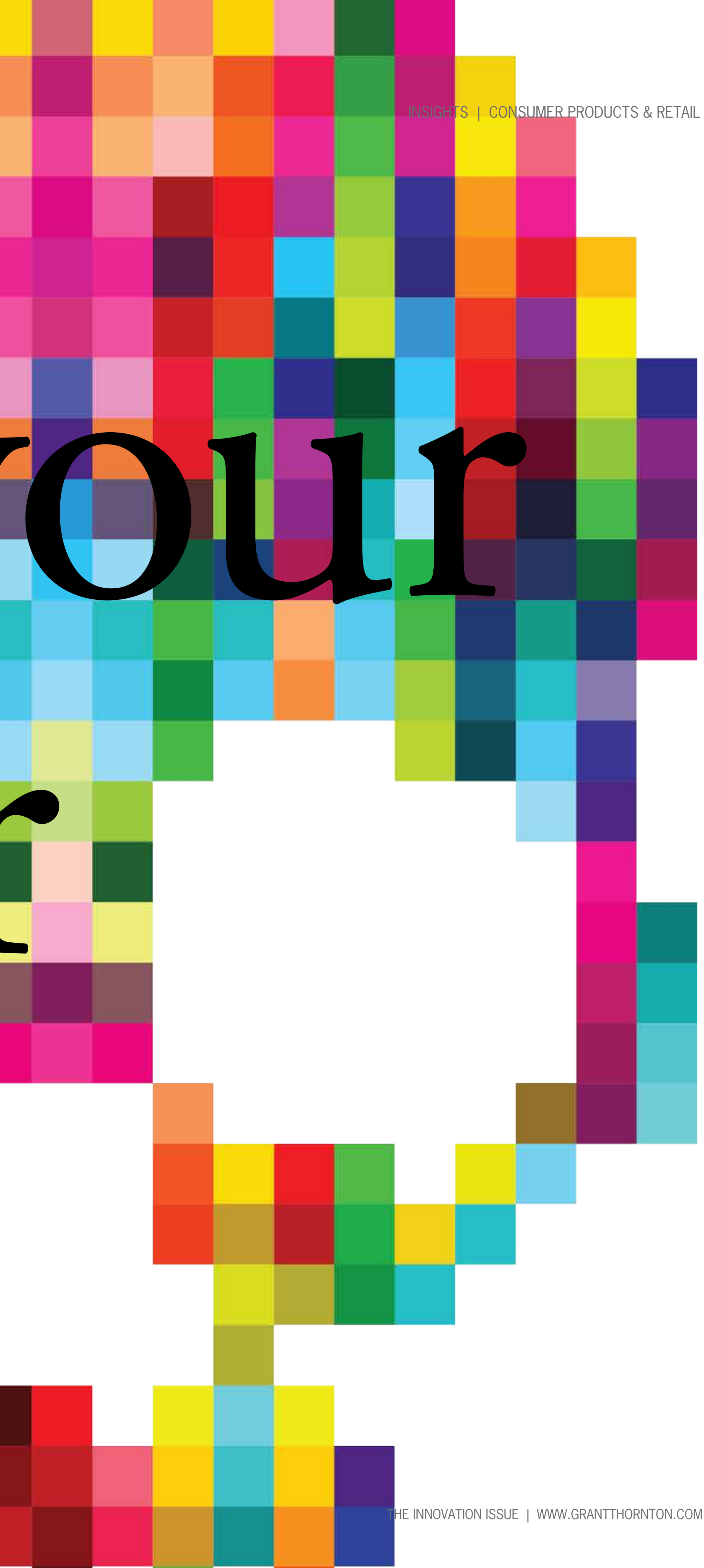
Meet y
Hacker

THE INDIVIDUAL WHO IS TRYING TO BREACH YOUR COMPANY'S SECURITY MAY BE ON THE OTHER SIDE OF THE WORLD, NEXT DOOR, OR IN YOUR OFFICE, BUT IT IS POSSIBLE TO PROFILE WHO THEY ARE AND HOW THEY WILL ATTACK



It used to be the case that you could spot trouble when it was in the neighbourhood. The perpetrators would turn up in longboats or chariots and, even if you didn't actually encounter them personally, the evidence of their passing was clear.

The internet has changed all that. Invisible, undetectable, the invasion of your personal computer or business may have been going on for years before the damage is finally revealed.

Dr Stanton Samenow believes that those who commit cyber-crimes are indistinguishable from 'bricks and mortar' offenders. Samenow, the author of Inside the Criminal Mind, has been studying the criminal mind-set since long before the PC was invented. He contends that criminal activities are driven by the same personality traits, whether they're carried out digitally or physically.

'There's a whole mentality and a whole view of looking at life in which you see yourself as the hub of a wheel around which everything revolves,' he says. 'It's power and control for the sake of power and control. It may be about the proceeds and what you get from it but they're really just an index of how successful a crook you are.'

While criminals are the same regardless of what channels they use, technology may afford them more opportunity to do what they do, Samenow adds. 'If you were going to be a bully, that was something you did in person. Now, you can bully and intimidate a larger number of people and you never have to confront them.'

The same may go for those who break into an organisation's systems online: they may have always had the inclination to intrude, but the ability to do it from a distance could be what pushes them into action.

Kevin Brown, General Manager for Threat Intelligence and Investigations at BT Security, identifies four kinds of hacker: the criminal enterprise, the hacktivist, the terrorist and the nation state. 'The motivations of a cyber-criminal will vary from someone wanting to claim "kudos through hacktivism" to someone working a regular 9 to 5 role,' says Brown.

The aims of a cyber-criminal will affect their operating patterns and even their targets. 'In a general sense, knowing the motivations of hackers and how likely you are to be a target can be useful in justifying a budget for defence,' says Joe Stewart, who directs malware research for the Counter Threat Unit research team within Dell SecureWorks, the security division of PC giant Dell.

Ollie Whitehouse, Technical Director of IT security consultancy NCC Group, breaks down these motives into ideological, financial and revenge-driven.

Those tasked with corporate espionage – especially nation states with virtually unlimited resources – could conceivably have all three of those motives. They often have specific attack parameters, mounting what security experts call advanced persistent threats (APTs). These are stealth attacks, during which intruders can stay inside a network for months at a time, pilfering data on the quiet – they don't want to be found.

Criminal enterprises are driven by money as a motive, but they still tend to play a long game. One of the biggest enterprises was a group led by Albert Gonzalez, a US citizen sentenced to 20 years in jail after a multi-year crime spree that saw him compromise more than 250 companies, causing more than $1 billion in damage.

Gonzalez and his partners would break into retail networks and place malware on their back-office computers that would secretly read and transmit credit card information as it was processed. He stole 45.6 million credit card records from retail network TJX alone. His motives were clear: he called his operation Operation Get Rich or Die Tryin', and spent the money on lavish, drug-fuelled parties for his cohorts.

Conversely, hacktivists are often driven by ideology, which leads them to grandiose acts of cyber-intrusion designed to be highly visible. Such was the case with Jeremy Hammond, part of a hacktivist group called LulzSec, who was sentenced to 10 years in a federal US prison for stealing data from private intelligence firm Stratfor and posting it online.

In 2004, the then 17-year-old Hammond had given a talk on 'electronic civil disobedience' at the Defcon security conference. He called hacking 'a practical application of network insecurity skills … as a means of fighting for social justice by putting direct pressure on politicians and institutions'.

INSIDE JOBS

There's another kind of cyber-attacker: the cyber-insider. Employees who use their privileges to wreak damage on their employers' systems can cost companies millions. In the 2014 US State of Cybercrime Survey, 28% of respondents blamed insiders (including employees, service providers and contractors) for data breaches, while almost a third (32%) said that cyber-crime perpetrated by an insider was more damaging.

Insiders are perhaps easier to profile and predict, because they are already known to an organisation.

'There is a psychological element to it – for example, identifying those individuals who are prone to stress, pressure, radical changes in behaviour or have a personality type that exhibits riskier behaviour,' says NCC Group's Whitehouse. 'However, companies always need to look at this element in the wider context and ensure they don't discriminate.'

How can you defend yourself against an unknown threat? Start by thinking outside the box – because hackers will. In fact, many IT security consulting companies employ 'white hat hackers' for this reason. One such company is Core Security, a security advisory company that runs a research division called CoreLabs.

'It's safe to say that hackers – whether we're talking about white hat or black hat hackers – are usually creative, curious people who like to think outside the box,' says one white hat hacker from CoreLabs, who asked not to be named. However, hackers tend to follow a basic path to get what they want: that of least resistance. 'That understanding can help you predict how you might be attacked,' they concluded.

HOW TO PROTECT YOURSELF

You can only determine the path of least resistance if you understand what a cyber-intruder might be looking for. Harry Sverdlove, CTO of IT security firm [Bit9 + Carbon Black], advises organisations to carry out a risk assessment. Decide which assets are of the highest value, he suggests, then think about who might want to attack them in order to highlight what's most at risk.

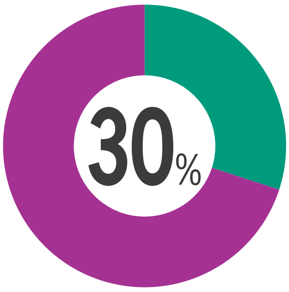
Once you've analysed the risk and worked out what you want to protect the most, it's time to implement that protection. Here, a technique known as defence in depth can be useful. Rather than implementing one means of protection, such as an internet firewall, it makes sense to use many.

Cyber-intruders will try to breach your defences in multiple ways, including everything from sending malware-infected emails through to telephoning employees and trying to fool them into giving away account credentials (a technique known as 'social engineering').

A healthy selection of technical measures can complement other protective steps, such as a mature IT management processes, whereby software is patched with security updates at regular intervals. Cyber-security awareness training for employees is also important to help to thwart potential attackers or employee misadventure.

In the world of cyber-intrusions, there is never such a thing as 100% security. Organisations have to get their protection right every single time, whereas attackers only have to succeed once. Understanding where your risks lie, and allocating the finite resources at your disposal to protect them as best you can, will give you a head start in the game.

CYBER-CRIME IN AUSTRALIA

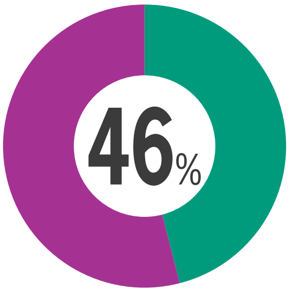


OF RETAIL BUSINESSES CITING CYBER ATTACKS AS A MAJOR THREAT[1]

AVERAGE COST OF A DATA BREACH IN AUSTRALIAN RETAIL

$165

PER RECORD STOLEN/LOST[2]



OF BUSINESSES HAVE A CYBERSECURITY STRATEGY[1]

$81BN USD

VALUE OF APAC CYBERCRIME[1]

SOURCE

[1] GTI IBR 2015 Q2

[2] Ponemon Institute 2015 Cost of Data Breach Study

THE EXPERT'S VIEW

SOME SIMPLE STEPS TO CYBER-SECURITY

MATTHEW GREEN, PARTNER AT GRANT THORNTON, EXPLAINS

The Australian government has classified cyber-security as one of its highest national security priorities, alongside building infrastructure resilience, countering international terrorism and preserving our border integrity.

Data and information risks can take many forms. All electronic information is at risk from attacks by hackers or others seeking to breach security in order to disrupt businesses or commit fraud or through process failure and user error.

It is estimated that 80% of cyber-attacks could be prevented through simple computer network 'hygiene'. So, to begin with, it's important to ensure your business has the basics right around data and information security.

A useful exercise is to identify your key information assets: what is the key information in your business and how are you protecting it; ensure you have someone accountable for information, and have a good governance structure.

Then, rather than asking, 'Can a hacker attack me?' ensure that your data users are aware of procedures to keep data safe, make sure you know where your data is, understand the security of third party providers and how they secure your data, and be aware of where information goes when (and how) it leaves your organisation. Keeping systems up to date through regular and active patch management and user access reviews will keep the basics in check and ensure protection against new vulnerabilities.

In addition, it's important that there is an individual responsible at board level, and that cyber-security is discussed regularly at board meetings.

Finally, having a plan to deal with a security incident or data breach is essential for a managed and controlled response, particularly where it could directly impact your brand and reputation.

All of these measures will help you to create a robust and controlled data security framework from which you can implement monitoring processes and a clear response strategy to any breach.

This article first appeared in Strategies for growth magazine, published by Grant Thornton UK, and edited with localised content for Insights: the Innovation Issue (2016). A Grant Thornton Australia publication for the consumer products and retail industry.