Cybercriminals are increasingly using ransomware, malware and hacktivism methods to finance their activities. Australia is not immune with 5% of worldwide ransomware incidents recorded in Trend’s 1Q2014 Security Roundup occurring here. The notorious CryptoLocker leads the charge. By contrast Germany, with a population of 82 million, accounted for just 4% of ransomware incidents. McAfee has also released its 2014 Threat Predictions, which highlight ransomware as the top threat against organisations over the next 12 months.

There are two main “vectors” by which organisations are likely to come under cyber-attack from cybercrime gangs – direct attacks on external facing web servers or indirect attacks using deception-based methods that bypass external security measures and provide deeper access to organisations’ IT infrastructure.

Direct external attacks, such as hacktivism, and brute force Distributed Denial of Service (DDOS) attacks seek weaknesses in organisations’ external facing security. These attacks can result in business process interruption (e.g., loss of capacity to conduct online sales) and reputational damage to organisations. For example, a cybercrime gang may “take down” an online store through a DDOS attack and demand payment to stop the attack.

Malware and ransomware attacks are more insidious and generally more dangerous. They can be generic, attempting to infect as many computers, individuals, or organisations as possible; or specifically targeted to particular individuals or organisations. Cybercriminals generally use social engineering techniques to trick employees into allowing their computer systems to be infected. An advanced attacker will often use highly customised malware or previously unknown security exploits that have higher probabilities of evading detection by anti-virus protection software.

Once a computer system has been compromised, most ransomware will attempt to encrypt user documents and other user-generated files before alerting a user that the files are inaccessible.

The user will be directed to pay the cybercriminal for a copy of an encryption key that unlocks encrypted files. The payment is often made via a Bitcoin transaction, which cannot be traced by law enforcement.

Apart from ransomware, most other versions of malware attempt to disguise their presence on computers or networks. Employee malware will often seek to infect other, more critical systems, and gather vital information. In a worst-case scenario, cybercriminals gain remote administration rights to organisations’ IT environments, resulting in complete data exposure.

The primary business risks posed by ransomware/malware include intellectual property theft, customer data leakage, business data loss and exposure to externally initiated fraud.

What are the potential costs to your organisation?

The most common ransomware attack on individual computer systems, CryptoLocker, is closely followed by a demand for an initial ransom payment to be made within 72 hours. Failure to pay within 72 hours results in demands for higher amounts.

Victims need to know that even when payment is made, there is no guarantee the cybercriminal will provide a key to unlock the files.

That means critical business files may remain inaccessible after the attack, resulting in further loss.
While most organisations at least have IT security basics covered (e.g., anti-virus software, firewalls), the following measures are less common but arguably more important in defending against the most dangerous attacks (e.g., zero day exploits, spear phishing).

- Make IT security and IT risk management a business issue rather than just a technical process.
- Install an intrusion detection system and monitor it.
- Ensure critical data and systems are backed up regularly and have appropriate business continuity procedures in place to recover from system interruptions.
- Ensure client/supplier-facing staff are trained to identify social engineering tricks and techniques.
- Purchase a LAUW eRisks Cyber insurance policy.

Malware that facilitates an externally directed fraud could cost an organisation many hundreds of thousands of dollars. The usually substantial costs likely to be incurred after a cyber-attack can be categorised as direct and indirect (or consequential).

**Examples of direct costs**
- The ransom or ransoms,
- Data recovery and data rebuilding (IT consultants and data capture personnel),
- Managing the reputational impact (external consultants, communications to staff, clients and other stakeholders, marketing and advertising), and
- Consultants’ fees to assist with quantifying losses and managing the recovery (including preparing an insurance claim).

**Examples of indirect costs or consequential losses**
- Loss of gross profit where sales have been lost (particularly when capacity to generate online sales has been impacted), and
- Additional costs incurred to maintain business operations or mitigate sales losses - examples include advertising to regain customers and costs to accelerate data recovery and systems repair.

Forensic Advisory Services (FAS) provides forensic accounting expertise to insurance professionals, undertaking assignments for claims managers, loss adjusters and legal advisers from initial notification through to claim finalisation.

**For more information: visit www.fas-au.com**

London Australian Underwriting (LAUW) is a specialist Lloyd’s underwriting agency.

LAUW partners with Forensic Advisory Services and other professionals, including risk assessors, forensic experts, public relations firms and top tier legal advisers who together form LAUW’s Incident Response Team.

**For more information: visit www.lauw.com.au**