# Managing Cyber Risks and Insider Threats

Worldwide losses from cyber-attacks are estimated to be in the order of 1 per cent of GDP, which makes the crime in Australia worth close to $17 billion.  Regardless of its value, one only needs to read the press to have some idea of how pervasive cybercrime has become in our society. The extraordinary growth in the 'Internet of Things' over the past several years has created a larger cyber-attack surface, increasing the prevalence of destructive attacks, improved counter forensics, attacks aligned with geo-political conflicts and cyber espionage, all of which show no signs of slowing.  What's more disturbing, is that we are seeing more attackers moving to the cloud; hosting command-and-control servers on pop-up cloud virtual machines and using social media channels for communications to avoid detection.

Cyber security threats come in many forms, and typically fall into two categories; external and internal.  External threats usually come from a competitor, organised criminal elements or a foreign government, and should obviously be taken very seriously.  However, with advancing technology and significantly improved perimeter defences against accessing confidential information, the insider threat is now more pervasive, evasive and disastrous than ever. The threat is no longer just an external one; it could be inside your business or via a trusted third party with access to your systems.  The ability to expose trade secrets, confidential information or proprietary documents over the Internet is at the fingertips of just about every individual in your organisation.  With the number of cyber incidents on the rise, as well as an increased legislative and regulatory focus on information protection, SMEs need to turn their attention to cyber risk and make it a priority.

No business is immune from attack.  Recent high-profile cases have highlighted the need for organisations to further strengthen their strategies to prevent, detect and respond to incidents thereby minimising their risk of attack. The consequences of cybercrime in all its forms – phishing, malicious software, hacking, e-mail spoofing, Distributed Denial of Service attacks or cyber extortion – can be devastating, leading to significant financial consequences, not to mention the damage caused to brand and reputation.

It is the incumbent responsibility of every company director to exercise their duty of care and diligence. This extends to assessing and addressing the risk of damage to the company from external cyber-attacks and internal unauthorised access to or disclosure of company data.  ASIC produced a "Cyber resilience: health check" publication back in March 2015, which helped guide thinking for corporate Australia.  It said that directors need to take head of their advice and evaluate if their company is properly managing cyber risk, including whether adequate resources are devoted to cyber security.

ASIC suggested that key questions should be asked of management by the Board such as:

- Which systems, if disabled, would create the most business risk?
- What data, if stolen or corrupted, would result in serious business risk?
- How is protection of these high-value assets prioritised?
- What is the current level and business impact of cyber risk and how is the executive leadership team informed on the issue?
- How many and what types of cyber incidents do we detect in a normal week? What is the threshold for escalation to our executive leadership?
- What is our plan to address identified risks and how do we preserve the integrity of data residing on our network?
- Do we have cyber security insurance that covers data breaches?

- What is the cyber security budget?  Is it adequate?
- Do existing risk management and governance processes address cyber risk and is there an annual company-wide awareness campaign around cyber security?
- Are our policies and procedures for responding to cyber incidents robust?
- How many detected security incidents have involved insiders? Are employees monitored for malicious activity?
- Do the company's outsourced providers and contractors have cyber controls and policies in place? Do they align with the company's expectations?
- How are industry standards and best practices reflected in our cyber security program and how do we compare with our peers?
- How comprehensive is our cyber incident response plan? How often is it tested? If we were breached tomorrow, who would we call?
- What constitutes a material cyber security breach?  How will those events be disclosed to the regulators and investors?

A well-designed and effectively implemented cyber resilience program will not eliminate external and internal risks, but it can assist in mitigating the likelihood of compromise and reduce the fallout from incidents, if and when they occur.

Training employees is a critical part of any cyber resilience program. Employees need to understand the value of protecting corporate, customer and colleague information, and their role in keeping it safe.  They also need a basic grounding in other risks and how to make good judgments when online.  Most importantly, employees need to know the policies and practices you expect them to follow in the workplace regarding the use of devices connected to the internet.

Importantly, when dealing with cybercrime there are a few considerations:

- Understand your threat
- Evaluate your maturity
- Assess your critical risks
- Develop your security roadmap
- Monitor employee behaviour
- Test your capability to respond
- Transform your environment.

In the 'hyperconnected world' where smart systems are merging everything digital and physical, cyber threats and the inadvertent disclosure of confidential information have a greater potential of occurring.  The challenge for owners of small to medium businesses is to understand the complexity of their systems, what they are doing and more importantly what they're interconnected with. The number of Notifiable Data Breach notifications being made to the Office of the Australian Information Commissioner suggests that Australian business needs to have a better grip on their data and tighter controls over it than ever before.  Maintaining an inventory of data assets and implementing secure network and process structures will go part way to helping your company keep ahead of potential compromises and minimise exposure to negative consequences from the interconnectedness of things.

It's worth remembering that even the best cyber resilience programs still rely on human interaction; it is critical that staff understand the cyber issue and the threats they face and their organisation faces, as well as their role in the corporate response.  Help your staff understand the risks, make them accountable for controls to manage the threat, have a plan in place to respond to an event, test that it works and ensure that everyone in the organisation remains vigilant and remember, don't be lulled into a false sense of security!

## About the Author

Scott Goddard is the Partner leading Crowe Horwath’s Forensic, Cyber and Data Analytics practice for Australia and New Zealand. He has over 30 years of experience working for professional services firms and industry in various assurance, regulatory compliance and consulting capacities.