# IT Governance:
# **The Directors Cut**

## What Directors Need to Know

Huntsman®
Defence-Grade Security Platform

Company directors are responsible for good governance in organisations and, increasingly, this means safeguarding a burgeoning volume of sensitive information.

Ignorance isn't a valid excuse in the eyes of the law or shareholders, and just because an action is 'legal' doesn't mean it is good practice. If organisations have a serious data breach, telling their customers or shareholders that they were compliant will be no help. As the Economist summed up way back in 2009, '… a box-ticking approach to the management of strategic risks is, in a post-crisis environment, more likely than ever to lead to corporate ruin.'[1]

In 2015 it is clear from the high profile attack at Target and, more recently, the US Office of Personnel Management (OPM) that the impact of control and governance failures really does reach right up to the board level. In both cases there were departures of senior management personnel as well as impacts to customers, market capitalisation and the organisations themselves.

Organisational governance processes must ensure that risk management and compliance programs are appropriate for the needs of the organisation.

*'You must be able to show that a governance program will lead to specific business improvements, even if the end result might simply be that your CEO won't go to jail.'*

**Gartner**

## 'BOARDS ARE STILL CLUELESS ABOUT CYBERSECURITY'

'Your organisation will come under attack,' Thor Olavsrud writes in CIO.com. 'It's not a matter of IF. It's a matter of WHEN.' He adds that '… technology has become the central component of nearly all business processes … [therefore] information security should sit firmly on the boardroom agenda.'[2]

New technologies such as virtualisation, cloud computing and smart mobile devices are creating new security challenges by moving more connections, transactions and data flows outside the organisation.

Directors need to better understand their organisations' exposure to cyber attacks, whether their intent is theft of intellectual property or customer data, or crippling your operation (hacktivism). A good reputation is a company's greatest asset, and damage to that asset can be painful and expensive. Just think about Sony's Playstation: the cost of its data breach was calculated to be around US $1.25 billion[3]. More recently Target has reported costs running into the hundreds of millions[4] and following the breach several executives, including the CEO, lost their jobs.

## WHY REGULATION IS NOT PROTECTION

As a business, Critical National Infrastructure (CNI) is far more serious than computer games. These industries deploy industrial control systems that were designed first for safety and reliability, and not at all with IT security in mind. In addition, although originally isolated, many of these control systems are now connected to corporate internets, which increases their exposure.

Compliance with industry regulations will not protect organisations from damage. As a business risk, IT security needs to be monitored and managed like any other. That means that directors need to ask the right questions, such as:

- What is our response plan in case of cyber attacks and data breaches?
- How fast can we identify, diagnose and resolve the cause of a breach?
- Are our records comprehensive enough to defend a court action?
- How often do we stress-test our IT security systems, and to what extent?
- How do we train employees to view security as their responsibility?

## FOCUS ON THE 'RIGHT' RISKS

An organisation's information governance strategy must be driven by business strategy, and have clear business metrics to measure performance. However, even with defined roles, agreed goals and performance metrics, information governance can only deliver if business and IT stakeholders collaborate closely.

*The GRC risk dashboard enables business managers to make informed risk-based decisions in real time, not hours or days later.*

To date, the fear of a breach has led to almost total reliance on protective technologies that claim to prevent attacks by IT security managers, yet this is false security. All organisations holding valuable information are targets and are at risk from attacks specifically seeking to circumvent or subvert those defensive controls to access valuable information.

The volume of business information held on portable devices is just as big a risk for information governance as cyber attacks or internal fraud. A survey conducted by the Cloud Security Alliance found that data loss from lost or stolen devices ranked higher as a security issue than mobile malware[5] with a considerable number of mobile devices lost every year. With continued wider adoption of mobile platforms and the interactions between these and cloud applications the organisational control environment is even more complex with more points of potential failure.

In its recommendations to minimize IT security risk, Australia's financial regulator APRA advocates regular assessments and audits of the security risk and control environment. One key suggestion is that 'appropriately trained and functionally independent security experts be used in conjunction with internal security teams.'[6] In other words, don't rely just on internal audits or those imposed by your industry's regulator; get an external perspective.

## APPLY ADVANCED APPROACHES

Advanced IT security technologies can also impact the effectiveness of Information Governance. Systems using machine based learning and other intelligent algorithms to 'learn' the pattern of events on the network, using Behaviour Anomaly Detection (BAD) capabilities, and alert the IT security team when unusual events occur or when traffic, systems or staff behaviour deviates from the norm. Using behavioural technologies, IT staff can detect unknown or unknowable threats that are stealthy, hidden or undetected by other security systems, and uncover intrusions or data theft in real time, before serious damage is done.

Visibility is also vital – not just in voluminous monthly reports but "live" - Governance, Risk and Compliance (GRC) dashboards are increasingly demanded to translate complex metrics of security and operational performance into clear graphs of business risk. These interfaces are based on business role, so key stakeholders can recognise the impact of the organisation's IT security status on their areas of responsibility, be it finance, operations, sales or customer support. A continuous view of GRC operations enables business managers to make informed risk-based decisions in real time, not hours or days later.

## BOTTOM LINE BENEFITS

From an information governance viewpoint, non-compliance and failed audits can impact confidence in the business and its operation. Perhaps a more telling observation, however, is that according to a recent Cyber Security Report: in 2014 successful attacks remained undetected in victim organisations, for an average 205 days[7]. For any organisation this is an unacceptable time at risk and a clear message, for all of us as Directors, that information governance needs our careful attention and diligence.

Effective information governance can prevent the painful consequences of data breaches or loss, including the penalties, embarrassment and damage to reputation. As cyber threats continue to emerge and evolve, it is central to businesses to have effective monitoring and control systems in place.

It is also essential for directors and other key stakeholders to take a more active role in establishing, defining and overseeing policies to safeguard information assets.

## REFERENCES


1 Beyond Box-ticking: A new era for risk governance, Economist Intelligence Unit Report, September 15, 2009

2 CISOs Must Engage the Board About Information Security, CIO.com, May 31, 2013

3 As Sony Counts Hacking Costs, Analysts See Billion-Dollar Repair Bill, Wall Street Journal, May 9, 2011

4 http://www.pymnts.com/news/2015/target-home-depot-reveal-full-breach-costs/#.VbH-yHgkCjA

5 Data Loss from Missing Mobile Devices Ranks as Top Mobile Device Threat by Enterprises, CSA, Oct 4, 2012

6 APRA Prudential Practice Guide PPG235, APRA, December 2012

7 M-Trends 2015: A View from the Front Lines, FireEye Inc, 2015

**Author: Peter Woollacott**
Co-Founder and CEO, Tier-3

Peter Woollacott is the co founder and CEO of Tier 3 Pty Ltd, the software company that holds the patent for Behavioural Anomaly Detection and developed Huntsman® Intelligent Security.

He has 25 years' experience in operational and risk management with companies like Lend Lease, CBA, AXA, EDS, PWC and Bain International. Peter holds Masters Degrees in Applied Finance and in Business Administration, and lectures in executive post graduate education at Macquarie and Sydney Universities.

Peter may be contacted at
pwoollacott@huntsmansecurity.com

Please visit the Huntsman Resources page at **www.huntsmansecurity.com/resources** for White Papers, Compliance Guides, Solution Briefs and more resources by this author.

**Huntsman | Tier-3 Pty Ltd**

**Asia Pacific**
t: +61 2 9419 3200
e: info@huntsmansecurity.com

Level 2, 11 Help Street
Chatswood NSW 2067

**EMEA**
t: +44 845 222 2010
e: ukinfo@huntsmansecurity.com

100 Pall Mall, St James
London SW1Y 5NQ

**North Asia**
t: +81 3 5809 3188
e: info@huntsmansecurity.com

TUC Bldg. 7F, 2-16-5 Iwamoto-cho,
Chiyoda-ku, Tokyo 101-0032

**Americas**
toll free: 1-415-655-6807
e: usinfo@huntsmansecurity.com

Suite 400, 71 Stevenson Street
San Francisco California 94105

huntsmansecurity.com linkedin.com/company/tier-3-pty-ltd twitter.com/Tier3huntsman