Optimal models for cyber insurance for the SME/SMB markets

By Monica Schlesinger FAICD

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.

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]

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.

[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

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%

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*
- *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*

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

- *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.

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

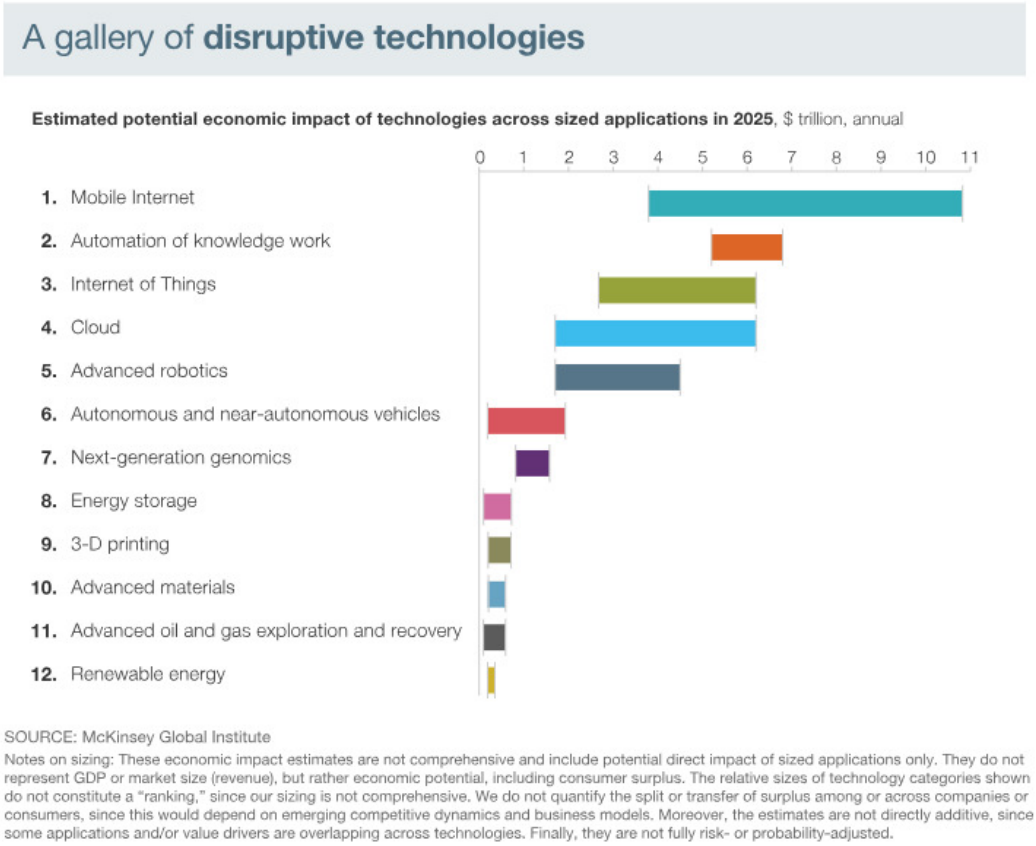
[6] http://www.aon.com/2017-global-risk-management-survey/index.html?utm_source=aoncom&utm_medium=2015-grms-redirect&utm_campaign=grms2017

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:



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.

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

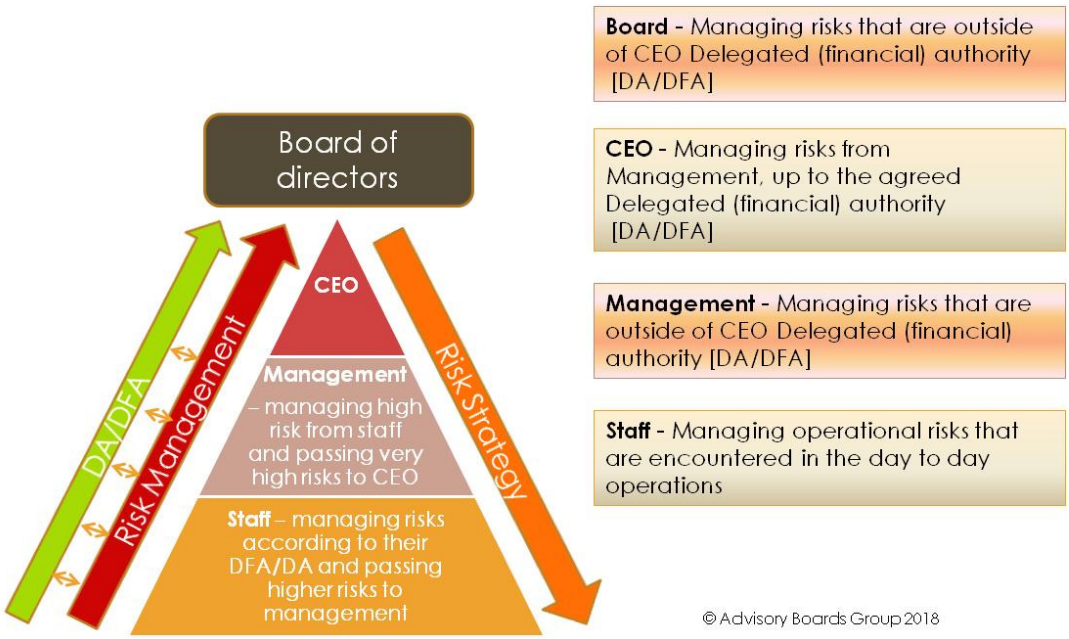
Risk management is usually documented in a Risk Management System document, Risk Policy, Risk Strategy and a **live** Risk Register.

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.



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.

[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/

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.

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.

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.

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:

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.

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

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 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

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

- 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:
    - 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

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

- 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?

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.

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

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]

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:

- 2 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.

[15] https://rsmus.com/what-we-do/services/risk-advisory/understanding-the-naic-insurance-data-security-model-law.html
[16] http://www.naic.org/documents/committees_ex_cybersecurity_tf_final_principles_for_cybersecurity_guidance.pdf

Case study 2: Law firm

Organisation:

- 1 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:

- 1 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.

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:

- 1 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:

- 100 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:

- 1 location
- Unknown employee numbers
- Unknown turnover

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
- Unknown turnover

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, notices 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™ (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)

[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

- 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.