & Sports Law Pepperdine
SEAN M. SOLON ▲ Consultant, Colorado

Editorial

Data breach issues are an unfortunate fact of modern life and modern business. The number of breaches, the frequencies and scale of breaches and the increasing number of individuals and organisation whom are attacked are also very pertinent factors. Some have suggested that it is not a question of if an organisation will suffer a breach, but rather a question of when. Against such a climate, no business or organisation can afford to ignore the necessity for cyber insurance or data breach insurance.

The cost of recovering from a data breach has been one of the more significant reasons for considering data breach insurance. However, more recently other important factors also jump out. These include claims and class actions from affected users, regulatory reporting and investigation (note that the GDPR, for example, required data breach reporting, as do comparable laws in the US; and also enhances the possibility of class actions in the EU), massive media attention and adverse publicity, costs of dealing with the breach, cost of recovery, lost sales, tarnished corporate reputation.

New consequences and costs are continue to arise as the nature of attacks and the demands of hackers continue to evolve. The ransomware attack on the NHS and other institutions raises the stakes on new ways. In that instance, the critical health care of thousands of patients could have been affected with tragic consequences.

In the US there have also been examples of ransomware attacks on hospitals, schools and state bodies.

Given that these examples are known, there is less justification for an organisation to ignore any consideration of having cyber breach insurance. Over time it would seem almost inevitable that ignoring the need for data breach instance coverage might been seen as remiss, reckless and even negligent. This is particularly so where a company is public or has large and sophisticated shareholders.

On the other end of the scale, just because an organisation might be official or a charity does not remove the risks, nor the need to security and appropriate insurance.

Gareth Wharton, the Cyber CEO of Hiscox Insurance provides the lead article and details how more businesses are taking insurance cover from data breaches.

Debbie Reynolds of EimerStahl Discovery Solutions details some of the increasingly nuance involved in the details of data breach effects. Carla Borda of R&R Insurance Services sets about detailing an understanding od cyber risk insurance issues and consequences. Monica Schlesinger refers to optimal models for cyber insurance, including a number of casestudies.

Ken Goldstein highlights “10 Considerations for Data Breaches and Privacy Losses Insurance” which every organization, and officers from data protection to security to board should be aware of.

Dr PB Lambert
editor

More Businesses Take Cover from Data Breaches

Gareth Wharton

Introduction

Data breaches come in so many different shapes and sizes these days that many organisations now prefer to transfer that risk to insurers, explains Gareth Wharton, Hiscox's Cyber CEO.

For many organisations, public or private, the risk of either losing - or just as importantly, losing *access to* - their own information has grown to become one of the biggest threats they now face. The risk is so varied - from an employee sending information to the wrong person or losing a USB stick, to a cyber attack by hactivists, professional cyber criminals or even nation states - that many organisations find it difficult to understand how to properly protect their data.

That is why more and more are buying insurance to help them cope with the potentially devastating fallout from a hacker attack or data breach. For the two thirds of companies that do not have a strategy to respond to a cyber attack, according to analysis by the World Economic Forum, cyber and data insurance offers a comprehensive response plan if a crisis occurs, with a group of experts on call to help get them back up and running again as quickly as possible.

Common Myths About Data Breaches

Although organisations' awareness of the threat is increasing, we find there are still some enduring misconceptions about the danger and who is at risk.

"Why Would We Be Attacked?"

Many still assume that attacks are carried out against carefully chosen targets, either because they have deep pockets, hordes of sensitive information or are controversial.

But many have already fallen victim to attack for no other reason than they use a particular computer software program. In 2017, the WannaCry and NotPetya viruses infected hundreds of thousands of PCs by exploiting vulnerabilities in Microsoft Windows. NotPetya seriously hit organisations ranging from shipping giant Maersk to parts of the NHS but for no clear motive. Although it purported to be ransomware, the virus's primary intention seemed to be to make mayhem, rather than money.

"We're Too Small/Uninteresting for Cyber Attackers to Bother With"

Many organisations think they won't be targeted either because they're too small or because the information they hold is not worth enough for a hacker to bother with them.

But, if your data is valuable to you then it will be valuable to a cyber criminal. And those that do not see themselves as vulnerable tend to be easier targets because they do not protect themselves as much as others. We've paid claims from high street businesses, including a local restaurant and opticians, which were crippled for days by ransomware that locked them out of their computer systems. Ask yourself how long you could operate without your core computer systems? Days? Hours? Minutes?

The Biggest Sources of Attacks

Cyber attacks are today's white-collar crime of choice. It is seen by organisations to be their biggest risk as well as the one that is most likely to intensify this year, according to the World Economic Forum's Global Risks Report. But organisations are struggling to get to grips with

the threat, because they tend to focus more on preventing an attack than on how to recover from one, the report suggests. They need to do more to increase their resilience so they can cope better with the consequences of an attack, it states.

Ransomware

Ransomware attacks are by far the biggest problem experienced by our clients, accounting for nearly 40% of our claims. Most are carried out by criminal gangs attracted by the enormous rewards on offer from online extortion. They do not need to have much computer knowledge these days because it's possible to buy DIY ransomware kits off the Dark Web, or even to rent the services of professional hackers. These are no fly-by-night operations: they have teams who are on hand to help first-time victims buy the necessary bitcoins to pay their ransoms - some even offer payment plans.

Attacks are now being run on an industrial scale, so much so that our research suggests you now have an almost even chance of being attacked. Nearly half (45%) of the more than 4,000 organisations surveyed for our Cyber Readiness Report 2018 suffered an attack in the past 12 months, with financial services, energy, telecoms and government organisations being hackers' main targets.

Phishing Attacks

The techniques used by cyber attackers are increasingly sophisticated. Phishing attacks were once relatively crude mass spam campaigns, but they are now so authentic that even many experts have trouble in spotting them because they use logos, typefaces, signatures and email addresses that are almost indistinguishable from the real thing.

Attackers will also use public information, such as someone's social media activity, to create tailored phishing emails in the hope of duping recipients, known as social engineering. They will try to trick them into downloading malicious software onto their systems, either ransomware or spyware, which monitors the user's keystrokes. Or they may try to use stolen username and passwords to break into people's email accounts or their user profiles on their work systems.

Although the methods differ, their purpose is the same: to steal data, like credit card details or bank account information, or to extort money, by threatening to put the data up for sale on the Dark Web unless the company pays. Hotels and leisure businesses are particular targets for this style of attacks.

Payment Diversion Fraud

As well as stealing information, cyber criminals try to trick people into sending money to accounts they control. "Friday afternoon frauds", as the name implies, seek to catch out busy finance or accounts teams by conning them into paying what appear to be genuine invoices from regular contractors or suppliers into fake accounts. Lawyers and building firms are frequently targeted because they regularly transfer of large sums of money - £85 million was reportedly stolen from law firms in "Friday afternoon frauds" in an 18-month period to March 2016.

"Man in the middle frauds", also known as "man in the email frauds", are another common ploy, where hackers use spyware to eavesdrop on email conversations and will pose as one of the parties in bogus emails to trick the other into sending money to an alternate, fraudulent account.

But attacks increasingly come in all shapes and sizes. Production ground to a halt at a German bakery because hackers got into its network and managed to switch off its computer-controlled ovens. As one of our clients, we were able to help it begin operating again quickly, but any connection between your systems and the internet makes your

organisation vulnerable, especially if it doesn't have strong firewalls to prevent hackers from penetrating deep into your system.

"We're Safe, Our Data's in the Cloud"

This is something we've also heard. The cloud has been revolutionary, but organisations need to bear in mind a number of important things about it.

Some cloud providers do offer great security, but the cloud is not a virtual Fort Knox. It never can be if it is connected to your systems down on the ground. We have seen instances when ransomware downloaded onto an organisation's network has infected and encrypted its data stored in the cloud.

It is your responsibility to keep your data safe, not your cloud provider's. The data-protection authorities will hold you accountable if your information is compromised or lost, even if it was your cloud service provider's fault.

The cloud can go down. An outage at Amazon Web Services lasting four hours in February 2017 caused hundreds of thousands of US websites it hosted to go down. The reliance of both private and public-sector organisations on the cloud has grown to such an extent that analysis in the WEF's Global Risks Report 2018 found that if just one of the major cloud providers was taken down it could cost somewhere between $50 billion and $120 billion.

If you have a problem with your systems then you want to know what is gone wrong, and what is being done to put it right. But if the problem is up in the cloud then you may not have all the information you need to explain to your clients and business partners what is being done to fix the situation. By the time you find out what is happening it could already be too late to prevent your reputation from being damaged.

You also should not think that a cloud provider would reimburse you for any business you lose if your operations were put out of action. You might be offered credits for the time their services were down, but you're unlikely to get much else.

So, while the cloud is great, it's worth considering that, without any back-up plan, a data breach could cost your organisation a lot more money than it is saving by using the cloud.

The Human Factor

Your organisation might have sophisticated anti-virus protection, strong firewalls or store your data in the cloud with a provider that has cutting-edge security. But you are only as strong as your weakest link.

Simple mistakes, rather than cyber attacks, account for most data breaches. Four of the five most frequent causes of lost personal information dealt with by the Information Commissioner's Office in the final quarter of 2017/18 were due to human error: lost paperwork, information sent to the wrong person and the loss or theft of a device on which information was stored unencrypted.

In the 18 months to September 2017, we found that 67% of the cyber-related insurance claims we received from businesses were caused directly by employee error, negligence or social engineering. Two mistakes - divulging sensitive information like passwords, or simply losing a device or documents - resulted in 8% of the cyber claims we received.

In our recent Cyber Readiness Report we consistently found that the best prepared organisations were those that implemented security training and awareness throughout their workforce. Over 80% of those said employee training has reduced the number of cyber incidents that disrupt their businesses and employee training was present at almost every

company (97%) that ranked as “Cyber Expert.” This figure was under 40% for those businesses ranked as “Cyber Novices.”

An organisation’s data security culture is crucial in helping prevent data breaches. GDPR demands that “appropriate technical and organisational measures” are put in place to ensure people’s information is kept safe. Regulators could take tough action against those organisations that suffer a breach and whose processes and training are subsequently found wanting.

Some staff members might not understand why they need to take care when taking work home, why they need to have strong, unique passwords that are updated regularly, or why it can be risky to log into the network using one of their own devices.

That is why Hiscox offers its cyber and data insurance policyholders that are UK organisations with a turnover of less than £10 million access to its CyberClear Academy, which has been accredited by GCHQ, the UK’s intelligence agency responsible for cyber security. It is an online interactive suite of training modules to help their employees understand the risks of phishing or social engineering attacks and therefore reduce the risk of their organisation falling victim to a hack.

Patching Things Up

The string of high-profile malware attacks in the past couple of years has also put organisations’ IT-security processes under the spotlight. Many could have avoided falling victim to last year’s Wannacry virus if they’d upgraded their systems quicker, as Microsoft issued its first patch against the EternalBlue exploit nearly two months before it was used to propagate the Wannacry virus.

Organisations that in future fall victim to an attack because they have not kept their network security up to date might face more scrutiny, including potential lawsuits from investors or customers for failing to ensure they took the necessary precautions to prevent a cyber attack. Insurers might also dispute some claims, such as for the business interruption suffered from operations being out of action from an attack that was easily preventable.

Data security is a combination of three factors: people, process and technology. You can have the best technology available but if your processes are not tight or your staff does not understand how their actions could have major repercussions then your organisation will be vulnerable.

Cyber Insurance

An insurance policy offers a comprehensive crisis response to a wide range of events, from a dedicated denial of service attack to a malware outbreak or a lost laptop.

Dealing with a data breach can be a complicated and arduous exercise. It takes more than six months on average for an organisation to realise it has suffered a data loss, according to research by the Ponemon Institute, and the longer it takes to detect a problem the more expensive it is to handle.

It is not hard to see why. Working out what information has been lost and who is affected among your customers, employees and business partners can be a painstakingly detailed process. If malware has got onto your network then you need to quickly discover which type it is so you can combat it, before trying to get your systems back online and restoring as much of your data as quickly as you can.

GDPR dictates that every data breach must be reported to the data watchdog within 72 hours. But knowing how to contact the regulator (and if you have lost foreign customers’

information you will need to liaise with several supervisory bodies), what to tell them and how to update them about your breach is a daunting prospect for those who have never had to do it before.

Affected clients will also have to be informed quickly, and you might need to provide clients with support and assistance if necessary, such as an advice hotline or even credit monitoring if their personal identifiable information has been lost.

That can be very expensive. In 2017, the average cost of notifying regulators and customers of a data breach for UK organisations was around £120,000, according to the Ponemon Institute.

You will probably also need to deal with the fallout from the press and public, who will want to know what is gone wrong and whether you can still be trusted. For many, the cost of business lost following a breach is higher than dealing with the incident itself.

All of that is likely to involve the services of IT experts, lawyers, PR consultants and perhaps even crisis negotiators, if hackers demand a ransom to restore access to your computer system. Many organisations will not have suffered an incident like this before, so most IT Directors, Chief Information Officers or Chief Technology Officers will not have these companies on their speed-dial list.

Cyber and data risks insurance isn't a conventional policy. Its purpose is to get clients back up and running again as quickly as possible, rather than simply paying for the damage they have suffered. It offers organisations the peace of mind of knowing that if they have an emergency they have a number to ring day or night to mobilise a team of experts that will work with them to deal with it.

A cyber policy can also include:

- Payment for loss of income resulting from a cyber-attack;
- Compensation for any damage done to your systems and data by hackers;
- Protection against cyber extortion demands;
- Compensation and defence costs for claims of breaches of privacy, defamation; or intellectual property rights.

The string of malware attacks and data breaches in recent years has been a wake-up call for every business of the threat they face. Many are looking to transfer some or all of that risk to insurers. The cyber and data risks insurance market is forecast to grow by over 25% each year for the next ten years, to over $37 billion in premiums by 2027, according to research by Visiongain. Many organisations now see cyber insurance as an essential part of their risk management toolbox.

Gareth Wharton
Hiscox's Cyber CEO

The Increasingly Complex Issues Involved in Data Breach Fallout

Debbie Reynolds

Introduction

A data breach can be one of the most devastating and disorienting types of business loss events to occur to companies because of the massive expenses, legal pressures to respond quickly, and vigilant efforts required to halt or prevent future breach events. Companies have been bolstering their cybersecurity capabilities to guard against the persistent wave of data breaches which seem to be occurring globally with more frequency and with increasingly devastating effects. In the digital age, where data is like "the new gold," companies strive to operate in ways that will safeguard the data in their possession, continue uninterrupted business operations, retain their revenues, and maintain their reputations. Although no organization wishes to be the victim of a data breach, it is vital that companies proactively develop comprehensive and actionable plans to navigate any data breach event. As organizations control growing volumes of valuable information, both the global data privacy and cybersecurity landscapes are becoming more demanding due to a variety of new regulatory requirements currently being brought into full force. Also, while navigating these new regulatory requirements, it is critical to closely reevaluate an organization's cyber insurance coverage to be fully aware of what is protected and to address any gaps that may increase a company's business vulnerability in the event of a data breach. Three key areas creating increased complexity in managing a data breach fallout will be navigating impact of data privacy and cybersecurity laws, managing data breach notifications, and reevaluating cyber insurance policies.

Impact Data Privacy and Cybersecurity Laws

As illustrated in the EU's most recent major data privacy and cybersecurity frameworks, the General Data Protection Regulation (GDPR)[1] and the Network and Information Systems Directive (NIS)[2], are already having significant ripple effects around the world on how organizations handle data entrusted to them. The GDPR is focused on the handling of personal data about EU persons, regardless of where their data is located in the world, with fines that can reach up to four percent of an organizations' worldwide gross annual revenue or 20 million pounds, whichever is greater. The NIS is focused on the EU cybersecurity protection of operators of essential services (OES), like energy, transport, health, digital infrastructure, etc., and digital service providers (DSP), like search engines, cloud providers, and online marketplaces, with fines that can reach up 17 million pounds. These rigorous data privacy and cybersecurity frameworks are complex for companies to navigate both inside and outside of the EU. Both the GDPR and the NIS support proactive accepted measures to prevent or minimize the damage of data breaches, like the need for risk assessments, data encryption, and incident response management. Although both the GDPR data privacy and NIS cybersecurity frameworks serve different purposes, in the event of a data breach, companies to whom both the GDPR and the NIS apply, could potentially draw substantial monetary penalties from both the GDPR and NIS authorities for a single data breach event. The overlap in the fine for data breach for the GDPR and the NIS could create a kind of "double jeopardy" situation for companies who could be fined under both

1 General Data Protection Regulation - (GDPR) - Regulation (EU) 2016/679, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679.

2 Network and Information Systems Directive - (NIS) - DIRECTIVE (EU) 2016/1148, https://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ:L:2016:194:TOC&uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG.

frameworks. Also, the NIS directive is not a regulation like the GDPR, which means the NIS can be implemented differently into laws for each EU member state, with additional requirements and potentially different penalties that may be applied based on the EU member state in which a company is operating. Though the EU authorities for the GDPR and the NIS can coordinate efforts and share information, it remains to be seen how complicated data breach events will be managed when both the GDPR and the NIS apply.

Some major tech companies, in their race toward full GDPR compliance, have started to simplify their data privacy policies and update their terms and conditions, not only for persons in the EU but to customers around the world. Many of us anywhere in the world now are likely navigating to our favorite websites while having to newly agree or dismiss pop-up notices about tracking cookies and other information that websites retain about us, or the accept the new terms of service for digital services to continue their use. The GDPR has set a very high standard for the handling of data about EU persons, and some of the fundamental changes that are needed for companies to comply with GDPR may result in changes that will impact the way these companies do business and, in turn, affect non-EU consumers of their services.

The NIS directive, although it is more targeted in this mission is no less transformative. The NIS directive is a focused EU cybersecurity framework aimed at organizations who provide essential services and companies who support them. The purpose of the NIS directive is to cause the proactive improvement of cybersecurity for both private and public sector companies which may be used as a guide for countries around the world to protect their vital data assets against cyber threats.

Managing Data Breach Notification

Data breaches draw the rapid attention of government regulating bodies, impacted parties, and consumers. Most data breach notifications are required, at a minimum to address; what data was breached; who is affected by the data breach; what is the damage or consequences of the data breach; and what measures will be taken to minimized or contain the data breach. To quickly gather these notification details in the event of a data breach, it requires proactive pre-event efforts by organizations to target and provide the necessary evidence as soon as possible.

Companies may be required to notify one or more regulators, depending on their locality and jurisdiction, as well as contacting any affected parties or customers. Regulators have some flexibility in determining how severe penalties should be when levied against organizations and what remedies are best to address impacted parties and customers. Data breach reporting timeframes (from hours to days) and governing agencies may vary in different countries. For example, the EU's GDPR and NIS frameworks have initial data breach notification timeframes of 72 hours or less which is extraordinarily abbreviated and among the most rigorous in the world. As companies around the world begin to demonstrate their ability to comply with the EU's abbreviated data breach notification timeframes in the GDPR and the NIS, it is likely that other countries, who now have different notification periods will begin to adopt the 72 EU data breach notification timeframe as their new standard.

Evaluating Cyber Insurance

Cyber insurance is quickly moving from being elective indemnification protection to a modern-day business necessity. When companies handle more valuable data, their cyber risks increase. Losses that businesses would otherwise absorb without cyber insurance may, not only, be financially damaging, but the cost of responding to a data breach incident could put these companies out of business. The marketplace for cyber insurance is continuing to evolve and mature; as a result, not all cyber insurance policies are created equal. Even those companies who have cyber insurance should reevaluate their indemnification plans periodically as cyber risks and laws that impact a company's cyber

liability may change rapidly. Although cyber liability limits vary widely based on the cyber policy that companies carry, most cyber insurance policies will cover; the data breach incident (like data hack, theft, intrusion); the business damage, (like data loss, business interruption); and the response to the data breach incident, (like customer contact, public relations, IT resources to contain or eliminate the data breach). Some cyber insurance policies may not cover things like lost business due to reputational damage, funding technology improvements needed to make the company more cyber secure after a data breach event, or massive regulatory or legal fines. Higher regulatory requirements for a company's 'data and cyber management will likely become a factor cyber insurability, increased coverage deductibles, and higher insurance premiums. However, it remains to be seen if a company, who is fined the maximum four percent of the worldwide turnover under the GDPR, would have a cyber insurance policy provider that would cover most or all of this massive regulatory penalty.

As enforcement actions begin and hefty penalties are levied, as part of GDPR data privacy and NIS cybersecurity frameworks, it will be interesting to see how companies and insurers adjust and change their ways of doing business to survive a data breach fallout.

Debbie Reynolds
Director of EimerStahl Discovery Solutions llc, an affiliate of Eimer Stahl LLP, advises Fortune 500 companies on data privacy and the management of electronic evidence in high-stakes litigation. Ms. Reynolds also is an adjunct professor at Georgetown University, a guest lecturer for various U.S. Law Schools, a published author, and speaker on the impact of global data privacy in legal matters.

Understanding Cyber Risk and Insurance

Carla Borda

Crimes using a computer are being committed globally every day. The insurance industry identified this as a risk decades ago and still has not reached any conclusion on the best way to insure for this risk. There are over 100 variations of cyber insurance available in the market today. These range from stand alone policies to endorsements on almost every conceivable policy. The availability of an insurance product does not mean that they are all insuring the same risk.

Unlike the most common of risks, wind, flood, theft, fire, etc. crimes using the computer, and more specifically computer code, are difficult for the lay person to identify and understand. Technology is driving rapid change in the way business is conducted. The side effect of technological advancement is an increase in risk, one that may not be apparent.

According to a report recently published by Lloyd's *Counting the cost-cyber exposure decoded,* cyber attacks were the 12th largest business risk in 2017. By way of contrast, natural disasters ranked 20th. Computer code is never released error free, per the report. The industry average number of bugs for every 1000 lines of code range from 15-50 bugs. Bugs lead to vulnerabilities which lead to network attacks, data breaches, and ransomware.

You may think that insuring for a data breach or privacy wrongful act is standard in policies. Policies may say "privacy wrongful act" but how the act is committed varies from policy to policy. Is the breach the result of "any unintentional violation of any privacy or cyber law", "unauthorized access to, misappropriation, disclosure, accidental release or failure to protect confidential information", or the "insured's unintentional and unauthorized disclosure or loss of non-public personal information"? In addition, will the policy respond if the breach was caused by a third party and does the information include third party confidential information/intellectual property/trade secrets? Not all information is stored electronically. Many companies maintain paper records and files. Will the insurance respond only if the data is stored electronically? Of real concern is a policy that contained warranty language "*provided that no senior executive knew of or had reason to know of any such conduct*" that caused the breach.

Because a computer is being used to perpetrate crime, is this risk insured as computer fraud or cyber? The answer is "it depends". In *American Health Inc. v Dr. Sergio Chevere,* 2017 WL 6561156 (12/22/17), the District Court made the following distinction:

1) acts in which a computer is the target of the malicious activity

2) acts in which a computer is used as a tool that is essential for the malicious activity

3) acts in which the use of a computer is incidental to the malicious activity

Depending on the details coverage could exist under either the Crime form or the Cyber form. Not every cyber policy insures for crime. Not every crime policy insures for all types of crime using the computer. Most crime policies require that the instruction going into the computer be fraudulent. This is a distinction especially when the user is tricked into transferring money as a form of social engineering fraud. A crime committed using a

computer does not mean it is an insured crime. Some, but not all cyber policies will insure for this type of loss either.

Global ransomware damage costs are predicted to hit $11.5 billion by 2019, according to a report from Cybersecurity Ventures. They also predict that there will be a ransomware attack on businesses every 14 seconds by the end of 2019. The insurance covering ransomware/extortion is available on many cyber policies. However, it is important to understand the details on what constitutes “money” paid to the criminal to either stop the attack and/or prevent the release of confidential information. If the definition of “money” is limited to “cash” the policy probably will not be much help. The definition should include cyptocurrencies, digital currencies, and virtual currencies even though not all policies do.

When cyber policies were first introduced, computer networks were fairly simple — two or more computers connected to a server. Many policies intertwine Privacy and Network Security. If a breach occurs due to a network attack or the breach must be triggered by a network attack, it is important to understand what constitutes “network”. Technology has enabled shared systems, including data hosting, cloud services, data processing, platforms, software as a service and infrastructure as a service. Artificial intelligence and blockchain add another dimension. If your network doesn’t match with the definition in the policy gaps and coverage denials are imminent.

One of the important aspects of insuring this risk that is often overlooked are the responsibilities of the insurer following an actual or suspected loss. Many policies are written on a reimbursement basis which puts the insured in position to manage the situation which can be complex and time consuming. Other policies are written on a duty to defend basis which shifts management to the insurance carrier. And others reimburse in certain situations and pay on behalf of in others. Does the carrier offer vendor relationships to provide outside services such as forensics, legal, notifications, and post breach services (credit monitoring, ID theft repair, social media monitoring, and medical ID monitoring)? If not, it would be important to have those vendors under contract and to make sure that the carrier has approved use of your vendors.

Understanding the risk is half of the battle when it comes to insuring the risk. As complex as the technological world is the insurance world is equally complex. There is no standardization in coverage, language, definitions, pricing, risk management services and post loss response. The policy that may work for you today, may not be the one to work tomorrow or next year.

Carla Borda
R&R Insurance Services

Optimal Models for Cyber Insurance for the SME/SMB Markets

Monica Schlesinger

Our Cyber World - Overview

Technology has changed the way we live and do business drastically over the past 20 years. Computers, networks and technologies have been designed to a large extent without security and privacy in mind, as in the beginning breaches were not as pervasive as they are now.

In 2012, retired General Keith Alexander, former Director of the National Security Agency from 2005 - 2014, stated that the loss of industrial information and intellectual property through cyber espionage constitutes the "*greatest transfer of wealth in history*."[1]

Intellectual property theft is only one of the drivers pushing the cyber security importance on the risk scale. The others being ransomware, cryptocurrency mining, identify theft, fraud, etc.

The Cyber Security Market

How Big is the Cyber Security Market? We can only be certain that it grows exponentially. Various forecasts and predictions are made, based on research done at Cybersecurity Ventures[2] who say that the global cost of cybercrime will double, from $3 trillion in 2015 to $6 trillion in 2021.

According to a research report published by MarketsandMarkets, the cyber security *Solutions* market size is expected to grow from USD 137.85 Billion in 2017 to USD 231.94 Billion by 2022 and at a Compound Annual Growth Rate (CAGR) of 11.0% during the forecast period.[3]

The market is driven by cyber terrorism and crime and the data protection directives and regulation.

The security breaches target businesses, individuals and governments. Many attacks are drive-by visiting websites, phishing, vishing (telephone scams), or by scanning the Internet for vulnerable PCs and servers. Cyber criminals don't discriminate and size of the organisation is not a main consideration.

The first hackers date back to 1903 (dealing with insults in Morse code), but the computer vulnerabilities started to appear in 1965. Two years later, in 1967, the first incidence of network penetration hacking was recorded. In the '80s and '90s however, the hackers were more motivated by bragging rights, disruption and fraud. In the '90s, the credit card criminals were already in operation. This forced laws to come into effect, criminalising any unauthorised access to a computer system.[4]

1 http://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/.
2 https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf.
3 https://www.marketsandmarkets.com/PressReleases/cyber-security.asp.
4 https://en.wikipedia.org/wiki/Computer_Misuse_Act_1990.

The 21st century saw an exponential increase in hacking and criminal activity. The initial hackers were technical experts, often young computer programmers who were testing the limits and possibilities of the machines. Over the last 15 years however, criminals have taken over these markets and the barrier to entry into the “hackers” club has dropped significantly. A “script kiddie” is the lowest level you can get, and it represents someone with hardly any skills to write code, but willing to purchase tools or parts of the hacking process at low prices from a smorgasbord of services on offer on the *Dark web*.

The web as we know it is only the tip of the iceberg, as it equates to the searchable and indexed sites that the search engines’ robots can find. This represents only 4% of the Internet. Underneath this known web there is the Deep web, sites that are not indexed and the Dark web. To get to the dark web, one needs other technologies and the usual browsers won’t reach the sites. The dark web can be accessed only via peer-to-peer applications and VPNs (Virtual Private Networks). TOR (The Onion Router) is a well known open source program that allows users to protect their privacy and security against the network surveillance. Initially used in the name of privacy, by journalists, the military, activists and law enforcement officers, it became the vehicle for cyber criminals.

Cyber Criminals

A Natural question is who are these cyber criminals and how many are operating out there? IBM Global Security Analysis Lab states that around 100,000 hackers worldwide are threatening our systems and networks:

- The Amateurs (cyberjoyriders) make up about 90%
- The potential professional hackers for hire (corporate spies) make up about 9.9%
- The world-class cybercriminals are only 0.1%

Cost of Attacks

How easy and inexpensive is it though to run attacks? A former consultant for the FBI scoured the Dark Web to see what was being sold. Here are some of the cybercrime price lists that he compiled for "Fortune"[5]:

Malware

- *Remote Access Trojan $200*
- *Password stealer $50*

Ransomware

- *Sophisticated license for widespread attacks $200*
- *Unsophisticated license for targeted attacks $50*
- *PC malware installation $1*
- *1 million malicious spam $400*

Software

- *Remote desktop control tool $100*
- *Distributed Denial of Service (DDoS) attack software $700*

Payment and Login Info

- *Credit/debit card for online use $5*
- *Credit/debit card info that can be cloned on plastic $10*
- *Bank account login (username and password) $5*

[5] https://www.komando.com/happening-now/426551/a-hackers-toolkit-shocking-what-you-can-buy-on-dark-web-for-a-few-bucks.

- *Bank account login with access to email, security answers etc. $25*
- *Existing PayPal account $1*

Personal Information
- *Social Security and date of birth verification $3*
- *Credit report 750+ credit score $150*

Database Records
- *1 million compromised email/passwords $25*

Hacking Services
- *Email account $100*
- *Social media account $100*
- *CMS website (WordPress, etc.) $300*

User Obfuscation
- *Bulletproof hosting in a lax jurisdiction (China, Eastern Europe, etc.) $150*
- *Virtual private network (VPN) $20*

Malware Services
- *PC malware installation $1*
- *Malicious file encryption $25*

Spam
- *500 SMS (Flooding) $20*
- *500 malicious email spam $400*
- *500 phone calls (Flooding) $20*
- *1 million email spam (legal) $200*

Fake Documents
- *Digital copy of fake credit/debit card $25*
- *Digital copy of fake driver's license or passport $25*
- *Digital copy of fake utility bill or Social Security card $15*

So price is not a barrier, nor is knowledge or expertise.

Targets of Attack

Who is the target of cyber attacks? The targets are not necessarily large companies – the target is anyone that has a computer and data that is of any value if stolen or encrypted. Often, the large companies have sufficient resources to recover from cyber attacks. The biggest issue is for the medium and small companies.

Insurance group AON has been producing the Cyber Insurance benchmark report since 2007. In the report from 2016, they noted that:

> *"Smaller companies, with less than USD 5 billion in revenue, put post-breach extended business interruption as a close second. This is typically because large companies have the prowess and financial wherewithal to recover from reputational losses caused by a cyber-related business interruption, whereas smaller companies are more vulnerable, especially when cyber attacks cause lengthy disruptions."*

In their most recent survey from 2017[6], the listed the top ten risks as seen by directors and company executives:

1. Damage to reputation/brand
2. Economic slowdown/slow recovery
3. Increasing competition
4. Regulatory/legislative changes
5. Cyber crime/hacking/viruses/malicious code
6. Failure to innovate
7. Failure to attract/retain top talent
8. Business interruption
9. Political risk/uncertainty
10. Third party liability

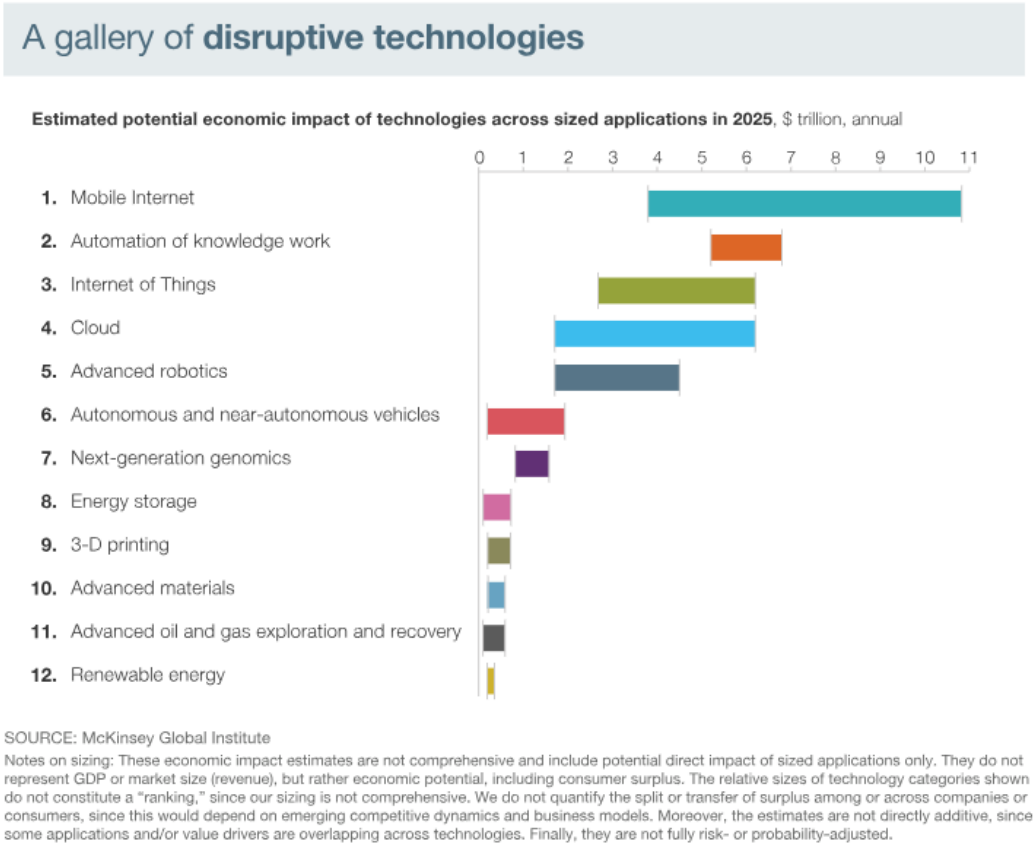
Cyber risk has maintained its place at number 5 on the list from the previous year.

Predictions are only upwards, as we become more and more entangled in the digital world we created. We are becoming more and more dependent on technology in all areas, our details are getting captured and stored by more and more government agencies and commercial companies.

A recent study done by McKinsey[7] shows the disruptive technologies' predictions to 2025. In more than one way, we are and will continue to be affected:

6 Aon 2017 Global Risk Management Survey.

7 https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/disruptive-technologies.



There is no way of going back to a "non-cyber environment".

As we become more and more connected, the risks of cyber attacks are growing. The measures to protect the networks, the data and the computers are not keeping the same pace.

We need to protect ourselves against the cyber risks at the individual level and in the corporations we work.

Risk in General

Risk management should be seen as a dynamic and never ending activity. It must be managed for the entire life of a business.

Risk management is usually documented in a Risk Management System document, Risk Policy, Risk Strategy and a *live* Risk Register.

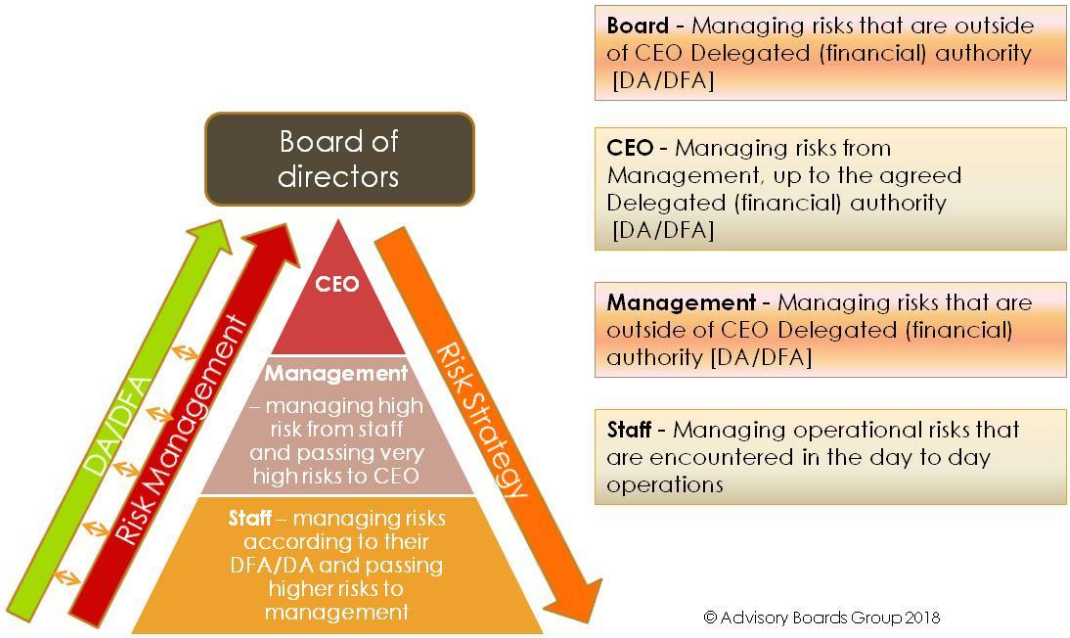
The risk register needs to be updated on a regular basis (weekly is a common frequency) with the Extreme and High risks reviewed by the Board.

Approaches to Risks can entail:

- Risk refusal – choose NOT to take the risk
- Risk acceptance – in order to pursue any business initiative organisations take risks
- Risk transfer – a part of the risk can be transferred to a third party (eg insurance company), but it can never be transferred in totality, as ultimately the board is held responsible for extreme and high risks

- Risk mitigation or management – the probability, the impact or the exposure can be mitigated or decreased; sometimes, any of these three aspects can increase due to linked events or circumstances

The Risk should be treated with a pyramid style approach, whereby the risk management is done upwards, in close connection to the DA (Delegated Authority) and DFA (Delegated Financial Authority), whilst the Risk Strategy including the Risk appetite flows down the layers of the organization and stems from the Board of Directors.



The Cyber Risk Fit

Where does the Cyber Risk fit and why? The risk of getting out of business, which happens in over 60% of cases for Small to medium enterprises/businesses[8] has not entered all the boardrooms as yet, despite having a lot of publicity around some of them. A well publicised case study in Australia was Distribute.IT, a company that was forced to close down in 2011, in the space of two weeks after it was hacked.[9]

Distribute.IT, an Australian online services wholesaler, domain name registrar and hosting provider, was hit by a deliberate and calculated cyber attack. The company tried unsuccessfully to recover its services, until the regulators and the Federal police stepped in. The customers had left the company going to the competition after 3 days. In today's figures, this time it takes for customers to move to competitors has decreased to one day.

The media, well publicised cases and mention of cyber in almost any context at conferences and courses that deal in some form or another with computers and IT have not penetrated the Boardroom walls to the extent they should have. Companies are still insufficiently prepared to deal with cyber attacks.

8 https://www.csoonline.com/article/3267715/cyber-attacks-espionage/4-main-reasons-why-smes-and-smbs-fail-after-a-major-cyberattack.html.

9 https://www.cio.com.au/article/569410/case-study-when-hacker-destroys-your-business/.

A more significant driver for preventive measures has been triggered by the recent changes in the regulatory environment.

In Australia, the Mandatory Data Breach Notification Bill was passed in the Senate in 2017 and came into full effect on 22 February 2018. Organisations that are subject to the Privacy Act and the Mandatory Data Breach Notification Scheme must have in place systems and frameworks to comply.

The compliance test used to determine if an organisation is subject to the Privacy Act includes:

- Revenue over $3m/year
- Healthcare services organisation regardless of revenue
- Contractor to government agency
- Organisations that trade in personal information with or without consent of individuals
- Related to an organisation that is subject to the Privacy Act
- And other conditions[10]

In Europe the GDPR (General Data Protection Regulation) comes into effect on 25th of May. This affects all companies that have European clients.

In the US, there is a patchwork of laws requiring notification in particular if some sort of financial data or password information is involved. But the laws have been there for more than 10 years in some cases. Most likely this helped grow the cyber insurance industry in the US, which sees 9 out of 10 insurance policies written worldwide.

Other Organisations

What about the rest of the organisations? Our recommendation to Australian companies is to prepare and act as if THEY were subject to the Privacy Act. This does not necessarily mean that they need to report a breach, although one could find out or give useful information to authorities and OAIC (Office of the Australian Information Commissioner). But failing to report a breach to Stakeholders may have serious negative consequences.

Recent developments in the cyber security space have seen directors being sued for not discharging their duty of care and diligence and other regulatory obligations.

Associations that trade only in one state are trading under the Associations Act in the respective state where they operate. If an association is trading in more than one state, it should be registered under ASIC (The Australian Securities and Investments Commission – Australia's corporate regulator).

All entities trading under the Corporations Act are regulated by ASIC, Australia's integrated corporate, markets, financial services and consumer credit regulator.

ASIC takes a strict approach when dealing with listed entities and promotes cyber resilience.

"Cyber resilience is the ability to prepare for, respond to and recover from a cyber-attack. Resilience is more than just preventing or responding to an attack—it also takes into account the ability to adapt and recover from such an event." (source: ASIC report)

[10] https://www.oaic.gov.au/agencies-and-organisations/faqs-for-agencies-orgs/businesses/small-business.

As part of its regulator duty, ASIC may ask the following questions:

> "*Governance*:
> - Are your board and senior management aware of your cyber risks?
> - Have you assessed your organisation against the NIST cyber security framework[11]?
> - As a Director – are you meeting your legal obligations?"

Additionally, in a report released in 2016, in relation to listed entities, ASIC stipulated:

> "You may not have considered how cyber risks may affect your directors' duties and annual director report disclosure requirements.
>
> We encourage you to review your board-level oversight of cyber risks and cyber resilience as part of your systems managing your material business risks, and consider if you need to incorporate greater consideration of cyber risks into your governance and risk management practices.
>
> If you are a corporation – a cyber attack will need to be disclosed" (source: ASIC report)

Any organisation, including the Not For Profits that will raise the bar in Corporate Governance and strive to align itself to ASIC guidelines will gain a competitive advantage in the market, attract more clients and become a leader in its space.

Accountability for Cyber Risk

Where does the accountability for cyber risk sit? Risk management in general should be a component of the Board charter for the board of any organisation, large, medium or small. A typical charter should include:

11 https://www.nist.gov/cyberframework.

Note: DA and DFA are Delegated Authority and Delegated Financial Authority

We now need to answer the question of WHY the risk sits on the Board agenda.

Even if it is being recorded, reported on and mitigated as part of the overall Risk Management System, the cyber risk should be seen as a *special risk*, due to the speed with which it can hit an organisation and the huge consequences it can have.

To further back this advice to treat cyber risk as a special risk, we want to bring the view of IOSCO, the international body that sits above regulators like ASIC.

IOSCO (International organisation of securities commissions – of which ASIC is the only Australian member), in a report on cyber security released in April 2016, isolates the Cyber Risk as a special risk that needs to be elevated and treated differently:

> 'In many respects, cyber risk is not "just another risk." Cyber risk is a highly complex and rapidly evolving phenomenon. And the human element of cyber risk, combined with rapidly evolving technologies, gives it some unique characteristics: as organizations upgrade their defences, criminals continuously develop new and more complex approaches.
>
> Ultimately, in a highly interconnected and interdependent financial ecosystem, cyber-attacks may have systemic implications for the entire financial system, and also affect over time the trust on which financial markets are built.
> For these and other reasons, regulators, market participants, and other stakeholders must work together to enhance cyber security in securities markets.'

How to Mitigate Cyber Risk at Board Level

If we take the top down approach, the Board is responsible for the Extreme and Very High risks. The Cyber risk is one such example. The Board is also responsible for the Risk Strategy, and in this case the Cyber Risk Strategy.

The Board should:

- Become knowledgeable in the governance of cyber risk by undertaking a "Directors and Officers Cyber Security Course"[12]
- Start by asking the right questions
- Undertake a Cyber Healthcheck/Assessment and include the recommendations into a future Cyber Strategy
- Create the Cyber Strategy with management involvement, allocate resources to back up the initiatives needed to meet the Cyber goals from this strategy
- Oversee the implementation of this Cyber Strategy
- Oversee the reporting and management of Cyber risks

The first step is to add Cyber risk to the Board agenda.

Any board should have a Finance, Audit and Risk Management Committee, that could also incorporate in its Terms of Reference the Security aspect. We talk about Security in general of which Cyber security is a component. The work and recommendations of the Committee, which we like to call FARMS, is brought to the board through the report of its Chair. In some

[12] Advisory Boards Group offers such a course http://advisoryboardsgroup.com/services.html.

organisations the Risk Management is dealt with in a separate Committee than the Audit Committee.

The Board can then oversee the implementation of the Cyber Risk Strategy, the Cyber risks that are Extreme and Very High and take the company to a state of cyber resilience.

In managing the Cyber risks in the bottom up approach, going through the different layers of the organisation, many departments or functions of the organisation will be included:

- Finance – asset management
- Procurement – contracts with third parties which should include clauses about how the organisation will be supported by these third parties in a breach scenario
- Facilities – security of doors, locks, magnetic passes, surveillance, etc.
- HR – hiring and employment termination policies, security checks of personnel, etc.
- ALL employees will need training in cyber awareness
- IT – measures to create a cyber resilient environment whereby the network is being monitored and suitable intrusion detection and protection systems are implemented.
- Transfer of risk to third parties: Cyber and business/management liability insurance, D&O insurance, Product insurance, etc.

For Boards that do not have a Director with Cyber Governance knowledge, the questions and steps may be daunting.

How does the Board know what is needed in terms of measures? How does the Board know how to articulate the right questions?

It all starts with the Education of the Board – in the Governance of Cyber Security.

It is also important to have an independent Cyber Security Governance review, which is impartial and can give the Board an objective view of the gap and what is needed. When management talks to vendors in the Cyber security space, most of the time the answer is a sales pitch, and it does not take into consideration all the aspects of creating a Cyber resilient organisation.

Compliance to Standards and Regulatory Environment

Risk management standards and practices are well documented in a number of publications:

- ISO 4360 – previous ISO Risk management standard
- ISO 31000 – current ISO standard – will be overhauled and a new standard should be released in 2018 – 2019
- ASX Corporate Governance Principles and Recommendations (2010)[13] – Principle 7
- Risk management as one of the Knowledge areas in PMBOK (Project Management Body of Knowledge).

Cyber security is dealt with at an IT Governance level (*NOTE*: the difference between Corporate Governance and IT Governance) in a number of publications:

- COBIT version 5 - Control Objectives for Information and Related Technologies) is a good-practice framework created by international professional association ISACA for information technology (IT) management and IT governance and it covers:

[13] https://www.asx.com.au/documents/asx-compliance/cgc-principles-and-recommendations-3rd-edn.pdf.

  - ISO 38500 principles
  - ISO 20000
  - ISO 27000 series
  - ISO 31000 series
  - TOGAF 9
  - CMMI
  - Prince II
- NIST framework
- CIS controls, etc.

There is no one-size-fits-all approach to implementing Governance of Cyber security and most of these standards and methodologies do not embed the Cyber governance into the overall enterprise/organization Governance model, despite claiming to do so.

In conclusion, what is important to understand is that:

- Cyber security is NOT only an IT risk and is NOT something that should be dealt solely by the IT managers
- Organisations will get be affected at one point in time or another by a cyber attack and staying in business will be dependent on the level of preparedness (Cyber Resilience)
- The regulatory environment is getting stricter and bodies like OAIC may exercise the options to apply fines
- The customers will leave organisations that are breached and cannot demonstrate their level of preparedness

Risk Transfer Through Cyber Insurance Policies

The Cyber insurance industry is still new (despite having been around for quite some time). Its roots go back to the '90s in connection with digital cash and distributed systems. The waves created by Y2K and the 9/11 attacks have not managed to motivate organisations and people into action and the Cyber insurance remained a niche market.

Insurance companies have devised coverage for a number of events like cyber attacks, theft and fraud, forensic investigations, business interruption, extortion, data loss and restoration, handling the lost or stolen customer data and customer credit rating, PR, regulatory fines and so on.

Around 90% of all the cyber security policies are written in the US, where the market is more mature. This was partly a consequence of constant attacks, higher levels of litigation and regulatory environment.

The coverage is for first party and third party. First party claims cover on malicious destruction of data, denial of service attacks, viruses, human error, power surges and natural disasters, IT systems failures and extortion threats. Third party refers to breaches of privacy, misuse of personal data, defamation and transmission of malicious content.[14]

In comparison to other types of insurance for assets or events that have been around for 50 years and for which there is sufficient data to calculate the premiums that will ensure everything balances and the business cases make sense for the brokers and underwriters.

But the main question is how much of the risk should be transferred and how much should be managed in-house?

[14] http://locktonprofessionalinsurance.com/difference-first-party-third-party-cyber-liability-insurance/.

In order to qualify the risk profile of the client, many insurance brokers ask a set of questions that include:

- What is your data protection policy and procedures?
- Do all employees have to comply with these policies
- Do you have a Business continuity plan?
- Does your company collect, store and maintain or distribute credit card or other personally identifiable information?
- Do you have antivirus systems in place? Intrusion detection and intrusion protection?
- Does your company perform backups (offsite storage)
- And other questions

Practice and our experience has shown that whether the client responds yes or no to any of the questions, they will get the policy. The question is will the insurance pay if the information given was correct but perhaps insufficient to protect a network of the complexity the client required?

The analogy that comes to mind is to the content insurance for a house with no locks – will the policy pay for the damage or theft if it gets broken into?

Often the brokers or larger underwriters associate themselves with law firms who "manage the risk" after the event – ie after the data breach.

Even larger law firms are now offering "risk management" consulting over the phone in case of a breach. Is this enough? Is this the right, informed and educated approach to risk? Perhaps not.

An Enterprise Risk Management System needs to be implemented throughout the entire organisation, risk needs to be managed at all levels regularly and a culture of resilience needs to be embedded in all departments, management and board.

The Cyber risk is not an entirely transferable risk. The history of cyber shows that organisations can go out of business in a very short space of time – no policy will pay for losing all your clients.

The approach should be seen as a partnership between the Client, the Insurance Broker, the Auditor (who comes to audit the company's compliance to a satisfactory level of cyber governance), Risk consultant/manager (who helps implement and maintain the framework for managing risk). And not last, nor least, the Board.

Cyber risk management should be done continuously and be part of day to day operations and strategic thinking. Not after the cyber or data breach event only.

Best Practice in the Insurance Space

In a best practice approach, the NAIC (National Association of Insurance Commissioners) in the US has adopted the Insurance Data Security Model Law (October 2017).[15]

This is a framework for the insurance organisations themselves to operate complete cyber security programs. NAIC also adopted and prescribes its 12 Principles, of which we quote Principle 10:

> "*Principle 10*: Information technology internal audit findings that present a material risk to an insurer *should be reviewed with the insurer's board of directors* or appropriate committee thereof."[16]

[15] https://rsmus.com/what-we-do/services/risk-advisory/understanding-the-naic-insurance-data-security-model-law.html.

To extrapolate, Advisory Boards Group recommends that the Policy review and coverage needs to undertaken by a Committee of the Board, such as a Finance/Audit, Risk management/Security committee, which reports its findings and recommendations to the board of directors.

Case Studies From Australia

The case studies were provided by Mr Blake Deakin, principal at Cyber Insurance Australia, an insurance broker specialized in Cyber insurance, Management liability and D&O insurance. He can be contacted at blake@cyberinsuranceaustralia.com.au.

We have chosen small to medium business case studies, as the breaches suffered by larger organisations are well publicised; but the smaller end of town is slow to implement adequate protection measures. And the myth of "we are too small to be attacked" is still present in the Australian SME/SMB space.

Case Study 1: Eye Surgery Clinic

Organisation:
Two locations;15 employees; $8 million turnover.

Incident:
An employee opened an email attachment which contained ransomware, causing the Insured to lose access to their network of digital patient records. The cyber criminals demanded ransom payment in Bitcoin of approximately $6,000 at the time of writing.

Outcome: $126,000 in forensic IT expenses, First Party damage and lost work hours.

Case Study 2: Law firm

Organisation:
One location; 55 employees; $20 million turnover.

Incident:
An unknown organisation gained access to the law firm's network including a public company's acquisition target, another public company's prospective patent technology, the draft prospectus of a venture capital client, and a significant number of class-action lists containing plaintiff's personally identifiable information (PII). Soon after, the firm received a call from the intruder seeking $10 million to not place the stolen information online.

Outcome:
The law firm incurred $2 million in expenses associated with a forensic investigation, extortion-related negotiations, a ransom payment, notification, credit and identity monitoring, restoration services and independent counsel fees. It also sustained more than $600,000 in lost business income and extra expenses associated with the system shutdown. $2.6 million total costs.

Case Study 3: Raw Materials Manufacturer

Organisation:
One location*;* 28 employees*;* $7.5 million turnover.

Incident:
The Insured's system was hacked via an email they received carrying a Ransomware virus. The criminals held the clients system to ransom and would only release files if the client paid $12,500.

---

[16] http://www.naic.org. *Cybersecurity Principles for Cybersecurity Guidance*.

Outcome:
$12,500 in ransom costs plus an additional $25,000 in IT expenses related to diagnosing the problem, decommissioning the old servers and installing a new network.

Case Study 4: Hardware Store

Organisation:
One location; 20 employees; $5 million turnover.

Incident:
An employee at a hardware store ignored internal policies and procedures and opened a seemingly innocuous file attached to an email. The next day the hardware store's stock order and cash registers started to malfunction and business trade was impaired as a result of the network failing.

Outcome:
The hardware store incurred over $100,000 in forensic investigation and restoration services. They also had additional increased working costs of $20,000 and business income loss estimated at $50,000 from the impaired operations. $170,000 total costs.

Case Study 5 - Malware Theft – Accounting Firm

Incident:
Hackers sent a phishing e-mail with a bogus word document attachment to a member of the accounts team within a small firm of accountants. Upon opening the attachment, a piece of key logging software was automatically installed which allowed the hackers to gather crucial access data and then log into the firm's bank portal with the credentials of one of their users.

The insured was contacted by the bank after the hackers had initiated several wire transfers and ACH batches from the insured's account to accounts located in Nigeria. After checking with the user whose credentials had been used to instruct the transactions, the firm instructed an IT forensics company to establish what had happened and to remove the malware from the system. After managing to recall some of the wire transfers, the firm were left with $164,000 lost in theft of electronic funds
and costs of $15,000 for IT forensics work

Cause of action:
Negligence, stolen laptop leading to an Invasion of Privacy

Coverage triggers:
Incident Response Expenses, Data Asset Loss, Privacy Liability, Business Interruption, Recovery Costs, Regulatory Fines, Potential Payment Card Loss

Case Study 6 – Energy firm

Organisation:
One hundred employees; $20 million Annual revenue

Incident:
An energy company executive's laptop was stolen from a corporate vehicle. The laptop contained significant private customer and employee information. Although the fi le was encrypted, the overall password protection on the laptop was weak and the PIN for accessing the encrypted information was compromised.

Resolution:
After assessing the nature of the information on the laptop with a forensic expert and outside compliance counsel at a cost of $50,000, the energy company voluntarily notified relevant

customers and employees and afforded call centre, monitoring, and restoration services, as appropriate. While the additional first-party cost was $100,000, the energy company also incurred $75,000 in expenses responding to a multi-state regulatory investigation. Ultimately, the company was fined $100,000 for deviating from its publicly stated privacy policy. Total costs associated with the event: $325,000

Case Study 7: Healthcare Firm

Organisation:
One location; unknown employee numbers.

Incident & Outcome:
A director of a medium-sized healthcare firm in Brisbane received an email from an unknown individual who claimed that he had breached the company's systems and was holding confidential patient data which he would release to the public unless the company paid 25 bitcoin (approximately $7,500 at the time of attack). The insurer's claims team first helped identify that this was a credible threat and then work closely with the company to determine if paying the ransom would be the best course - which was the ultimate outcome.

Case Study 8: Manufacturer Pays For Invasion of Privacy By Intermediary Firm

Cause of action:
Intermediary stealing personal information leading to Negligence and Invasion of Privacy.

Coverage triggers:
Incident Response Expenses, Data Asset Loss, Privacy Liability

Organisation:
Industry Manufacturer; number of employees*:* 50; annual revenue: $10 million.

Description of event:
A manufacturer leased a copy machine over a two-year period. During that period, the company made copies of proprietary client information and its employees' personally identifiable information, including pension account numbers, driver's license numbers and other personal identifiers.

After the lease expired, the manufacturer returned the machine to the leasing company through an intermediary company. Prior to making its way back to the leasing company, a rogue employee at the intermediary firm accessed the machine's data for nefarious purposes.

Resolution:
The manufacturer incurred $75,000 in expenses in connection with a forensic investigation, notification, identity monitoring, restoration services and independent counsel fees. It also incurred approximately $100,000 in legal defense. Total costs associated with the event: $175,000.

Case Study 9: IT Managed Services Provider

A leading provider of managed services including IT platform hosting and infrastructure and support services suffered a sophisticated electronic security breach. The company had an extensive mainframe platform with partitions configured to customer requirements. A hacker employed malicious software tools and used masking techniques on the company's mainframe, concealing their IP address to gain unauthorized access to the network. The security breach cost over $1m to resolve including $600,000 data restoration expenses and Business Income Loss.

Case Study 10: Australian Healthcare Provider

Organisation:
100 Employees.

Event:
A healthcare provider misplaced multiple storage devices which contained sensitive information for over 1 million patients. The provider was unable to determine if the devices were lost, stolen or destroyed. Their lawyers advised the company to notify the affected individuals and assisted the company to address a regulatory investigation into the incident. This investigation saw the company fined for failing to adequately protect the information.

Outcome:
The company was fined $75,000 which was covered. Legal costs were covered and totalled just over $1 million including costs in defending claims brought by affected individuals, costs associated with regulator enquiries, and for miscellaneous notification related work. Total cost to the business was around $5,000,000.

Excerpts From The AON Reports

Sadly, and as shown in the Case studies above, small and medium size organisations are unprepared and do not give the cyber and data breach risks the right attention.

AON, notes in their 2016 Cyber Insurance Benchmark report[17]:

> "Smaller companies with less than USD 5 billion in revenue, put post breach extended business interruption as a close second. This is typically because large companies have the prowess and financial wherewithal to recover from reputational losses caused by a cyber related business interruption, whereas smaller companies are more vulnerable, especially when cyber attacks cause lengthy disruptions."

This is very true with respect to smaller companies (definitions may differ from country to country and industry to industry), but recent examples of breaches have shown that no one is immune (Facebook alone has suffered $50 billion market losses since the Cambridge Analytica scandal[18]).

Partnerships With The Clients

Organisations need to insure their data, networks and computers against cyber attacks. To do so, it is important they undertake reviews and implement suitable solutions that mitigate the residual risk (the risk that remains unmitigated after internal measures were already taken to decrease the probability, the impact or the exposure).

Advisory Boards Group partnered with Cyber Insurance Australia and a Host and IT services provider, OzHosting, to create a model whereby the approach to helping SMEs/SMBs follows a number of steps designed to de-risk the client before it qualifies for Cyber insurance.

The first step is the undertake a Cyber governance assessment, which will highlight which areas are deficient, what the gap between the current status and the desired best practice status of the organisation is and recommend the best course of action. Following this assessment, the clients are offered the implementation of CRIS™.

CRIS

17 http://www.aon.com.au/australia/risk-solutions/cyber-risk/cyber-insights-report-2016-australia.jsp.

18 https://www.recode.net/2018/3/20/17144130/facebook-stock-wall-street-billion-market-cap.

CRIS™ (Cyber Risk management & Insurance Solutions) has three components:

Governance components:
- RMS (Risk Management System) – review or implementation
- Business Continuity Plan – review or create
- Data Breach Notification Plan – good practice would require to have such a plan even if it is not required by law (to be able to inform stakeholders, clients of breaches)
- Education for the staff and management/board of Directors

IT components (offered by OzHosting):
- Antivirus, Firewall, Patches, Intrusion Detection & Protection Systems

Cyber insurance (offered by Cyber Insurance Australia):
- Review of existing policies to ensure there is no gap in case of breaches
- Implement tailored cyber insurance policy

Implementing a comprehensive solution means that the claims have a much higher chance to be paid and the organisation is more resilient to attacks and data breaches.

Conclusion

Cyber resilience is a status that should be attained and maintained by applying tailored controls that mitigate the specific risks of an organisation. Cyber insurance alone is not the answer to achieve and maintain cyber resilience. The approach must strengthen:

- Governance aspects: through annual cyber governance assessments, education of the board and creation of a company wide cyber strategy
- Risk management: embedding cyber risks in the overall risk management system yet giving it a higher status due to how swiftly it can affect the organisation, implementation of risk management frameworks and correlation of cyber risks with the cyber insurance
- Tactical plans: implement and execute tactical plans (or review existing plans) across all departments (IT, HR, Procurement, Operations, Logistics, etc)
- Awareness: maintain awareness and introduce a cyber safe culture

Organisations must take steps to prepare for the increasing cyber attacks, which are both more frequent and more sophisticated. No company should be complacent and think they won't be attacked. By achieving cyber resilience, this risk can be transformed into an opportunity which gives an organisation an advantage over the competition. Any client will prefer to choose a cyber resilient organisation.

Monica Schlesinger
FAICD, PMP, BEng, MEng
AdvisoryBoardsGroup.com

10 Things to Think About When Considering Insurance for Data Breaches and Privacy Losses

Ken Goldstein

With the advent of the GDPR, companies are surely focused upon the impact to turnover and reputation stemming from data breaches and privacy losses. At the same time, however, policyholders need to give careful consideration to the nature of network security and privacy ("cyber") insurance coverages available to adequately protect them. Along these lines, below are 10 key areas to consider as a part of the cyber coverage evaluation process. The list (which could easily be longer) is not meant to be exclusive or replace a broader dialog with your company's insurance agent or broker.

1. What type of private and proprietary information is your company responsible for? This not only includes information that you collect, store or transmit but also data that you outsource to third-party service providers for safe keeping. Once you have catalogued that information, consider whether it would "fit" within the context of the definition of "private and proprietary information" (or Record) under your cyber policy.

2. How broad are the policy triggers for third-party liability coverage (e.g., lawsuits)? Does it respond to "potential or actual" unauthorized access to private information? Negligent disclosure? Does the same coverage apply to the extent that information is outsourced to others? Be sure to have comprehensive coverage triggers along with a comparable limit of liability for third-party service provider breaches or privacy losses.

3. Is there expansive enforcement proceeding (regulatory) coverage? Is there an adequate response for fines, penalties, and consumer redress funds (to make victims whole)? Make sure the relevant regulatory landscape is properly evaluated and addressed in advance with your producer partner.

4. To the extent your company has responsibility for the collection, storage, or transmission of debit or credit card information, is PCI coverage being offered, including for notification expenses, card replacement costs, fraudulent transactions, and penalties? Payment card industry security standards have the potential to lack objectivity (e.g., contracts favor the card brands, etc.) and often result in significant financial exposure to companies.

5. Do you have flexibility to partner and select forensic and legal experts? These first-party expenses often drive significant dollars at the point of a data breach or privacy loss and managing your approach (including hourly rates) with the correct business partners is critical.

6. Do you have discretion to provide notification on both a "number of records" or "limit of liability" basis? The broader insurance responses in the industry provide options for both.

7. Relatedly, do notification costs include an expansive definition for "monitoring and restoration services?" Flexible policy responses include credit, identity, and healthcare records monitoring and restoration.

8. Is ransom-related coverage contemplated by the policy being proposed? This might include coverage for a "negotiator" along with your company's ability to pay a "ransom-related demand."

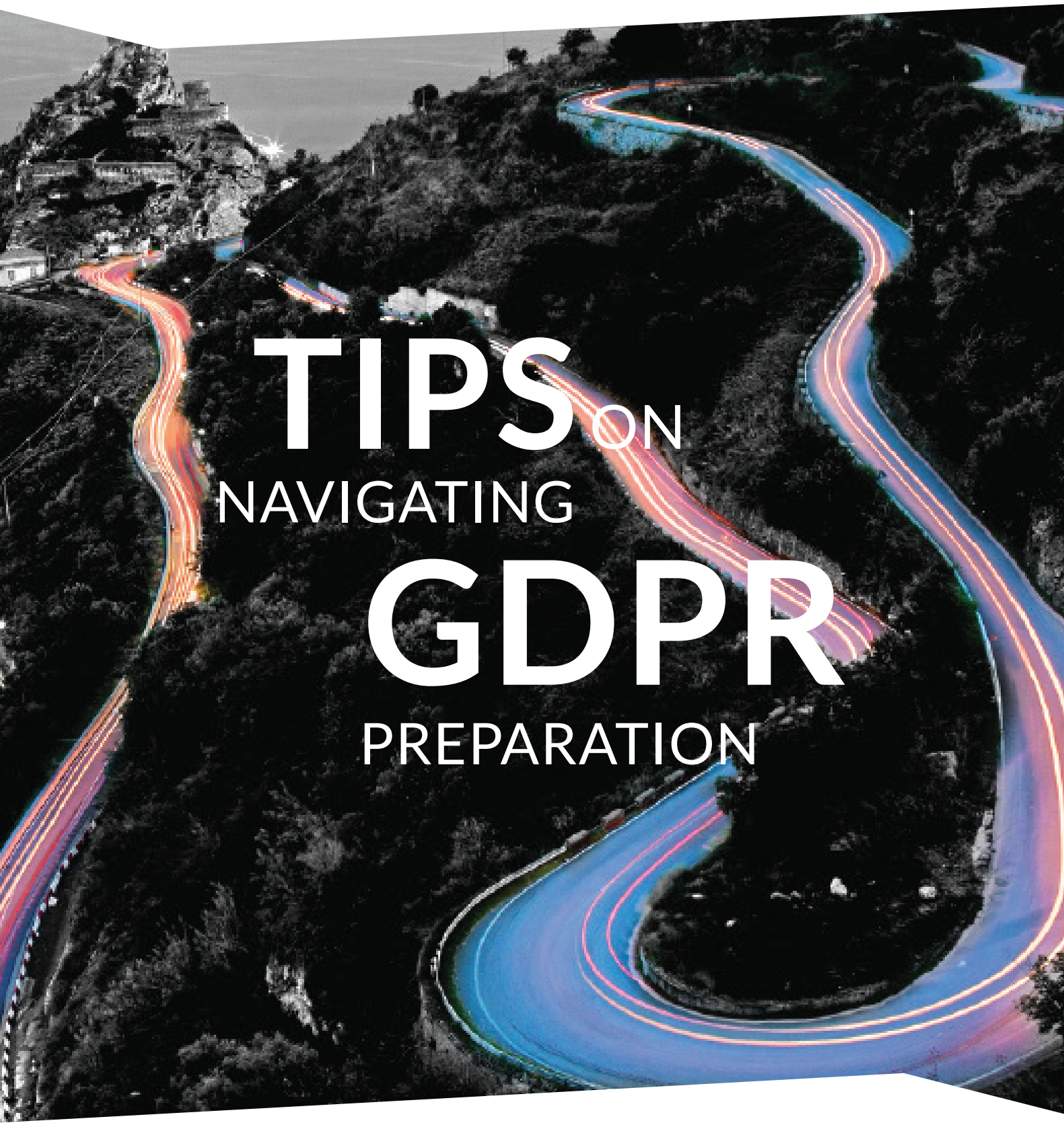
9. Is business interruption coverage afforded, including a competitive “waiting period” without a monetary deductible? The broader insurance policy responses will provide an alternative for both as opposed to requiring a waiting period “plus” a financial deductible.

10. While the market has an extensive amount of cyber capacity, ask your producer partner about whether the carrier provides comprehensive loss prevention and risk management services. The better (forward-thinking) ones do.

Ken Goldstein
Visiting Instructor of Business Law and Insurance, University of Hartford, Barney School of Business

Ken Goldstein is a former global Cyber Security Product Manager at legacy Chubb and current Visiting Instructor of Business Law and Insurance at the University of Hartford, Barney School of Business. He is actively co-developing InsurTech curriculum in partnership with the University of Connecticut (School of Business) as a part of a recent grant received through the Spencer Educational Foundation. Professor Goldstein may be reached at kgoldstei@hartford.edu.

RSA BUSINESS-DRIVEN SECURITY™



TIPS ON NAVIGATING GDPR PREPARATION

The General Data Protection Regulation (GDPR),the European Union's new data protection law, represents a major evolution in global data security and privacy practices.

Visit **rsa.com/gpdr** for information to help you navigate GDPR preparation.

International journal for the Data Protection Officer Privacy Officer Privacy Counsel

Contact
Subscriptions and submissions should contact the
International Journal for the Data Protection Officer, Privacy Officer and Privacy Counsel at:

lex@mydistillex.com.