20 October 2020

Reference: QA Report – FM Global

1. **If you only had time to focus one thing in the first instance as part of the roll out of a cyber risk response plan, what would that be? Employee risk awareness and training?**
   If you had time to focus on one thing, focus on documenting an actionable incident response plan protecting the integrity of your business and ensuring recovery in the event of a cyberattack. Though just having the incident response plan is not good enough, ensure members of incident response team practice it periodically and keep themselves prepared to deal with the incident when it does take place. Additionally, ensure everyone in the team understands their roles and responsibilities, as cyber incidents can be chaotic and perplexing. The goal should be to restore the business with minimized downtime.

2. **How have you seen cyber security changing as a result of the pandemic and the move to remote working?**
   Many businesses are arguably more exposed than ever before, as they need to manage a digital workforce now working away from on-site environments. For businesses looking to build resilience, one simple step would be to initiate more security checks within IT systems. Businesses could follow a defense in-depth approach, adding extra layers of security, with multiple defensive mechanisms put in place to thwart potential attacks and increase the security of the whole system. Digital checkpoints can be used to authorize the right people and prevent cyber criminals from accessing sensitive systems. This can be achieved with, for example, corporate laptops using specific controls like endpoint protection or multifactor-authentication not only for remote VPN-enabled access—each method adds a defensive layer to make sure the people with appropriate access can connect securely but also for privilege escalation, internet and mobile applications and more so for business partners connecting remotely.

   When everyone was working internally this was much easier to control, but the model changes when people are connected from the outside world. For further details please check out the full article written by my colleague Tiago Dias for remote working and cyber resilience.

3. **What is the estimated cost to establish a cyber security program and maintain it? (including initial assessment, followed by building the infrastructure)**
   The cost of a cyber security program really depends upon the nature of your business and risk it inherits. For example, financial institutions, government entities, critical infrastructure supporting a nation require a much more stringent security program due to the risk it inherits vs. a food manufacturer, education or retail business where security program doesn't need to be as stringent. Investment in a security program shall be done based upon your business needs and the risk it inherits. Additionally, the initial cost (CapEx) is not the only thing, it's also important to understand the total cost of ownership (TCO) including the maintenance of security program, yearly licensing fee, employee trainings etc. based on what needs to be protected.

4. **Are you seeing a change in the way ransoms are being paid? I.e. the type of crypto currency**
   Cybercriminals ransom demands continued primarily in Bitcoin, the popular digital currency due to its perceived anonymity and ease of payment. Though such ransomware attacks have become highly targeted on businesses in past few years. We are seeing most businesses refusing to pay the ransom due to the fact that these businesses have backups available for restoration and also to dissuade criminal activities.

5. **FM Global is well known for its risk control standards. To what extent are there similar standards for Cyber. In terms of insurance products, is FM Global looking to provide proper Cyber insurance in future?**
   Presently we have standards covering physical security (DS9-1) and industrial control systems (DS 7-110). Information security is a derivative of NIST, but we do not currently maintain our own IS standard though it is definitely something to be considered in the future as the risks and needs of our clients evolve.

   The FM Global Advantage policy offers broad property coverage for common cyber threats, such as introduction of a virus or other malware, denial-of-services attacks, and events that cause interruption of data services. In addition, unless the type of property or the peril is excluded, resulting damage from a cyber event is covered up to the policy limit.

   We are not looking to expand our coverage beyond property. We are specialty focused and cyber is no different. We focus 100% of our insurance offerings on the protection of commercial and industrial property. That means all our capital, research, and knowledge is dedicated to keeping our clients resilient to risk including cyber risk. However, we also understand the needs of our clients for other types of cyber insurance that may have overlapping coverage. To remove the uncertainty over how the FM Global Advantage policy will interact with another cyber policy, the Cyber Optimal Recovery Endorsement works to maximize your insurance recovery by enabling you to position your FM Global Advantage policy as primary, excess or contributing.

   Our cyber loss history further illustrates how the FM Global Advantage policy responds to a cyber event. In 2020 ransomware has been the leading cause of loss, resulting in damage to data and the associated business interruption.

6. **Have you ever been unable to pay a ransom because it is uninsurable at law?**
   The best thing you can do is to regularly backup and be able to restore systems quickly in case of a breach. Understanding your cyber risk and mitigating it earlier is the most cost-effective way to defend against such malicious events. In short, preparation before the breach, not reaction after. Additionally, ransom is not a contractual agreement with the cybercriminal to return the keys to restore environment. Some businesses chose not to pay ransom for dissuading such illegal activities and avoid being known as ransom-payer.

7. **Where do you think companies should seek security first, through management of internal process or risk transfer?**
   A business can lose millions of dollars due to a cyberattack - business interruption, lost revenue, loss of intellectual property, rebuilding operational capabilities and legal liabilities can quickly add up to severe business losses. Moreover, cyberattacks on industrial control systems have the potential to cause physical damages to the production environment. So, combination of both, a robust security program and risk transfer can help build cyber resilience. In addition, understanding your cyber coverage is important before relying on it as a supplement to your security program. The insurance coverages can be different depending on the insurance provider, so importance of understanding cyber coverage shall not be negated.

8. **Are you able to share your views on any key takeaways / learnings from the Toll and or Lion major cyber incidents?**
   Ransomware attacks have emerged as massive cyberthreat, causing serious damages to businesses – as witnessed in the case of Toll and Lion cyber incidents. Cyberattacks are inevitable in the digital era as our dependency on technology rises. No one is immune. The best way to deal with cyberattack is to understand your risk by identifying gaps in your security program through a cyber risk assessment meeting your objectives. Mitigate these gaps based on the exposure, impact on your business and your risk appetite. Build proper incident response plan, crisis management plan, train people and ensure backups are regularly done and protected. So, if the inevitable cyberattack does take place business restoration is prompt and the impact is isolated with minimized downtime.

9. **In your experience, how mature do you think Australian Manufacturing businesses are regarding Cyber Risk Resilience - perhaps on the NIST scale?**
   In my opinion manufacturers are required to enhance their security posture due to the risk they inherit due to high dependency on digitization, IIoTs and convergence between Information Technology (IT) and Operational Technology (OT) upon which their daily operations depend. Digitization brings many benefits, but it also introduces cyber risk. Generally, the level of security of the OT systems lags behind the IT. The impact of cyberattack can be severe unless security is taken seriously, and threats are managed proactively rather than reactively.

10. **How does Australia's cyber related regulations/laws compare to other countries? Are we keeping up globally?**
    Generally, cybersecurity laws cover criminal activities including the jurisdiction and corporate governance / regulations. Australia covers common issues in cybersecurity laws and regulations, including criminal activity, applicable laws, specific sectors, corporate governance, litigation, insurance, employees and investigatory and police powers – in 32 jurisdictions, further details available here at iclg.com.

11. **How do complement resourcing of cyber security with spend on cyber risk insurance**
    Risk mitigation and risk transfer are both critical to maintaining business continuity. Understanding your exposure is key to understanding the correct balance.

    Insurance is important because the majority of losses are due to social engineering or a human element factor. For example, someone clicking on a phishing email. However, just like other perils, the majority of cyber losses are preventable making risk mitigation just as important. In addition, not all loss is recoverable from insurance. FM Global recently surveyed CFO's and other senior financial executives at some of the world's largest companies to understand their perspective on cyber risk. Based on potential losses stemming from a cyber-attack the respondents noted the following impacts: degradation of their company's brand or reputation, increased scrutiny from the investment community, decline in revenue/earnings, introduction of regulatory compliance problems, decline in market share, decline in share price and new costs to mitigate the loss. The majority of these losses aren't covered by insurance. Our Cyber Risk Assessment can help clients better understand their cyber exposure at both the account and location level, which can be beneficial in understand the correct balance of risk mitigation and risk transfer.

12. **Understand that most cyber policies include a bodily injury and property damage exclusion, with write back for privacy breach. With many insurers applying cyber exclusions (removing "silent cyber" following the London market changes) - do you expect that cyber liability will evolve to cover property damage and bodily injury caused by cyber incident? E.g. an elevator or escalator hijacked through internet of things**
    We cannot comment on what the cyber liability market is going to do with property or bodily injury. The FM Global Advantage policy does respond to a cyber event that results in physical loss or damage to property other than data (e.g. machinery and equipment, building) not otherwise excluded under the policy. An example would be a virus introduced into a control system for a power plant that causes a turbine to overspeed to failure.

13. **How should we address potential cyber risk exposure by third party provider? For example, cloud based services.**
    Establish security policies, guidelines and processes for third party service providers based on your business and regulatory needs. Define the sensitivity of data and transactions done with third parties. Require third parties to follow your defined security standards and controls to manage data accordingly. Have these standards included in the service level agreements (SLAs) to ensure their applicability. Consistently evaluate third parties' security practices and regularly review your third party management policies to ensure security measures are compliant with your dynamic business and regulatory needs.

14. **What is the best framework for Cyber Security?**
    National Institute of Standards and Technology (NIST) and International Organization for Standardization (ISO) 27000 series are commonly used standards and cybersecurity frameworks. A business can choose one or more frameworks to improve the overall cyber security posture based on their familiarity with the framework, compliance and regulation needs. A misconception is that a business must chose a cybersecurity framework, factually both NIST and ISO can be used for risk assessments, data security and security programs.