BY
Pat Larkin

As co-founder and co-owner of Ward Solutions, Pat Larkin has over 17 years' experience in the IT industry, the last 10 of which have been spent in commercial IT management. Prior to entering private business, Pat was an officer in the Irish Defence Forces, serving in both a line role and subsequently as IT Operations Manager of the Defence Forces Communication and Information Services Corps.

The business impact of the current cybercrime spree and what to do about it

Pat Larkin, Ward Solutions, looks at the impact of cybercrime on business.

Cybercrime is not a new development; the first recognisable virus was produced way back in 1982. Scammers and social engineering have existed in numerous different forms since the serpent managed to con Adam and Eve in the Garden of Eden!

Much has been written, both in this magazine and on other forums, about the current cybercrime situation in Ireland. Ward Solutions recently conducted a survey to assess the state of information security in Ireland and Northern Ireland, compiling the results in our whitepaper *Mapping the CyberSecurity Landscape.* The results provide a fascinating insight into organisations' approach to information security, and the relative maturity of their processes and strategies.

One of the most striking findings to arise from the survey was the fact that one-third of Irish and Northern Irish businesses suffered a security breach in the past year. In our experience this cybercrime spree is having a real impact on businesses throughout the country and is forcing many to reassess their approach to information security.

To understand the long-term impacts of the current cybercrime crime-wave it's important to look at the short term impact that it is having on organisations and the steps that they are taking to protect themselves.

The day to day impact

- **Financial Loss** – Ransomware, which developed from email phishing scams and now incorporates advanced malware strains, has enabled cybercriminals to easily extort money from businesses both big and small. Faced with the potential loss or encryption of sensitive data many businesses are opting to pay the ransom demanded of them. Ransoms can range from €300 to €50,000, depending on how valuable the encrypted data is perceived to be and how deep the company's pockets are.

- **Loss of data** – Recently the spotlight has moved from larger data breaches to ransomware but data breaches are continuing year on year, while also becoming larger in scale and more frequent. While the tactics employed by attackers are similar to those using ransomware their focus is more on liberating valuable data rather than making it inaccessible. The spoils can then be resold to the cybercriminal ecosystem that specialises in buying and utilising personal data, financial data, healthcare data, intellectual property, blackmail data, etc. Recently, the frequency of reporting loss of consumer data has resulted in breach fatigue setting in among the general public. However new legislation, such as General Data Protection Regulation (GDPR), will give regulators very little latitude for generous interpretation of non-compliance. This, coupled with harsh fines of up to 4% of global turnover, will bring protection of personal and privacy data into sharp focus in 2017. To use a recent example, the Talk Talk breach in the UK which resulted in a fine of over £400,000 by the Information Commissioner's Office would (under the new General Data Protection Regulation (GDPR) coming into force in May 2018) potentially be over £70M.

- **Targeted attacks on employees** – A lot of effort goes into applying the best security technologies to try and help secure your information. Cybercriminals often have best effect in targeting people to help get around process or technology controls. Lots of ransomware and fraud attacks are achieved by targeting those with obvious relationships to the organisation that are easily discovered via social and professional networks such as Facebook, LinkedIn etc. By sending simple but credible emails either asking you to click on a link or open an attachment, malware can quickly and easily be uploaded to your network.

- **Risk transferral down the supply chain -** A number of high profile security incidents have resulted from larger firms being compromised by suppliers who are closely integrated into their information systems and networks. We estimate that within three years, as larger enterprises improve their supply chain assurance and due diligence processes to manage risk, a recognised information security accreditation such as ISO27001 will effectively be mandatory for suppliers looking to do B2B business model in several key sectors.

- **Misspending or misallocation of resources** – One of the trends that we identified in our 2016 survey was the significant increase in organisations' information security spend. 48% of organisations surveyed stated that they planned to increase security spend in 2017, with more than a quarter of organisations planning to spend between 25 and 40% more than the previous year. Ward's experience is that in a lot of cases this spend is directed at what we would ironically call 'silver bullet solutions,' i.e. the latest and greatest new security platform or technology. This is often done by organisations that are unable to assess the current state of their security play or form a quantifiable ROI argument against this spend. It is also frequently done without correlating a prioritised mitigation plan against a specific risk register. Without any of these activities being undertaken, significant security spend is often simply wasted in the rush to be seen to do something.

- **Miscommunication between the board and the IT department -** Increased risk of cyber-attack coupled with increasing compliance demands has resulted in boards showing heightened interest in their organisation's risk profile and what is being done to improve weaknesses or sub-optimal states. There has always been a historic communications gap between security professionals and the board, primarily because in the past the board weren't listening. Now they are listening and talking – and asking hard questions. IT staff are now finding it very difficult to produce language and data that the board needs or understands. Any gaps in this critical communication channel lead to confused or ineffective organisation security strategy.

- **Consumption of scarce resources** – Skilled Information security resources are in very short supply and are becoming increasingly expensive to hire as a result of increasing risk. As well as this, these employees are frequently stuck firefighting day-to-day IT issues and are typically not being used to develop a coherent organisational security strategy as a main priority. Similarly, ICT infrastructure is facing increased workload in trying to detect, prevent or recover from the increased security threats. Legacy technologies such as traditional anti-virus and firewalls are increasingly ineffective against modern threats and attacks. Organisations need to either push their vendors to deal with the new threats much more effectively, or else stop paying good money for ineffective controls and move to vendors or new controls that help reduce their risk profile.

- **Cybercriminals lurking in systems for up to 7 months prior to detection** - Ward Solutions' survey showed that almost half of the organisations we surveyed had experienced some form of security incident within the last 12 months. International statistics show that on average an organisation may have been breached by malware up to 229 days before this breach is detected. In industry terms this is 'dwell time', i.e. the time that a cybercriminal has to encrypt or steal your data or execute a fraud. Organisations must aim to reduce this time.

Organisations' Responses

We recommend that organisations take the following steps to manage their information security processes and reduce risk:

- Organise your approach to information security strategically and systemically – e.g. use a best practice framework such as ISO27001

- Engage your board in a language they understand – tell them your current security posture and report regularly on progress using baseline and metrics relevant to the board members and the business. Following this, seek direction from the board in terms of risk and mitigation priorities

- Secure your supply chain and don't be hypocritical about your own organisation's approach to your customer or partner's information security

- Secure the 'human firewall' by continuously engaging your staff with targeted training, awareness and incident response commensurate with their roles

- Focus your efforts on identifying and mitigating prioritised risks – don't be tempted by 'silver bullet' solutions not tied to your organisational risk register

- Move from prevention only strategies to whole security lifecycle – identify, protect, detect, respond, recover

- Seek to achieve compliance to new standards early

- Regularly review your security spend for efficacy.

Despite changing techniques, the fundamentals of fighting cybercrime remain the same. Identify your risks and prioritise them according to likelihood of occurrence and impact on your business. Target your risk mitigation efforts to your highest priority risks and adopt a layered defence strategy incorporating people, processes and technology to protect the confidentiality, integrity and availability of your information. Do so in a systemic way and don't seek to reinvent the wheel.

Ward Solutions works closely with organisations to develop tailored information security models to fit their needs. If you would like to read more about Ward's survey findings the full report is available to download from our website - www.ward.ie