



7 STEPS AND MAKE YOUR BUSINESS CYBER RESILIENT



Cyber security is the most prominent risk issue facing company Boards of Directors and executives worldwide. We are inundated almost daily with accounts of major corporate data breaches and compromised networks. Recent high-profile attacks such as the targeting of point-of-sale terminals at Target, Home Depot and Staples, server software at JP Morgan, and employee databases at Sony, demonstrate how vulnerable even the largest and most sophisticated companies can be. In this highly challenging environment, board members and executives are, not surprisingly, unsure of how best to protect themselves.



Proactive prevention with a focus on cyber resilience: A “how to” guide:

The first and most important step is to take measures to prevent intrusions from occurring in the first place. Just as a proper diet, exercise, hand-washing and regular flu shots are important to minimizing your odds of developing the flu, maintaining standard systems hygiene is critical to protecting your organization from being infiltrated by hackers. In fact, the Centre for Internet Security claims that up to 80% of cyber-attacks can be prevented by:



Unfortunately, blocking four out of five attacks still leaves open the possibility that a substantial number of attacks might succeed. And today, it's more a matter of when rather than if you will, eventually, be successfully attacked. What happens then?

Even well prepared companies may not know immediately that they have been breached. But those that have prepared for such an event will be much better off than those that have not. Just as conducting fire drills can save lives in the event of a real fire, preparing for the aftermath of a cyber-attack can make an enormous difference in how quickly your company gets back on its feet and how well officers and board members do in the limelight after a major breach becomes public.





How to Achieve Cyber Resilience in 7 Steps



Source: AIG

The good news is that building a cyber-resilience action plan is a step-by-step process that any company willing to commit the time and resources can accomplish. And, after ensuring you have good system hygiene, the next step is to put the right group together to work out the details. This working group should include a cross-functional collection of senior managers (Sales & Marketing, IT, Finance, Legal, Risk, HR, etc.) each of whom is willing to meet regularly to discuss cyber security, monitor evolving threats (as seen from his or her unique perspective in the company), and participate in modelling and analysing hypothetical attacks.

Once formed, the group can begin to map out the plan by, first, assessing the company's cyber risk profile. A recent study from Verizon has concluded that 95% of all cyber-attacks can be analysed in terms of nine basic patterns. A thorough study of the patterns, facilitated perhaps by the help of an external cyber security expert, can help the group determine the types of attacks their company is most vulnerable to; preventive measures can then be tailored to these patterns.

To go deeper, the team should then develop hypothetical scenarios, based on the most relevant patterns identified above, to help identify in detail possible attack modes, targets, vulnerabilities and impacts. There is no need for, and it is in fact a detriment to require, great precision in this exercise.



No one can know for certain, ahead of the event, how much damage a successful data breach will cause in terms of lost revenue, reputational harm, or stock price declines. All that is needed are rough estimates that give enough sense of scale and types of potential harm to enable the team to put together a risk mitigation strategy.

Such a strategy will involve steps to mitigate the damage to the most relevant targets in an attack. For example, if a company determines that its greatest threat is malware installations in point-of-sale software systems, directed by domestic operatives, via vendor access rights, then it might consider investments in end-to-end encryption, Application White Listing (AWL), File Integrity Monitoring (FIM), system access software, vendor access controls and regular reviews of all vendor access logs. It is important to realize that cyber-attacks cannot be fully mitigated. In these instances, having the right cyber insurance coverage in place can make all the difference in how your company performs in the days, weeks and months following a successful attack. Cyber insurance can provide critical capital and expert assistance when a cyber-security event occurs.

Companies may also want to acquire Directors and Officers (D&O) liability insurance to protect board members company officers against claims of negligence following a breach. In addition, they may want to review their property, casualty and business interruption coverage to ensure that sufficient protection exists in the event of a successful cyber-attack on the company's infrastructure. Fortunately this type of attack has, to date, been rare. But such attacks are not unheard of, and the potential for them is growing more likely given current geopolitical instabilities, especially for multinationals with exposure in more sensitive countries around the globe.

By taking the steps outlined above, a company can increase its cyber resiliency and be much better positioned to quickly recover from a successful cyber-attack.



Check these Facts Out



36.6M CYBER ATTACKS

35% Cyber attacks are from outside, the rest from inside of country from 2012 to 2014.

Source: Security Threat and Symantec, Gvernment CSRIT



497 CYBER CRIMES

497 Cyber crime cases are registered from 2012 to April 2015.



60% DEFACEMENTS

60% of government domains encountered web defacements.



\$2,300 INDIVIDUAL

Average loss per individual burglary in the U.S.

Source:IBM



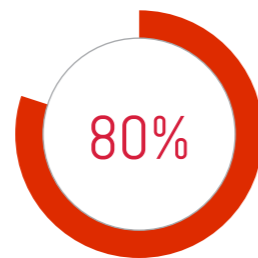
\$ 30,000,000

The largest bank robbery in the U.S. history.



\$ 445 BILLION

Annual cost of cybercrime to the global economy.

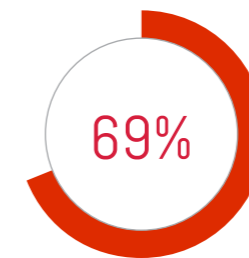


Of cyber-attacks are driven by organized crime rings in which data, tools, and expertise are widely shared.

Source:IBM



Of in-house security teams rely on multiple sources of untrusted external intelligence




Of enterprise organizations could not estimate financial impact after detecting a cyber security incident



World Class Cyber Resilience Excellence 2016

3 Day Master Class

 27th July - 29th July, 2016

 Grand Copthorne Waterfront Hotel, Singapore

OVERVIEW

Cyber attacks against companies are on the increase. They are becoming more sophisticated, destructive and costly. Cyber security is no longer an IT problem, it is major boardroom concern. The risks posed by cyber criminals are enormous – theft of money and data from corporate and customer accounts, disrupted services, sabotaged IT systems and damaged reputations. The most serious attacks can hit revenues and profits so hard that a company's very existence is threatened. This comprehensive course aims to provide business leaders with key mechanisms that organisations must develop to respond positively to change and to recover faster from adversity.

LEARNING OBJECTIVES

- ✓ Understand the basic principles of enterprise resilience and cyber resilience
- ✓ Understand how to identify risk and translate this into a risk management strategy
- ✓ Understand how to respond in a crisis, both in terms of business continuity and crisis management
- ✓ Understand the term cyber security and the evolving cyber threat landscape
- ✓ Understand how to treat cyber security as a business risk - and roles & responsibilities
- ✓ Where to focus cyber protection to get the most from your budget
- ✓ Explore how crisis and resilience management will fit into your organization

COURSE LEADERS



Jamie Rubbi-Clarke
Associate Director,
Cyber Risk Consulting



Matthias Wieser
Cyber Crisis Management
Expert



Ben Wootliff
Heads Control Risks' Cyber
Security, Practice in the
Asia-Pacific region

Quest Masterclass

Founded in 2002 in Singapore and with 8 offices in Asia, Quest Masterclass is a leading consulting and training company helping organizations and individuals achieve their goals by sharing knowledge and insights gained by experienced Quest professionals and other industry experts. Our Master Class training sessions combine the best in research; expert trainer and excellent delivery thus providing attendees opportunity learn from the practitioners and develop lasting networks with fellow successful professionals.



www.questmasterclass.com