Cyber Risk
and Insurance

Collection
KEEP IT
SIMPLE
MDS

Geoff Kinsella

MDS
Publications

Cyber Risk
and Insurance

Collection
KEEP IT
SIMPLE
MDS

Geoff Kinsella

MDS
Publications

Book Title: Cyber Risk and Insurance

Author: Geoff Kinsella

Collection: Keep It Simple

Publisher: MDS Group

Print Run: 300 copies

Date: July 2022

Legal Deposit: 503261/22

ISBN: 978-989-54810-4-0

Printed by: Lidergraf, Sustainable Printing

Contents

II. What does a cyber insurance policy cover?

With the increasing digital threat landscape in which businesses operate, it is paramount to assess, mitigate and protect against cyber risk. Cyber insurance should form an integral part of any cyber security risk management approach. The additional support received both pre and post loss from many cyber insurers will be of great benefit to any organisation.

Geoff Kinsella FCII MBA, an insurance consultant who has worked in the cyber insurance arena for more than 10 years, believes that the main reason that cyber insurance is still not widely purchased is due to the lack of knowledge and appreciation of the coverage and benefits associated with this nascent class.

In this book, we explore the evolution of cyber insurance, explain the coverage and its advantages, and offer some insight into the risk management considerations for businesses around cyber risk. We will also endeavour to highlight some of the leading markets in this space and how the market may evolve in the future.

“You often hear it said by cyber security experts that ‘it is not just a matter of time before you are hacked, you probably have been already!’

So when things do go wrong, it is important to have a risk management programme in place to help your business mitigate the impact of a cyber event. Cyber insurance should form part of your risk management response.”

I. Cyber risk – a growing threat

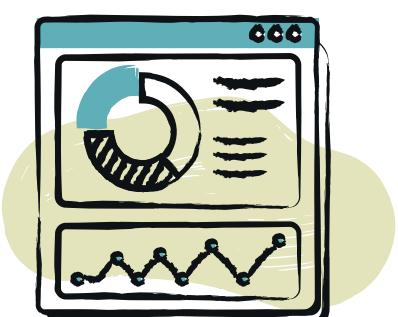
Do you think the advancement in technology is driving a need for cyber protection?

Yes indeed. Although it does sound like a cliché now, we are without question living in an interconnected, digital world. When the internet first raised its head in the public domain back in the mid-1990s, most people, me included, did not see the remarkable impact it would have. From the way we buy goods and services to the way we communicate, technology in one shape or another has infiltrated every aspect of our lives. The speed of change is startling.

The speed of change is startling

The 'Internet of Things' has also added another layer of interconnectivity that pervades many of the products that we own. Whether it is the car on your drive, the smart meter in your home or appliances in your kitchen, technology now allows you and third parties to remotely monitor and streamline your daily routine.

We have all become accustomed to those we interact with online gathering our personal data. In the recent past, would you have ever imagined giving personal details so readily to complete strangers? From your date of birth, to driving licence details; from your mother's maiden name, to your bank account details; we all merrily fill in online forms that give the recipient the keys to unlock your life. Data is now the new currency and the amount of data that is collected is unprecedented. I saw a statistic recently that said that 'more data was generated in the last two years than in the entire human history before that'!



And this hunger for data is not going to slow down. You cannot even go for a walk these days without wanting to record the number of steps that you take! On Google we submit about 95,000 search queries per second. 500 Hours of new video show up on YouTube every minute and in the same minute, users send 8 billion messages on Facebook! Remarkable.

The more that we rely on technology to shape our lives, the more demand for cyber protection will grow.

On Google we submit about 95,000 search queries per second

Is the use of technology also impacting the business world?

Technology is clearly also driving the way that we do business. We use technology to buy, sell, design, transport, meet, share, monitor, assess and so on. We depend more and more on our systems, whether they are informational or operational technologies. As with our personal lives, businesses now also interact digitally with their vendors, sharing secure information and often allowing them access to their systems. Businesses keep vast amount of Personal Identifiable Information (PII) about their customers that helps them to shape the customer experience. And just like our personal possessions, technology has also infiltrated many of the processes and equipment used in industry to allow remote monitoring and control. With this remote access comes inherent danger.

We depend more and more on our systems, whether they are informational or operational technologies

The potential for businesses to increase their net income, reduce their costs and increase their operating margins by adopting Big Data is no doubt driving the adoption of technology. In a survey by Accenture in 2014 entitled 'Big Success with Big Data', 79% of executives at the time believed that failing to embrace Big Data would lead to bankruptcy. Being digital in the past used to be an aspiration, now it is an imperative for survival. If one considers the speed in which organisations had to move the majority of their workforces to remote working due to the pandemic: it would not have been possible without the digital revolution that had already been taking place. This revolution is going to continue to shape our world.

Companies spend vast amounts of money on security and ensuring that their systems are stable. If the technology fails for whatever reason, the livelihoods of staff and the profitability/ longevity of businesses can be severely impacted.

It is becoming more important for businesses to protect themselves should they suffer a cyber event.

What happens when things go wrong?

You often hear it said by cyber security experts that ‘it is not just a matter of time before you are hacked, you probably have been already!’

We have all read the stories that make headline news about major companies severely impacted by the consequences of a system failure. Financially and reputationally the companies often struggle to recover. But for every case that makes the news, there are many companies that suffer losses due to cyber related incidents that go unreported. What is also of interest is that the vast majority of cyber insurance claims actually affect Small to Medium Sized Enterprises (SME). A recent study by NetDiligence (a provider of Cyber Risk Readiness & Response services) found that 98% of all claims that occurred between 2015-2019 were to SME companies with 77% from companies with less than $300m revenue.

So when things do go wrong, it is important to have a risk management programme in place to help your business mitigate the impact of a cyber event. Cyber insurance should form part of your risk management response.

Why then is there such a slow take-up of cyber insurance?

There are many reasons, but in my opinion one of the main ones, is the lack of knowledge about the product and what it covers. Would the number of businesses buying this coverage increase if, for example, they were more fully aware of the scope of coverage afforded by a cyber insurance policy?

Equally, many buyers still believe that cyber insurance is a very new and untested class of insurance. Perhaps they are waiting to see if the market develops. Although by insurance industry standards, cyber insurance is a nascent class, most people are not aware that cyber insurance in various forms has been underwritten since the 1990s. However, it is only in the past 10 years or so that the market has grown exponentially with a plethora of insurers and products now available for the corporate buyer. Increased pervasiveness of cyber-attacks, the mounting legislation which promotes data security, and the high number of losses incurred are the key factors driving the growth of the

global cyber insurance market. Add to these factors the focus at Board level on cyber risk and the increasing contractual requirements to purchase the coverage, one can expect the demand for cyber insurance to keep rising.

Munich Re estimates that the global cyber insurance market is currently worth over USD 7bn. North America remains the strongest market with a value of USD 5.3bn. The value of the European cyber market in 2020 is estimated at more than USD 1bn. Many commentators expect the total market value to reach $39.5bn by the year 2028. If you compare, for example, the current total global premium volume for D&O insurance of circa $20bn against the above numbers, you can see that there is great growth potential.

I am hoping to provide the reader with a simple but informative overview of the coverage available and the protection it affords. With this knowledge, I hope that you will be able to make an informed decision about the value of the product and its place in your cyber risk management programme.

II. What does a cyber insurance policy cover?

How has the coverage evolved over time?

Like many other classes, cyber insurance policies have changed over time and the coverage offered has evolved to meet market dynamics, legislative changes and buyer needs. For example, in the mid-1990s, much of the focus at that time was on protecting the ISP providers in the new internet age and responding to the risks associated with the Y2K bug. This era spawned the original technology insurance policies that ultimately 'morphed' into the cyber policies that we know today.

In 2003, the focus of the coverage shifted to Data Breach and Privacy liability. A driver at the time was the Californian State enacting privacy laws, making notification to affected data subjects mandatory. Specific industry regulations also appeared at this time, for example in relation to the Payment Card Industry (PCI) and also Healthcare. (It is interesting that GDPR in Europe similarly had an impact on the cyber take up rate from 2018 onwards.)

As the decades unfolded, the focus changed again as buyers became more concerned with first party coverages such as data recovery, recovery of data assets and business interruption. Cybercrime such as wire fraud, social engineering and extortion became more prevalent in the mid-2010s and insurers responded to this need. As we moved into the late 2010s and early 20s, in addition to cybercrime, system failure, outsourced services, and contingent business interruption became the key coverage components for many buyers. Again, the market responded extending coverage accordingly.

As is the case with every class of insurance, the "devil is in the detail!"

Are all cyber policies the same?

As is the case with every class of insurance, the ‘devil is in the detail!’ It must be understood that every policy ‘is not created equal’. It might be an oversimplification to say it, but insurers will only cover what they want to cover! So, it is important to read the wordings to compare and contrast different insurers’ forms.

In general, your cyber policy should offer you protection around three main areas namely: data security; data integrity and data availability. These are the key coverage components that you should be looking for when buying a cyber policy. So as an example, if the integrity of your data (confidentiality) is compromised due to tampering, or your business systems are not available to allow the business to effectively operate (availability), the policy should respond.

Do cyber insurance policies offer ancillary services?

Yes, one of the unique features of cyber insurance is the access that the policyholder has to a panel of experts pre and post-loss. Cyber incidents are incredibly time sensitive, so knowing you have a highly specialised team on your side is an invaluable asset. These teams, comprising IT forensics/security, legal and PR expertise, will ensure that the loss is mitigated effectively and efficiently. This type of resource is of particular value to SMEs who would not normally have access to in-house resources of this nature. To be honest, I have known of SME companies that use these resources almost like their outsourced IT providers. After all, if your systems go down, who better to call than a team of IT experts!?

Examples of breach response companies utilised by insurers include: Cyberscout, ReSecure and KROLL.

Many insurers will also offer their insureds access to online portals where they can find invaluable information to help them to manage their cyber risk. These often comprise whitepapers on security protocols and policies, incident response plans, regulation summaries, risk management advice, staff training videos and the like. Many also offer a 24/7 helpline that you can call pre or post breach. Considering that these services are included within the premium, it does highlight the advantage of buying cyber insurance.

Many also offer a 24/7 helpline that you can call pre or post breach

More recently, insurers have also started to provide more sophisticated risk management tools to their customers to help them, for example, monitor their systems for vulnerabilities. As the 'bad actors' get more sophisticated, the insurance industry has had to respond more innovatively to the increasing threats.

So what are the main coverages provided?

As mentioned previously, different insurers offer different levels of coverage. But we can give an overview of the principal covers offered in the market today.

At this stage I would like to dispel one of the misconceptions concerning the coverage offered by a cyber policy. It does not only cover data breach liability or offer protection for businesses that hold Personal Identifiable Information (PII). The coverage also protects the insured for their loss due to system failure, system damage, business interruption and cybercrime. And to dispel another myth, the policy also covers physical files and data. So if you leave confidential paperwork on a train or it is stolen from your car, the policy will respond.

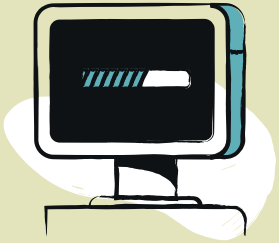
One word of warning. As with any insurance with an aggregate indemnity limit, it is important to look closely at the way this policy limit is eroded, and how the policy deductible is applied, across the different coverage sections. Here are some examples of things to look out for:

- To ensure early engagement of the insured with their panel of experts, some insurers will not apply a deductible to the costs associated with the initial response services;
- Others will provide for notification costs to affected third party subjects outside of the policy limit;
- Most insurers will apply the indemnity limit only once across the various sections of the policy. But some offer standalone limits per section. A major enhancement;
- Watch out for sub-limits within the policy for certain covers e.g. cybercrime;
- Limited reinstatements in the policy period.

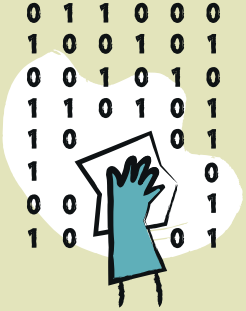
Most cyber insurers have taken a modular approach to the cover offered, dividing their policies into first-party and third-party risks. Let's look at the principal coverages offered:

Third Party Cover

- Security and Privacy Liability and Defence costs
  - Network security breaches;
  - Transmission of Malicious Code;
  - Damage, alteration, corruption, disposal or loss of Third Party digital assets;
  - Breach of Third Party or employee privacy rights;
  - Causing DDoS attack, phishing or pharming.



- Privacy Regulation Defence costs, Fines and Penalties[1]
  - PCI fines, assessments, chargebacks, reimbursements;
  - Regulatory agency's award of a fine or penalty to a third party.
- Multimedia Liability
  - Infringement of intellectual property, copyright, slogan or trademark;
  - Defamation, libel, slander;
  - Emotional distress, mental anguish.



The above are the general Third Party protections offered, but some insurers do extend the covers to include for example contractual liability and management liability.

1 - Where insurable by law

First Party Cover

- Cyber incident response costs including
  - Notification;
  - Credit monitoring;
  - PR / crisis communication;
  - IT Forensics;
  - Legal.
- System damage and business interruption
  - Loss of income;
  - Extra and additional expense;
  - Data re-creation/ restoration;
  - Hardware repair or replacement;
  - Consequential reputational harm;
  - Cyber Terrorism.

Note that system damage and business interruption can be triggered not only by malicious cyber events, but also by accidental system failure. This is another key component to look out for in your specific insurer's wording. Many of the events that have been covered by the cyber market have simply been the result of human error.

It is also important that the policy wording does not only specify 'your system' as being covered, but also extends to include the systems of others, for example, the insured's technology suppliers. In some instances, insurers will go beyond technology providers and offer contingent business interruption for named suppliers.

One other thing to look out for is an unencrypted device exclusion. Many policies will not respond if for instance, your laptop or mobile device is not encrypted and you lose data. But again, this is not always the case and you should look to include this coverage.

- Cybercrime
  - Loss of your or a third party's money, credit, securities, products, goods or services;
  - Theft of money from a senior executive's personal bank account;
  - Phishing attack expenses;
  - Transfer of funds in good faith to a third party as a result of fraudulent or deceptive communication;
  - Social Engineering;
  - Ransomware or targeted extortion;
  - Use of system resources through means such as cryptojacking or botnetting;
  - Identity theft expenses.

These are the principal coverages offered. However, it is important to dive into the detail of any policy wording. The definition sections of the policy need to be carefully scrutinised, as many insurers have different interpretations of insured events and policy terms.

I would also counsel looking out for Retroactive cover restrictions. As a cyber-attack is often discovered long after it first occurred, you should seek to have full retroactive cover prior to the inception date of the policy. This is more common in SME policies, but it is always worth investigation.

In the Appendix we will look at some examples of cyber claims and how the policy responded to these incidents. This hopefully will give the reader some real-world examples of how the coverages discussed previously operate following a cyber incident.

Who are the main cyber insurers?

The number of insurers writing cyber risk has grown significantly since the 1990s. However, as with other insurance classes, the market participants also change in line with market cycles. As loss ratios and pricing become out of sync, I have seen MGAs in particular struggle to survive. Increasing pressures on mainstream insurers from both their management and reinsurers, also lead to corrections in the market and in some cases, the withdrawal of insurers from this class.

Cyber insurance is still seen by many carriers as an area with significant growth potential

As mentioned previously, cyber insurance is still seen by many carriers as an area with significant growth potential, despite the inherent risks. It would be impossible to list every insurer in every territory that write cyber insurance. (By way of example, if one was to only consider the Lloyd's market, there are purportedly

77 cyber risk insurers active at this time!) Equally, the risk appetites differ greatly from insurer to insurer, with some favouring small to medium sized businesses, others writing excess layers: to those that favour more complex larger entities.

There are a number of markets that have been in this space for many years (or grew their involvement through acquisition) and continue to offer cyber capacity to clients. These include:

AIG	Hamilton
Allianz	HDI
Arch	Hiscox
AXA XL	Liberty
AXIS	Munich Re
Beazley	Markel
W. R. Berkley	Renaissance Re
BRIT	Swiss Re
Chubb	Travellers
Canopius	TMK
CFC	QBE
CNA	Zurich

*Note that a number of these entities also operate at Lloyd's.

How will the cyber market evolve in the future?

That is a very difficult question to answer with any certainty. There are a number of trends that are evident today that I believe will continue for the foreseeable future.

Market Correction - the insurance market has been hit by an unprecedented number of losses over the past year. Ransomware losses have grown exponentially fuelled in part by the Covid-19 shift in working practices and the squeeze on IT maintenance budgets. The availability of Bitcoin to pay ransoms also makes cyber extortion attractive to the miscreants due to its anonymity.

Ransomware losses have grown exponentionally fuelled in part by the Covid-19 shift in working practices

The losses have identified the mismatch between the premium being charged and the level of potential risk. Rate increases

of more than 100% have been the norm and I believe the increases will continue to be a factor for the coming years. Expect a squeeze on the availability of capacity and a focus on deployment of capital by insurers where there are better returns to be had e.g., excess layers versus primary. Higher deductibles (retention increases of 300% are not unusual at this time), exclusionary language and lower sublimits for high-risk coverages (such as ransomware) will also be factors going forward.

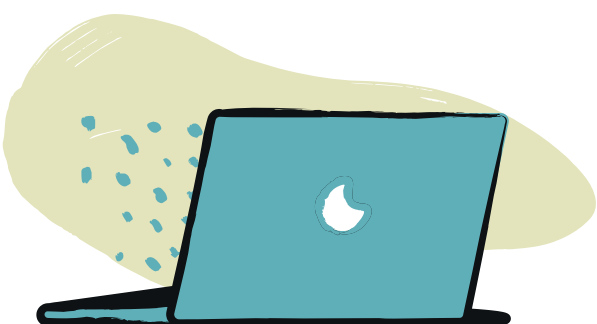
Focus on Risk Management - insurers will be scrutinising more closely the security controls and policies that the insured has in place. A cyber insurance policy cannot continue to be the main approach to cyber risk mitigation by businesses. Insurers will want to see evidence that companies have put the right risk management practices in place if they are going to continue to provide high levels of coverage. Companies that do not have the right approach or are not willing to instigate recommended solutions, will find it difficult to obtain coverage.

Growth in Cyber Security Vendors' Influence - the relationships between the insurers and those that provide cyber risk mitigation or response services will deepen. The imbedding of monitoring and prevention tools into the insurers' offerings to clients will become the norm. These services will adapt to the changing risk environment and also to the advancement in technology. These tools will also be more widely adopted by the larger cyber insurance buyers.

Distribution of Cyber Insurance - it is likely that insurers will continue to seek new or additional methods of distributing cyber insurance. Online portals, insurtechs and the imbedding of cyber policies into Affinity type programmes will also increase over the coming years. Traditional routes to market will naturally prevail, but the need to increase penetration of this product will encourage innovative routes to market.

Government intervention and collaboration - with the ever-changing geopolitical landscapes, the cyber threat from state sponsored attacks will continue to cause the market concern. The increased collaboration of government, law enforcement and national security bodies with the insurance sector will need to intensify. The intelligence about the 'bad actors' and the latest types of technological attacks needs to be more openly shared with the insurance market and also larger commercial entities.

This should be a two-way process, with the insurance market also willing to share what they are learning from each new loss variant that arises. The data will also need to be shared with data modelling providers to allow more robust models to be generated.

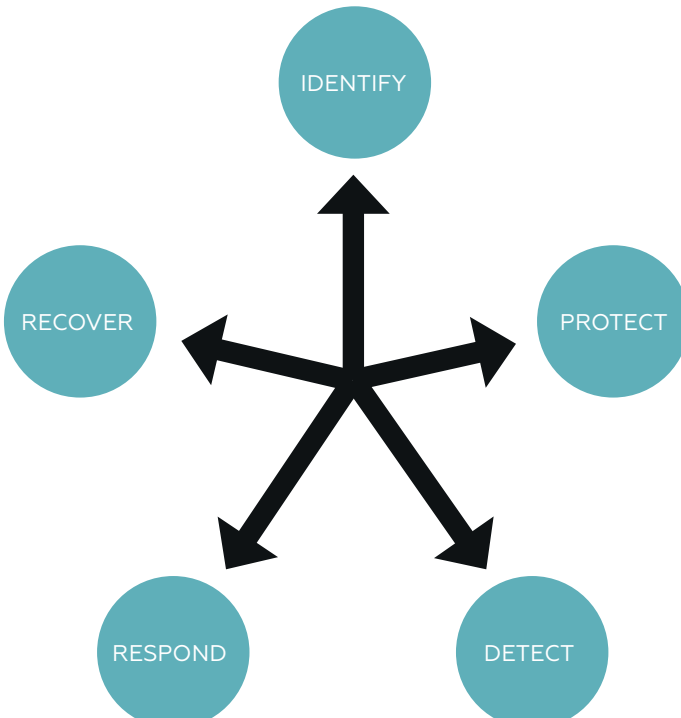


III. Risk Management Considerations

How should organisations approach cybersecurity risk management?

There are many risk management models/frameworks available that can be followed when designing your risk management programme. One such cybersecurity framework was created by the US Department of Commerce's National Institute of Standards and Technology (NIST). They have helpfully translated this framework into several languages which includes Spanish and Portuguese, to name a few.

This framework gathers standards, guidelines and practices that are working effectively in many industries today. The framework will help an organisation to understand, manage and reduce cyber risk. The framework covers topics across technology, physical, and personnel with a focus on key business outcomes. The core of the framework includes five high-level functions as follows:


IDENTIFY
PROTECT
DETECT
RESPOND
RECOVER

The Risk Managers reading this book will recognise that much of the risk management process headings described in this framework are very similar for other risk classes such as Property.

It would however be impractical in a book of this nature to go into depth regarding the many layers of detail required to develop a cybersecurity risk management programme based on NIST. But if an organisation follows a framework of this nature, they will have gone a long way to enhancing their cybersecurity. We must also be cognisant that many SMEs would not have the resources or sophistication to implement a full risk management approach of this nature. But every organisation can in some way mitigate risk by considering these headings whether they outsource IT management services or not.

But if an organisation follows a framework of this nature, they will have gone a long way to enhancing their cybersecurity

There are many quick wins that organisations can adopt to reduce cyber risks. These can include: keeping hardware and software up to date; using password manager technology; backup data securely and off the corporate network and; using two-factor authentication. In the remote working world that we now live in, it is critically important to educate your staff about cyber security.

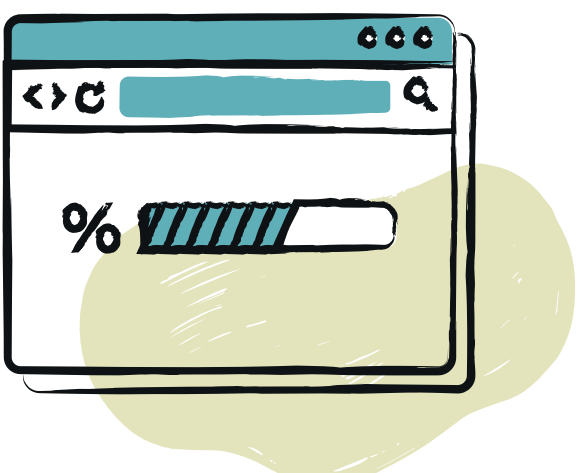
Do risk management practices influence underwriters' pricing?

When an insurer is pricing a cyber insurance risk, they consider many facets that should have been addressed by a risk managed focussed organisation. Let us work through an example by using some of the headings above that may offer some more insight into how the framework and insurance underwriting could overlap.

An underwriter considering writing a new risk would consider the following:

Culture of the organisation and awareness of cyber risk – has the organisation clearly identified, for example, the type of data the organisation processes, stores or holds? How this data flows through their business and who has access to it from within and outside the organisation? Do they know what their 'crown jewels' are and what might motivate an attack? Do they know how much of their critical processes are outsourced

to a third party? Culturally, do they educate their staff and key stakeholders on the dangers of risks such as social engineering and wire fraud? Is cyber risk taken seriously in the company and considered in a positive way?



Level of security around their data/ IT infrastructure – how does the organisation protect their data both inside the company's network and in transit outside of the network? Who is responsible for the security of data e.g. is an outside organisation used for this purpose? Do they use encryption? Do they use two-factor authentication[2]? How often do they carry out penetration testing of their systems or audit their security? Do they regularly update patches to respond to known vulnerabilities or weaknesses? Do they backup their data and where are these backups stored?

Incident readiness and response – does the organisation have a business continuity plan of how they will respond to a cyber incident? Have they allocated responsibilities within, and externally, should an incident happen? Have they tested the plan and if so, how frequently? How will they detect if an incident has actually happened? Do they regularly monitor their systems in this regard?

2 - With the recent increase in cyber losses, having two-factor authentication is becoming a prerequisite for many insurers

These questions, as can be seen, would give an underwriter a very good insight into the organisation's approach and attitude to cyber risk. If you have adopted a risk management model such as NIST's then the processes and procedures in place would lead to positive responses to the questions raised.

The cyber insurance policy can help to alleviate some of the uncertainties around cyber risk. The peace of mind of knowing for example, that you have a team of experts a phone call away to help you to respond to a cyber event, is invaluable.

If a cyber insurance policy were to form part of the risk management strategy, it would complement the high-level functions of the programme, especially if a loss occurs.

The table in the next page shows where the policy could complement your risk management programme.

Cyber Insurance can offer	Identification/ Awareness/ Detection	Protect	Respond/Recover
	Pre loss mitigation advice	Financial peace of mind	Highly skilled team of IT, Legal, PR and other experts available to identify cause and mitigate the loss
	Staff training resources	Crisis Management • PR Expenses • Notification Costs • Credit/ID monitoring • Fraud Consultation	
	Cyber response planning tools	Financial Loss • Fines & Penalties • Extra Expense • Business Interruption • Extorsion	Help the organisation to minimise Business Interruption and regulatory impact Achieve best case outcomes following cybercrime
	Penetration testing and vulnerabilities monitoring tools offered by some	Liabilities • Transmission • Security • Privacy • Intellectual Property	Offer legal advice and support

IV. Conclusion

The pace of change in the world of technology and the legislation surrounding data privacy have helped to fuel the demand for cyber insurance. The coverage and pricing afforded by cyber insurers has also changed over time to reflect buyer needs and claims activity.

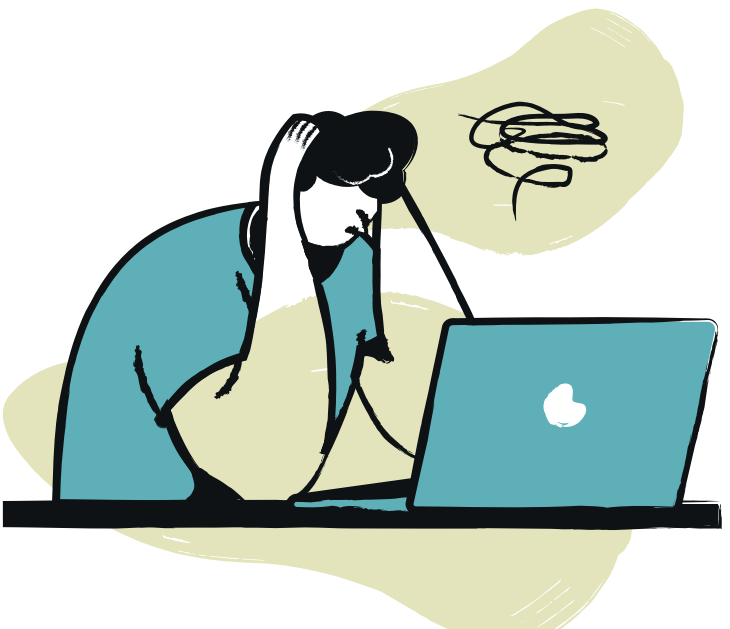
It is important for businesses to identify and mitigate the cyber threats faced daily due to the growing reliance on technology in commerce. Failing to do so can lead potentially to catastrophic financial consequences.

It is important for businesses to identify and mitigate the cyber threats

Cyber insurance can perform an important function in an overall cyber security strategy, removing some of the resulting uncertainties following a cyber incident. The pre-incident support also afforded by many cyber insurance policies can also be invaluable to businesses trying to manage their cyber exposures.

It is hoped that this book has offered a useful insight into this subject. Hopefully, it may encourage those yet to purchase this coverage to speak to their advisors for further details and/or to obtain a quotation.

As George Orwell once said, “To see what is in front of one’s nose needs a constant struggle.” And in the world of cyber risk, this struggle continues at some pace.



Appendix

Insurance Claims Examples

It is difficult sometimes to ascertain how the policy coverage I discussed earlier actually responds in the event of a cyber incident. I have therefore provided a number of case studies that hopefully demonstrate the scope of the coverage afforded by a cyber insurance policy.

Industry of Claimant: Medical Group
Nature of the Incident: Phishing Email
Total Payout: $550,000

Responding Coverage Sections: *Data Breach Response, Crisis Management, Social Engineering, Fines & Penalties*

A medical group employee inadvertently opened a phishing e-mail that infiltrated their network. Anti-virus software failed to keep out the malicious code. Personal Identifiable Information (PII), including names, addresses, medical information and diagnoses of over 1,000 patients were exposed. A computer forensics expert and a public relations firm was appointed. All the affected individuals were notified. The Office for Civil Rights launched an investigation and the medical group was fined for allowing unsecured access to their network.

Industry of Claimant: Financial services
Nature of the Incident: Misdirected Fund Transfer
Total Payout: $225,000

Responding Coverage Sections: *Data Breach Response, Crisis Management, Social Engineering and Cybercrime*

A financial services company was the victim of a social engineering event, which resulted in a fraudulent wire transfer of $200,000. The fund transfer was made following receipt of updated payment instructions that supposedly came from their vendor. The company transferred funds in connection with the closing of a property deal.

It was not discovered that the wire transfer was fraudulent until months later when the recipient notified the insured that they had not received the funds. The company retained legal privacy counsel and forensics to assist with investigating the incident.

Additionally, this incident triggered the Social Engineering coverage.

Industry of Claimant: Hospitality
Nature of the Incident: Data Breach
Total Payout: $80m

Responding Coverage Sections: *Data Breach Response, Crisis Management, Payment Card Industry (PCI) Fines and Privacy Costs*

This incident involved a credit card breach occurring at a hotel chain. The hotel was notified by Visa on two separate occasions of a potential credit card breach. The hotel engaged a law firm who retained a forensics company to carry out a forensic investigation. The investigation identified that there were two intrusions, impacting over 300,000 credit cards. Total costs included notification to affected individuals, defence costs, settlements with affected individuals and PCI fines and penalties.

Industry of Claimant: Pharmaceutical Manufacturer
Nature of the Incident: Ransomware Attack
Total Payout: $1m

Responding Coverage Sections: *Data Breach Response, Crisis Management, Cyber Extortion and Ransomware. Business Interruption and Extra Expense*

This incident involved a manufacturer specialised in equipment for pharmaceutical companies. The company experienced a ransomware attack which infected their network. Operations ceased as a result and $500,000 in bitcoin was demanded for the decryption keys. This ransom was ultimately paid. The insurers retained legal counsel, forensic vendors, and specifically, a vendor with the capability to quickly provide a large amount of bitcoin. Total costs in this matter were comprised of legal and forensic investigation costs in addition to the ransom payment.

Industry of Claimant: Municipality
Nature of the Incident: Ransomware Attack
Total Payout: $225,000

Responding Coverage Sections: *Data Breach Response and Crisis Management*

It became apparent that a significant number of the municipality's schools' servers were impacted by malware, when numerous users reported reboot issues. First party coverage under the Data Breach Response and Crisis Management Costs insuring agreement was triggered. The insured engaged legal privacy counsel and forensics to investigate and remediate. Notification, call centre services, and credit monitoring were subsequently provided to the impacted individuals.

Industry of Claimant: Retail Brand Distributor of Perfumes
Nature of the Incident: Social Engineering and Theft of Funds
Total Payout: $100,000

Responding Coverage Sections: *Social Engineering, Cybercrime and Data Breach Response*

A 'spoofed' email was sent to the insured's accounting manager requesting urgent payment to a vendor. The caller subsequently emailed the "ficticious" outstanding invoices to the manager which resulted in him authorising two fraudulent wire transfers. Following IT forensic investigations it was discovered that there had been no compromise to the insured's systems. However, payments of over $80,000 had been made before the company could stop the payments.

Industry of Claimant: Non-Profit Organisation
Nature of the Incident: Misdirected Fund Transfer
Total Payout: $800,000

Responding Coverage Sections: *Data Breach Response, Crisis Management, Social Engineering and Cybercrime*

A city food bank service experienced a breach that resulted in the disclosure of tens of thousands of donors' personal information. Due to the sophistication of the malware on their server, access to donor information happened over a three-year period. The personal information included names, addresses, credit and debit card numbers, security codes and expiration dates.

Computer forensic experts were retained to assist with the investigation. The food bank was required to notify all affected donors and provide identity protection and credit monitoring for a one-year period.

Industry of Claimant: Manufacturer
Nature of the Incident: Malware Attack at Supplier's Site
Total Payout: $5,000,000

Responding Coverage Sections: *Data Breach Response, Crisis Management, Contingent Business Interruption*

An external supplier of the insured suffered a malware attack that caused their plant to stop manufacturing for over 2 weeks. Engineers and IT experts worked feverishly to restore the affected systems and to get production back up and running. As a result of the cyber-attack at the supplier's premises, the insured could not source critical components and manufacturing operations were interrupted. Contingent Business Interruption cover had been purchased by the insured, and the insurers paid the manufacturer's loss of revenue and extra expense arising from the outage at the external suppliers' business.

Industry of Claimant: Law
Nature of the Incident: Cyber Extortion
Total Payout: $2.6m

Responding Coverage Sections: *Data Breach Response, Crisis Management, Cyber Extortion and Ransomware. Business Interruption and Extra Expense*

An unknown criminal organisation gained access to a law firm's network. It was considered that they may have gained access to sensitive client information, including the name of an acquisition target of a large public company, a client's patent information and the prospectus of a venture capital client. There were also a large number of Personal Identifiable Information (PI) from class action groups. The firm subsequently received a ransom demand of $10 million to stop them posting the stolen information online.

The insurers paid $2 million in expenses associated with the forensic investigation, extortion-related negotiations, a ransom payment, notification, credit and identity monitoring, restoration services and independent counsel fees. The firm also received a business interruption payment of more than $600,000 due to lost business income and extra expenses associated with the system intrusion.

Industry of Claimant: Accounting
Nature of the Incident: Loss of Documentation
Total Payout: $700,000

Responding Coverage Sections: *Data Breach Response and Crisis Management*

A senior employee travelling home late on a train from a business meeting left his briefcase on the train. As it was pay review season, the case contained papers that outlined employee payroll information including banking details, employee names, dates of birth, home addresses and social security numbers.

Although the case has never been found or no demand for a ransom has been made, the insured had to notify all the employees of the breach, appoint legal monitoring counsel and also offer credit monitoring services. Some compensation was also paid to affected employees. Although $700,000 has been paid to date, the file remains open in case future demands are made.

Industry of Claimant: Construction
Nature of the Incident: Email misdirection
Total Payout: Nil

Responding Coverage Sections: *Data Breach Response*

In this case, an email containing payroll details of 60 employees was inadvertently sent by the insured's HR department to all employees in another branch office. The insured notified the insurers. However, following investigation, the insured decided to take no further action. No payments were made in this regard. We have included this claim to demonstrate that sometimes breaches can occur through simple human error, but they do not always result in a claim payout.

About the author

During his career, which spans over 40 years in the insurance arena, Geoff Kinsella has lived and worked in a variety of insurance/reinsurance markets including Ireland, Middle East, Canada and the UK. Geoff has travelled extensively and has conducted insurance business on every continent (except Antarctica!).

With experience of insurance broking both as a retailer and a wholesaler, he has a firm grasp on the challenges faced by the stakeholders in the insurance market.

Proving the adage wrong, that 'you can't teach an old dog new tricks', Geoff turned his attention in 2012 to the emerging insurance market for cyber risk and ultimately joined Safeonline in London as a Partner in 2013. He has placed cyber insurance for many different entities, assisted MGAs find market capacity and has spoken on the subject at many market forums.

Geoff is currently acting as a consultant to a number of businesses.

Geoff is FCII qualified, a Chartered Insurance Practitioner, and holds an MBA.

MDS@2022

MDS GROUP

Brokerslink
Partner

With our Keep it Simple collection, the MDS Group publish short, incisive materials on topics of relevance to the insurance and risk management sectors, pursuing the Group's knowledge production and knowledge-sharing mandate.

mdsgroup.com