Deloitte.

# Cyber-crime – it's where the money is


## Cyber-crime is on the increase. Organisations of all sizes in all industries are being targeted. Despite growing investment in security, the number of extreme cyber-breaches and the average cost per breach continue to rise.

Beyond the direct cost of remediation, the consequences to a business of a successful cyber-criminal attack can be severe, and include increased customer churn, regulator actions, and reduction in company valuation.

Boards are increasingly concerned by the rising cyber-crime threats and unsure if their organisations are sufficiently protected. At the same time, many organisations continue to view security as a technical IT issue, lacking a clear understanding of the business impacts, and an appropriate level of cyber-security maturity for their businesses.

The key question any business needs to answer is: 'Are our security capabilities sufficient for our risk appetite?' In any assessment of capabilities, businesses must take care to note that *compliance does not equal protection*, and simply checking compliance with a controls scheme is not sufficient to ensure cyber-security maturity and capability.

### Scary cyber-crime statistics

News of mega-breaches is now commonplace; but, it isn't just the major breaches which are disturbing. The median number of IDs exposed per breach is 6,777[1], with the average cost of a malicious breach per stolen record reaching US$161[2]. The median cost for a malicious breach therefore adds up to more than US$1m.

It just takes days from initial cyber-compromise to the stolen data being taken out of the company for 85% of breaches. Unfortunately, the average length of time from initial cyber-compromise to discovery of the breach is, for 66% of breaches *months or years*[3]. It seems that businesses are giving the cyber-criminals plenty of time after a break-in to take what they want.

Not all the money to be made in cyber-crime is from stealing information assets. There is a thriving market in the dark internet for hacking kits, money laundering services, stolen identity and credit card brokers. And various cyber-crime services which can be rented like any other cloud services. Cyber-crime is big business.

### Boards are now focusing on cyber-security

Boards are now broadening the discussion of IT risk beyond financial controls to include a focus on cyber-security and protection of critical information assets. The increased focus is forcing businesses to rethink cyber-security and to question their capabilities.
Key questions for management include:

- Do you have recurring issues associated with information security, e.g. inadequate access controls to systems and data, or large numbers of technical vulnerabilities?
- What are your top three areas of concern around managing information security, e.g. the loss or disclosure of sensitive information? Inappropriate user access to systems, etc.?
- Are you aware of any recent significant cyber-security breaches? If not, are you confident that the business is well secured against potential breaches?
- Do you have a comprehensive response plan in the event of a breach?
- Do you know what and where your critical assets are?
- How do you confirm that you have performed all reasonable steps to protect the security of the critical information assets for which you are responsible?

1. *Symantec 2014 Internet Security Threat Report*
2. *Ponemon 2014 Cost of a Data Breach*
3. *Verizon 2013 DBIR Report*

- For significant technology or business transformation projects currently running or planned, does the business fully understand the information security risks associated with the projects and is it taking appropriate mitigating activities?

## Key principles to managing cyber-security risks

The following key principles underpin any successful cyber-security program, promoting an integrated approach to business, technology, and people.

1. ***Understand your risk appetite***
   Know your business, know your critical assets, and agree the risks to the business.
2. ***Understand your required level of cyber-security maturity***
   Define where cyber-security needs to be positioned in governance, technology, and operations to confirm that your risks are within the tolerances set by the business.
3. ***Be prepared for the worst***
   It is highly likely that most business have already experienced a successful cyber-breach. Determine if you have the organisational and technical capability to rapidly detect and respond to a successful attack to limit the impact.
4. ***Instil an awareness of cyber-security risks and a culture of security-by-design***
   Confirm that cyber-security risks and the security activities of the business are understood across the organisation, from the board to the staff to third party providers. Confirm that all business and IT changes incorporate security requirements from the outset.

## Security as an enabler

Doing the right things in cyber-security mean protecting the critical cyber-assets of the business.

All businesses will at some point be attacked, and most will be breached by cyber-criminals and other cyber-actors. It is those which view security as an enabler to the business which will be most prepared, and which may be able to limit the impact of the breach.

Security readiness is not about building walls around the business – the time is long past when firewalls and anti-virus alone offered sufficient protection.

Cyber-security readiness is about building and evolving a security program which is integrated into the business, which is capability, rather than compliance focused, and which is a true enabler of the business in the digital world.

## Contacts


**Tommy Viljoen**
*Partner, Risk Services*
Tel: +61 2 9322 7713
tfviljoen@deloitte.com.au

**Greg Janky**
*Partner*
Tel: +61 3 9671 7758
gjanky@deloitte.com.au





MCBD_Hyd_09/14_50933