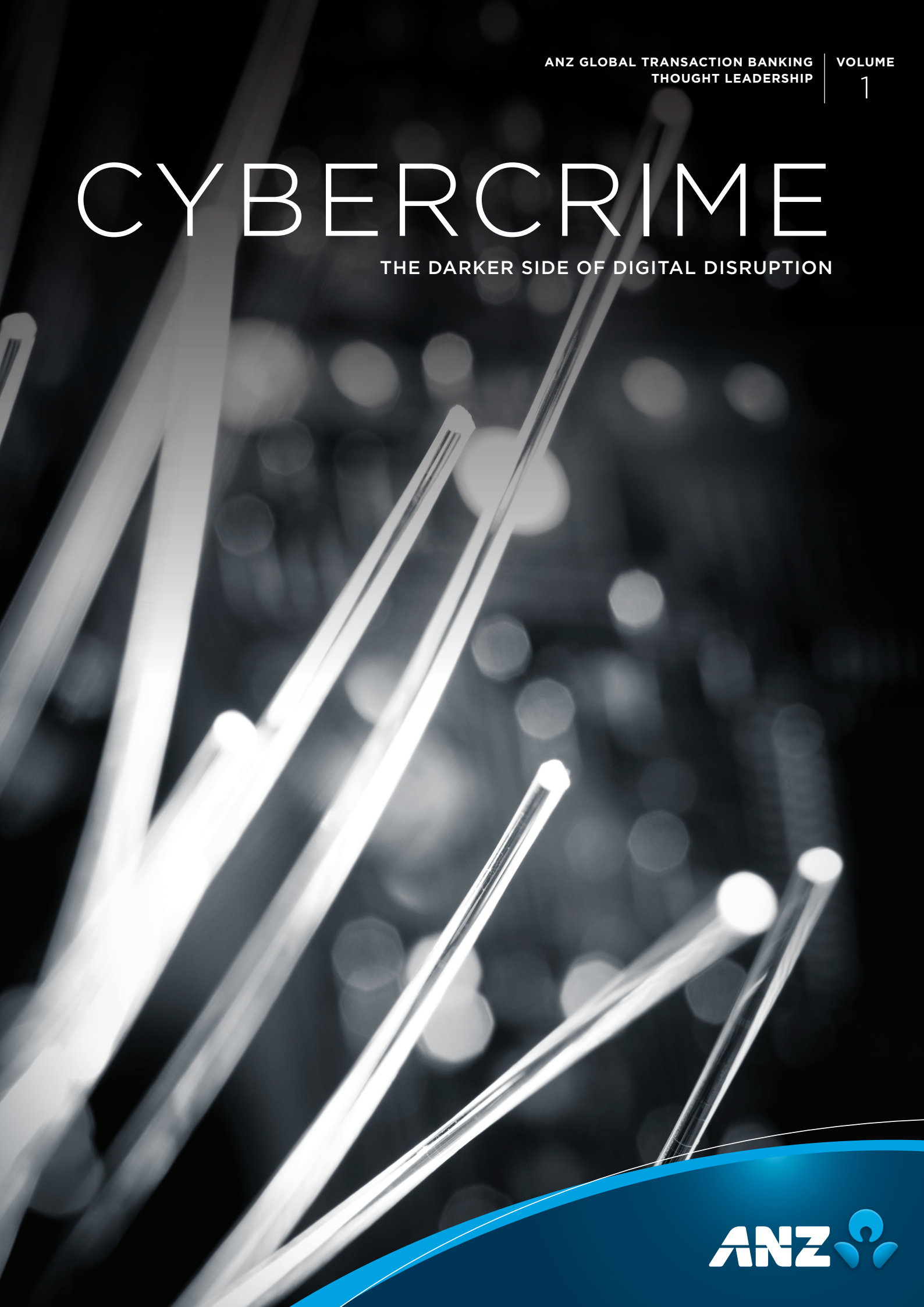
ANZ GLOBAL TRANSACTION BANKING
THOUGHT LEADERSHIP
VOLUME
1

CYBERCRIME

THE DARKER SIDE OF DIGITAL DISRUPTION



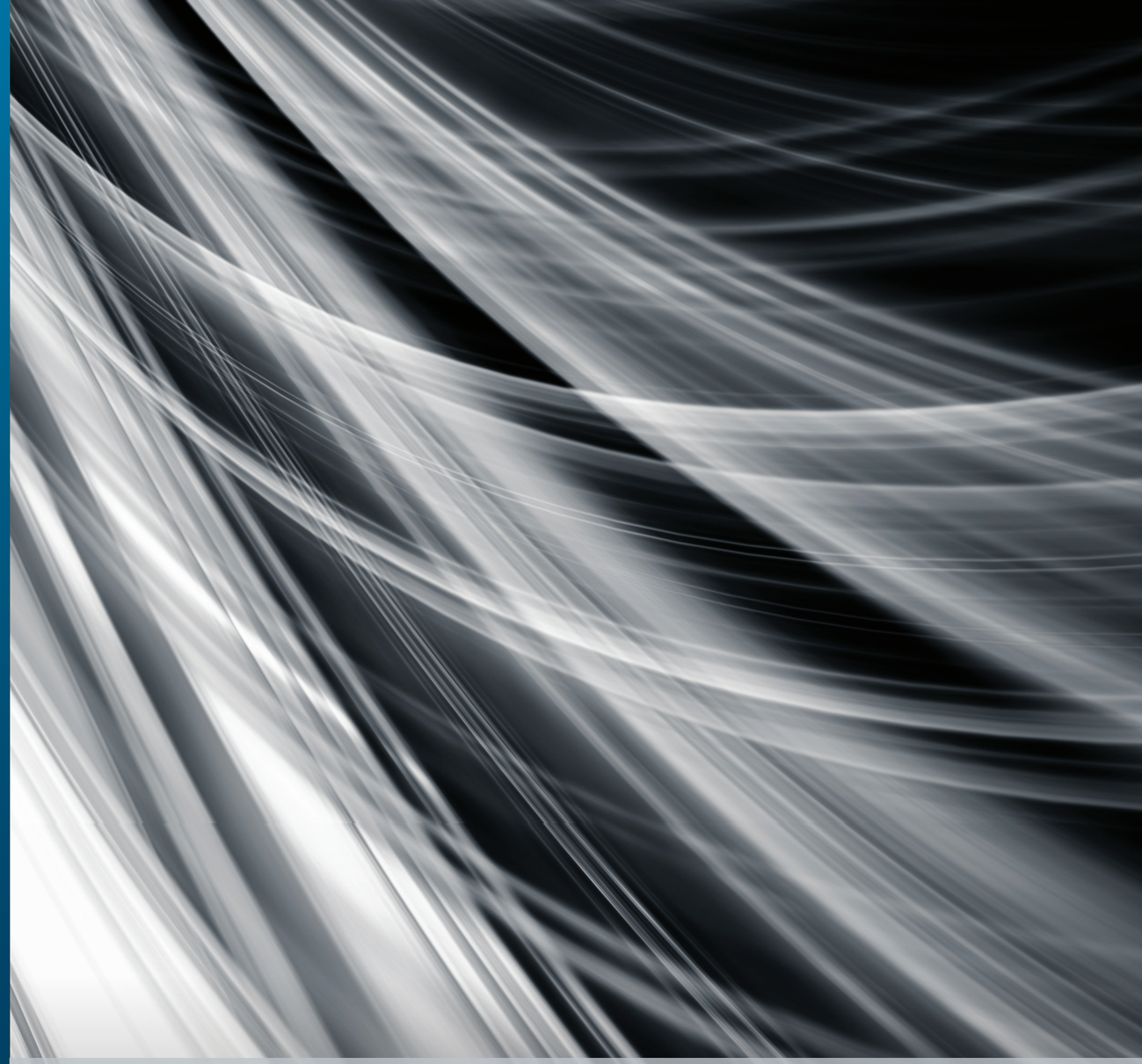
ANZ

A CORPORATE TREASURER'S GUIDE TO PROTECTING THEIR ORGANISATIONS

With business and consumer interactions moving to digital formats, there is a world of opportunities before us. Unfortunately this also brings increased risks and vulnerabilities for organisations regardless of their size, industry or location in the world. Digital development is making it very easy for others to intercept many aspects of people's professional and personal lives. It is no surprise that banks and corporates are ready targets for cybercrime, and we must continue to work together to prevent and mitigate the impacts of cybercrime.

At ANZ, we are committed to preserving the trust that our clients have in the quality and security of our banking services. As a corporate treasurer, we know the essential role you perform in managing risks within your organisational environment.

This guide 'shines a light' on some practical recommendations for keeping your organisation safe and secure, and together with the robust security practices we implement to help protect our clients, aims to minimise the chance of your organisation falling victim to cybercrime.



AT A GLANCE

- Cyber criminals exploit any weakness in an organisation's people, process or technology infrastructure
- Using humans to infiltrate organisations is a common factor in most current cybercrime attacks
- Effective processes together with a risk management approach are crucial
- Organisations benefit from a multi-layered risk management strategy – 'defence in depth'
- The agility to know, control and adapt to new cyber threats will differentiate the strong from the weak
- Cyber resilience plans are essential – expect cyber disruption and prepare to deal with it while continuing to operate your business
- ANZ works with our clients to help keep them safe

CYBERCRIME INNOVATION

Cyber attacks on large organisations are growing at a phenomenal rate. IBM recently sampled 1,000 clients in 133 countries and found that the average organisation surveyed now experiences nearly 17,000 security attacks each year[1]. It is estimated that failure to defend against cyber attacks could have an aggregate impact on the global economy of US$3 trillion by 2020[2].

Cyber criminals are increasingly sophisticated in their execution and can be equally opportunistic in who they target – from individuals through to large multi-national corporations, no one is immune from being attacked. This sophistication reflects the innovative methods used and speed of the execution. Cyber criminals innovate, make decisions and execute faster than many organisations are equipped to deal with. Moreover, cybercrime is now a business in every respect, with services that mirror those of multi-national organisations including customer support and technical helplines to ensure their criminal products and services work as intended.

As a custodian of financial stability, you must understand this changing landscape and adapt to protect your business.

Any modern corporate treasury function is comprised of three main elements – people, process and technology. Cyber criminals look for and exploit any weakness in one or more of these elements to infiltrate the business to gain access to either information or syphon money, often millions of dollars at a time, into their international network.

CYBER CRIMINALS INNOVATE, MAKE DECISIONS AND EXECUTE FASTER THAN MANY ORGANISATIONS ARE EQUIPPED TO DEAL WITH.

CYBERCRIME IN ACTION

In a recent cyber attack, a large US-based technology company fell for a simple scam whereby the criminal sent an email to their treasury department instructing a payment. To add legitimacy, the criminal used the identity of a senior executive as the author. This resulted in nearly $47 million being sent from the corporate bank account in Hong Kong to the cyber criminals in Asia. To date only a fraction of that money has been recovered[3].

Another recent breed of malware, Dyre Wolf, has also been used to target large organisations. Based on multi-layered social engineering tactics that circumvent two-factor authentication, it begins with a mass email which, when opened, triggers its download. The employee (victim) logs into online banking, Dyre Wolf alters the response from the website and tricks them into calling an illegitimate number. If he or she then reveals online banking credentials, the attacker transfers monies into several offshore accounts and delivers a high volume denial of service attack to distract or hinder investigation. In recent incidents, organisations have lost up to $1.5m[4].

[1] http://www.slideshare.net/ibmsecurity/2014-cyber-security-intelligence-index
[2] http://www.cso.com.au/article/548110/cyber_threats_makes_it_number_4_global_wef_agenda/
[3] http://www.thecorporatetreasurer.com/News/401030,the-47-million-scam-next-time-it-could-be-you.aspx?eid=33&edate=20150820&utm_source=20150820&utm_medium=newsletter&utm_campaign=alert_newsletter
[4] https://securityintelligence.com/dyre-wolf/

17,000

Security attacks the average company experiences each year[1]

$3 USD TRILLION

Impact on the Global economy by 2020[2]

HOW DO THESE ATTACKS TAKE PLACE?

Methods used by cyber criminals are constantly evolving. They are too varied and numerous to list here. However, here are some of the most common methods.

Social engineering

Social engineering involves targeting an individual to facilitate the fraudulent transaction or data breach. In fact a recent IBM study reported that 95% of all security incidents involve some degree of human involvement[5]. Cyber criminals are often experts in human psychology and social engineering. They will send a bogus 'last minute crucial payment instruction' email at 5pm on a Friday just as people are going home in the hope that shortcuts will be taken to get the job done. Under the disguise of suppliers or colleagues, cyber criminals will send emails with links to fake e-Christmas or e-birthday cards in the hope that it will install malware on computers and retrieve banking credentials.

Currently, we are seeing social engineering as a prerequisite in the cyber criminals' success. People must be empowered and knowledgeable to spot and challenge the unusual, and then follow clearly defined response protocols. Continuous education and awareness are crucial[6].

Malicious software

Malicious software or 'malware' involves tricking individuals into opening infected files so that the cyber criminal can either introduce spyware, ransomware, viruses, trojans or any type of malware that would allow them to gain access to data, devices or systems.

Some of this activity is highly targeted phishing (or spear phishing). Phishing is when a malicious link to an authentic looking website is delivered via email, tricking the recipient to enter their security credentials or download malware. Spear phishing is more sophisticated by targeting a specific organisation or individual and appearing to come from a trusted source.

Phishing attacks leverage information gained from social media or other publicly available information, such as annual reports or company registers, to create legitimate looking emails to be sent to specific individuals, often purporting to come from friends or colleagues. Spear phishing can trick even the savviest of users, and as we have seen in previous examples, often has significant consequences.

Cyber criminals can go to extraordinary lengths to infect target computers. Legitimate websites can be compromised to host malware that then infect user devices. Fake surveys, free gift offers, 'must see' videos are just some of the ways criminals attempt to lure their unsuspecting victims.

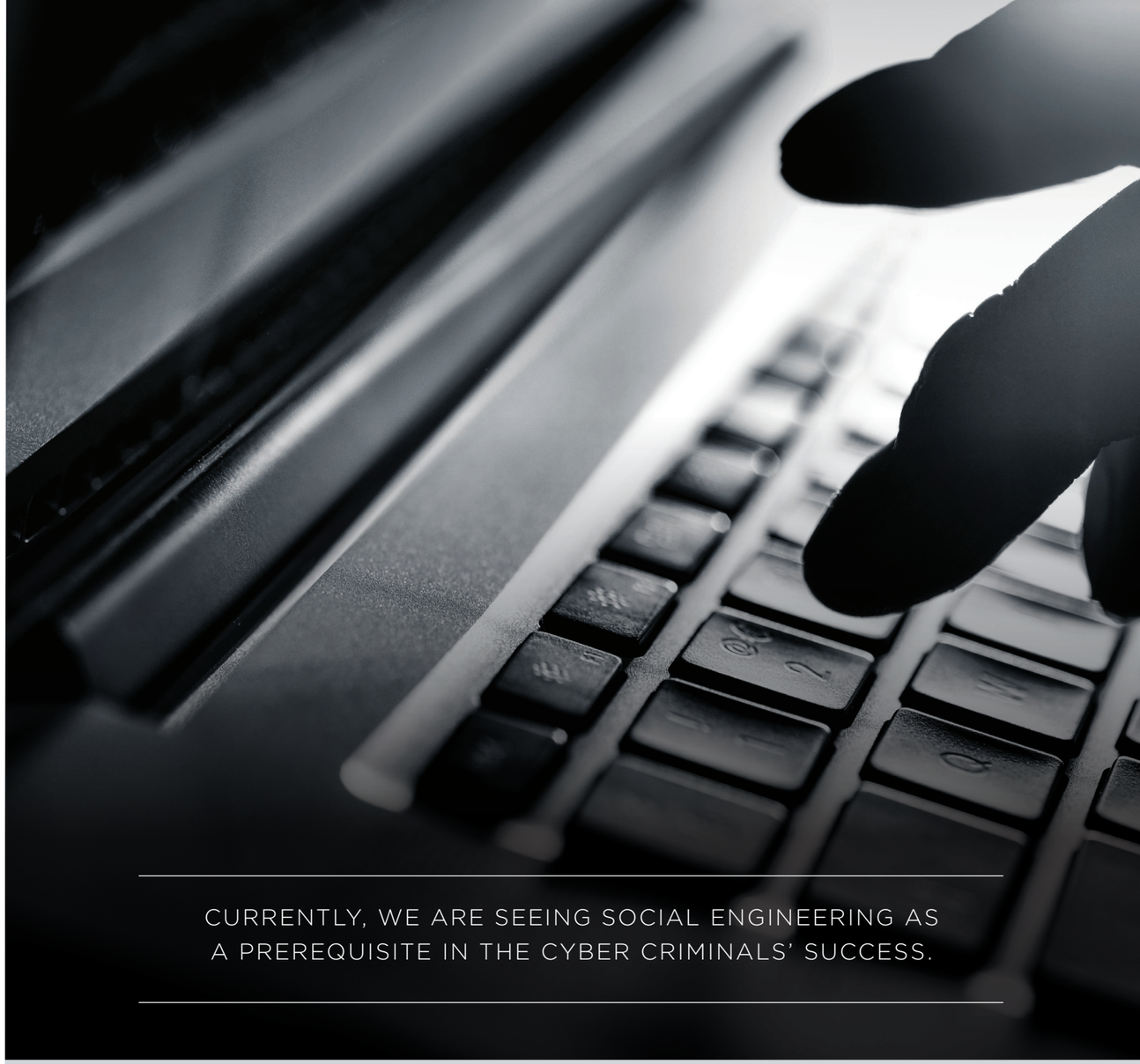
A new technique called a 'watering hole' attack, works by criminals understanding local websites that are often visited by employees of a particular company. This can be anything from the local gym to the local newspaper. That website is compromised with malware, knowing that the malware will affect a particular geographical area, company or set of companies.

Existing system vulnerabilities

Cyber criminals often rely on known, but unpatched exploits, to gain access to IT systems to commit their crimes. Unchanged default root passwords are easy pathways into corporate IT systems. Cyber criminals know that large organisations are slow to react to patch upgrades. A patch release often describes the vulnerability that is being resolved in detail. If a cyber criminal failed in a past attack, but in their efforts, gathered information about a company's infrastructure, now knowing exactly how that infrastructure is vulnerable enables them to succeed in any future attempt until the patch is applied.

Organisations battling these threats must ensure that they have a robust approach to tackle them.

[5] http://www.slideshare.net/ibmsecurity/2014-cyber-security-intelligence-index
[6] https://www.fbi.gov/news/stories/2014/april/understanding-school-impersonation-fraud/understanding-school-impersonation-fraud



CURRENTLY, WE ARE SEEING SOCIAL ENGINEERING AS A PREREQUISITE IN THE CYBER CRIMINALS' SUCCESS.

CYBERCRIME IN ACTION

In 2014, the FBI uncovered a social engineering fraud where criminals posed as a school purchasing officer when contacting suppliers. They acquired information about the school's account and used that information to place bogus orders of laptops, hard drives, printer ink and other items. The school was billed and the goods shipped. Criminals then contacted the school to say the shipment was sent in error. The school, believing it is returning the order, reshipped the items to a domestic address provided by the fraudster[6].

KNOW, CONTROL AND ADAPT

Those who perpetrate these cyber attacks have a vested interest in ensuring their methods are innovative and covert. However, while cybercrime seems a new threat, a risk based approach allows focus on what is important.

Understand your processes and your risks

Knowing your organisational processes is crucial to understanding the cyber security risks they present. With this in mind, reviewing the maturity of your transactional processes is the first and most fundamental step in protecting against cybercrime. This includes the identification of gaps or weaknesses in process or controls, such as user access management and payment authorisation, which present a risk.

Risk professionals can help in defining the risks associated with those processes, the people who execute those processes and the technology that enables them. After they have identified the risks that pose the highest threat to your business objectives, clear plans must be set in place to mitigate them. Organisations can reduce the likelihood and impact of risks by implementing effective controls.

Monitor threats

Controls are all those activities that detect or prevent undesirable events. Controls, much like processes, must be actively reviewed to make sure they are designed and operated in a way that reduces risk.

Remember all controls are not equal: they reduce in effectiveness over time. Process or technology change and time allows cyber criminals to adapt and change their tactics. This is where the controls to respond and recover from cyber incidents (as part of a cyber resilience plan) become even more imperative.

In the cyber security world we can also learn from other security principles such as 'defence in depth', making sure that we do not depend on a single control; and taking an end-to-end view that acknowledges how threats can enter at any point in our processes.

There are many different layers of people and process controls, from company level leadership to employee activities, behaviours, and culture. A robust, well documented and actively managed control environment is crucial. Any system is only as strong as its weakest link.

Monitor and adapt

During the ongoing governance of your organisation's process and controls, one core factor to take into account is the agility to change. As mentioned previously, cyber criminals are innovative and constantly change their approach, behaviour and tools to create new ways of stealing assets. Vigilance is key. The time to act is now.

Organisations must monitor security news, identify new best practices and source intelligence about the methods and tools used by cyber criminals. The flexibility to react to an ever-changing environment will differentiate the strong from the weak.

Governments are certainly taking the threat seriously. In 2013, the UK's National Cybercrime Unit became operational[7] and in 2014, The Australian Government opened the Australian Cyber Security Centre to co-locate cybercrime intelligence units[8].

Certain industries have already begun to create intelligence sharing groups, some of which have government representation. It is expected that this trend will continue to expand as more and more companies, industries and governments realise that cyber threats are here to stay.

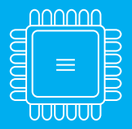
[7] http://www.computerweekly.com/news/2240206747/UK-National-Cyber-Crime-Unit-becomes-operational
[8] http://www.abc.net.au/news/2015-04-23/cyber-attacks-on-australian-businesses-rise-20-per-cent/6415026

A ROBUST, WELL DOCUMENTED AND ACTIVELY MANAGED CONTROL ENVIRONMENT IS CRUCIAL. ANY SYSTEM IS ONLY AS STRONG AS ITS WEAKEST LINK.

KEY CONTROL CONSIDERATIONS FOR TREASURERS

PEOPLE

Staff education: Invest in staff awareness on cyber risks and in particular new social engineering and phishing techniques. Your staff are the first and last line of defence against cyber attacks.



TECHNOLOGY

Network/ IT security controls: Consider robust logical access controls, new system strengthening, network and endpoint firewalls, up to date malware and anti-virus protection, intrusion detection systems, regular patching, vulnerability scans and penetration tests.

PROCESS

Governance and monitoring: Place cyber security on the agenda of senior executive and management meetings to ensure risks are regularly reviewed and appropriate proactive and reactive measurers are in place.

Insist on a robust security policy: Maintain clear protocols on segregation of duties, and controls for the use of all technology including mobile/portable devices. It should also explicitly define employee security screening processes, acceptable use of IT assets and staff training.

User access management: Ensure that only staff with the right responsibilities and security credentials has access to your systems and financial data, including two factor authentication for transaction signing/payment approvals. Regularly monitor and update user access privileges, and check that staff are protecting and not sharing their security credentials. Removing access when no longer required is equally important, including when staff move to new roles within the organisation.

Define a coordinated response to security events: expect a cyber incident, plan for and practice your response and resolution to minimise the impact of a loss.

Control payment authorisations: Consider strict procedures over all changes to customer/supplier bank details, key contacts and all other master data including identity verification and change accuracy controls.

Reconcile and review: Ensure reconciliations do not just serve as a rubber stamp activity but detect and escalate a leakage in funds whether small or big as a once off or over a period of time.

EVADING CYBERCRIME WITH ANZ

A corporate treasurer's world is one occupied by a broad range of financial management activities – we get that. We also understand that financial transactions are only as secure as the link between your organisation, your business partners and your bank.

Our digital security encompasses hardware and software, as well as best practice business process, experienced people and technology controls. Interfaces between both ANZ and clients, and ANZ and other financial institutions use the latest encryption and network security infrastructure.

Working together with ANZ, you get peace of mind from knowing that we are securing important links in the financial supply chain.

Australia and New Zealand Banking Group Limited (ANZ) ABN 11 005 357 522. ANZ's colour blue is a trademark of ANZ. 12/15 30143

This document is distributed by Australia and New Zealand Banking Group Limited ABN 11 005 357 522 ("ANZBGL"). The information contained in this document does not constitute advice and does not take into account your personal needs and financial circumstances. You should seek independent financial, legal, tax and other relevant advice and should independently verify the accuracy of the information contained in this document. This document may not be reproduced, distributed or published by any recipient for any purpose.