INFOSECURITY: A BOARD MATTER

THREATS AND COUNTERMEASURES – A WHITE PAPER FOR SENIOR MANAGERS

INTRODUCTION: WHAT IS HAPPENING

Information security is increasingly becoming a matter for boards and senior management, not just the IT department. It is a complex issue because technology now pervades every layer of an organisation. Consequently, addressing security needs the co-operation of all parts of a business. Recent high-profile data breaches are helping to push the issue to the top of many boards' agendas. Making a case for more investment in security, therefore, must be seen in terms of business risk and not just technology threats.

This white paper is aimed at senior management in Irish-based companies; it outlines some of the main cyber-security threats and offers advice on how better to guard against them. Material for this paper was prepared from presentations given by recognised experts and industry leaders at an Information Security Forum hosted by InfoSecurity Ireland in November 2013, which focused on presenting security issues to boards and senior executives.

"It's very hard to get a good name in this connected world – and very easy to lose it"

Kilian Colleran, CEO, BAE Systems Detica NetReveal and co-founder of Norkom

BREACHES: WHAT IS AT STAKE?

Key to making a successful business case for increased spend on security, or support for awareness training, is having good-quality, actionable information. By knowing where vulnerabilities exist, businesses can focus their efforts to minimise the risk. One of the nagging problems with information security has been the questionable quality of data available to make informed decisions.

There are useful independent sources which can help to identify risks to businesses. Verizon's annual Data Breach Investigations Report (DBIR), now in its sixth year, offers a wide-ranging snapshot of the nature and extent of cyber risks that many businesses face. In the process, it punctures a few infosecurity myths, helping businesses to avoid guarding against hyped-up threats that don't correspond to actual risks. For example, the 2013 report found that 75 per cent of attacks are opportunistic and not targeted at a specific organisation or person. The majority of these attacks were motivated by financial gain rather than corporate or state-sponsored espionage of the kind

"The acid test is not having the crisis, it's how you manage and respond to it"

Michael Baume, Associate Director, Risk Management International

COUNTERMEASURES: WHAT ACTIONS CAN BE TAKEN

The rapidly changing nature of the threats means that organisations need to become more aware of what is happening on an ongoing basis. The first step is to map the threat landscape that is unique to your organisation, in order to better allocate spending according to priorities and budgets. This involves knowing what information would pose a real risk to your organisation if it were lost; defining what risk means to your organisation, and what happens when that risk escalates. It's worth keeping in mind that in today's interconnected world, no organisation is an island: points of weakness may be in the business's wider supply chain and ecosystem – not just internally.

Businesses should prepare a plan for a range of risk scenarios, leading to the deployment of often simple security controls inside and around the assets that really matter. Having a system of checks and balances also helps to ascertain which controls are effective and which are not. Regularly proving and testing your defences will help to build confidence in your organisation's ability to manage risk in real time. Use this information to make targeted investments in places where protection is currently weakest, and this will deter many of the cybercriminals who typically look for the softest targets they can find.

Although the well-worn security maxim states that people are often the weakest link, they are also an excellent asset when employees are made aware of risks to the business and are given the means to easily report potential security incidents to a nominated person in the organisation. That's especially critical, given that, according to the Verizon report, two-thirds of security breaches remain undiscovered for months.

"You should be able to deploy simple security controls inside your organisation, around the assets that really matter"

Paul Pratley —Investigations Manager, RISK Team at Verizon Enterprise Solutions

CONCLUSION: WHAT TO DO NEXT

Making security a company-wide effort that combines people, processes and technology, goes a long way to improving an organisation's risk posture and its vulnerability to attack. For too long, a company's information security function was unfairly perceived as a barrier to doing business in an agile and flexible way; preventing organisations from responding quickly to opportunities and market changes. In fact, a fairer description of security's role is like the brakes on a car – you can travel faster when you've got good brakes. Become certified to a standard like ISO 27001: this will give demonstrable proof to customers and external stakeholders that your business takes active steps to protect the data it holds.

Good information security isn't just best-practice business: in a time of uncertainty around data protection and information privacy, establishing and maintaining trust in your organisation is a source of competitive advantage.

"Security is a complex business issue and requires co-operation across all parts of the business. It's not just an IT problem"

Brian Honan, CEO, BH Consulting and SC Magazine's Information Security Person of the Year 2013.

This document is produced by InfoSecurity Ireland (ISI), which is an industry-led organisation that facilitates networking, collaboration and marketing of the Irish information security sector www.infosecurityireland.org