

The evolution of Cybercrime, no longer just an IT problem.

US Centcom Twitter & YouTube accounts were recently hacked by a terrorist group while **Mr Obama** was giving a speech on cyber security threat stating: "enormous vulnerabilities for us as a nation and for our economy". The following prepared by **TestPoint** is aimed at helping Australian Executives and businesses to appreciate the risks and evolution of cybercrime expected over the next two years.

Richard Watson, Managing Director Asia Pacific and Middle East, BAE Systems Applied Intelligence, said: *"The research shows that Australian businesses are increasingly aware of the threat of digital criminality. However, they need to remain vigilant about the risks and possibilities of being under cyber-attack. Cyber criminals are highly sophisticated, constantly finding new ways to steal an organisation's valuable information, and targeting companies through a growing number of channels. Businesses cannot ignore this threat and have to take action to protect their business and customers..."*

- | | |
|--|---|
| 01 Cybercrime is no longer just an IT problem, but a business wide challenge. "Richard Watson". | 04 Business leaders must go beyond a preventive cyber strategy to also adopt an advanced " detection incident response " approach. |
| 02 Vast majority of Australian companies (84 percent) expect the number of targeted attacks to increase over 2015 and 2016. | 05 Information Analytics is the next major cyber security risk for organisations. Hackers are no-longer only focusing on computer systems. |
| 03 Most organisations still do not completely appreciate the risks posed by targeted cyber-attacks. | 06 Social Media sites can now provide key information about organisations systems simply by following employee's profiles on LinkedIn. |

Other Recent Cyber Attacks:

1. **Sony** expects that its most recent cyber hack with reported theft of personal and possibly credit card information theft will cost the organisation \$170 million per year. This is expected to increase as more details of the attack are emerging.
2. **Epsilon** the worlds largest provider of email marketing with one of the largest customer databases belonging to the largest brands was also hacked compromising personal customer information belonging to leading international brands.

Important Message: Not having a crisis response plan can cause nearly as much damage to an organisations brand than the breach itself. Companies need to continuously assess their exposure to cyber security risks. Organisations should also review their insurance cover to ensure they have cyber insurance cover which includes cover for costs associated with reputational management, business interruption, data breach notification/monitoring and finally regulatory fines. **TestPoint** can help you adopt an advanced detection incident response solution with our **Vansah ATSI** framework. Our propriety technology is an advanced detection and incident framework for organisations serious about cyber security.

3 Cyber Security Case Studies. How will your organisation respond?

A case study (fictitious example) released by EY's Global Information Security Survey 2014 involved three versions of a large telecoms operator (>US\$12b in revenue) with significant retail operations (>400 retail and customer service centres) and direct interaction with their customers, both in person and online. They will suffer a breach of customer data. Let's see how the event will unfold for the three companies based on their current cyber security maturity.

Company 1: Foundational level cyber security was implemented.

Scenario 1: This Company suffered a significant breach of customer data. The announcement was first released by an external source publicly and ultimately confirmed by the company. The company very quickly responded, confirming the breach had occurred and informing the public they had identified the problem, it had been resolved and the impact was minimal.

However, a week later the same external source stated that the damage was significantly worse than confirmed by the company, and millions of credit card details had been stolen. The company acknowledged this was true. The source made more discoveries, and this back and forth continued in the media for several weeks until eventually it was discovered that the number of records lost was over 10 times the original number quoted and that there was evidence that the breach was still active and not resolved.

Financial: The story played out in the media over a period of two months, right before their busiest time of the year. They lost many customers, but the ultimate cost was double-digit percentage loss in both share price and revenue. The company has still not seen a return to pre-breach numbers (over a year later). Eventually the total cost of the breach is expected to exceed 5% of annual revenue.

Operational: The company spent many months of effort focused on this problem and rather than fixing it, their efforts were focused on responding and managing the media crisis that occurred. They had to identify and provide credit monitoring services, work with banks and customers to settle their concerns and ultimately attempt to restore customer confidence.

Personal: This led to the termination or resignation of many executives and leaders throughout the organization, including both the CEO and CIO.

Company 2: Cyber security foundation and continuously adapts to ongoing change to business and environment.

Scenario 2: This Company suffered a significant breach of customer data. The announcement was first released by an external source publicly and ultimately confirmed by the company, but the company did not comment for almost a week.

They provided a very measured response, confirming the breach, identifying that they knew where it had occurred, felt confident they had addressed the problem and were waiting to confirm the extent of the problem until the investigation was complete. Two weeks later they came out publicly and confirmed the total loss, confident they had identified the source of the breach, and had put in place mitigating controls and were working on the permanent resolution. Since then there have been no contradicting reports.

Financial: This incident generated three primary news stories, but was in and out of the media fairly quickly. While the breach was significant, the company did not experience a high churn in customers. They did provide credit monitoring, and introduced special offers to bring customers back to the stores, at some cost. Within three months, they had returned to pre-breach revenue, share price and operations.

Operational: This story had left the media spotlight within a month. The company put more time and effort into fixing this problem than responding to media pressure. They had to work with banks, brands and customers and their efforts focused on accretive services and support for the business.

Personal: Throughout this challenging time the company showed solid leadership in the event of a crisis, and sustained the confidence of customers, shareholders and the board.

Company 3: Mature cyber security, adapting to future environments and has alert ready monitoring.

Scenario 3: This Company suffered a significant breach of customer data. In the months prior to the attack, the company had worked with peer organizations, law enforcement and their internal threat intelligence teams to collect relevant attacker activity information and identify the risks to the company. They also learned about other breaches in their sector. As a result, they were able to develop additional segregation and protective controls, and create scenarios for attack and response exercises.

Ultimately, they were not able to stop the attack taking place, but no payment details or sensitive personal information was lost as it had already been stored separately and protected with different controls. Due to additional monitoring, the breach was discovered internally first. Shortly after the incident, the company released a public statement about what had happened and how it had been addressed.

Financial: While the cost of recovery from the breach was significant, the impact on share price, customer churn and media exposure was minimal to none. The cost was confined to investigative and remediation activity. The company was able to control the media attention with enough confidence that they did not need to offer credit monitoring service, which is the usual response to a customer data breach. This alone will save at least US\$350m in potential cost of response and, arguably, it strengthened their customers' and regulatory confidence.

Operational: There was virtually no media coverage beyond the statement released by the company itself; they could therefore focus their efforts on returning to business as usual. The cost of investigation and remediation became an additional operational cost, so the breach investigation did not negatively impact their BAU processes and weaken their defences — a frequent error that creates an aftershock affect, which can cause subsequent breaches.

Personal: No terminations or resignations were tabled, and there is evidence of renewed confidence in the executives.