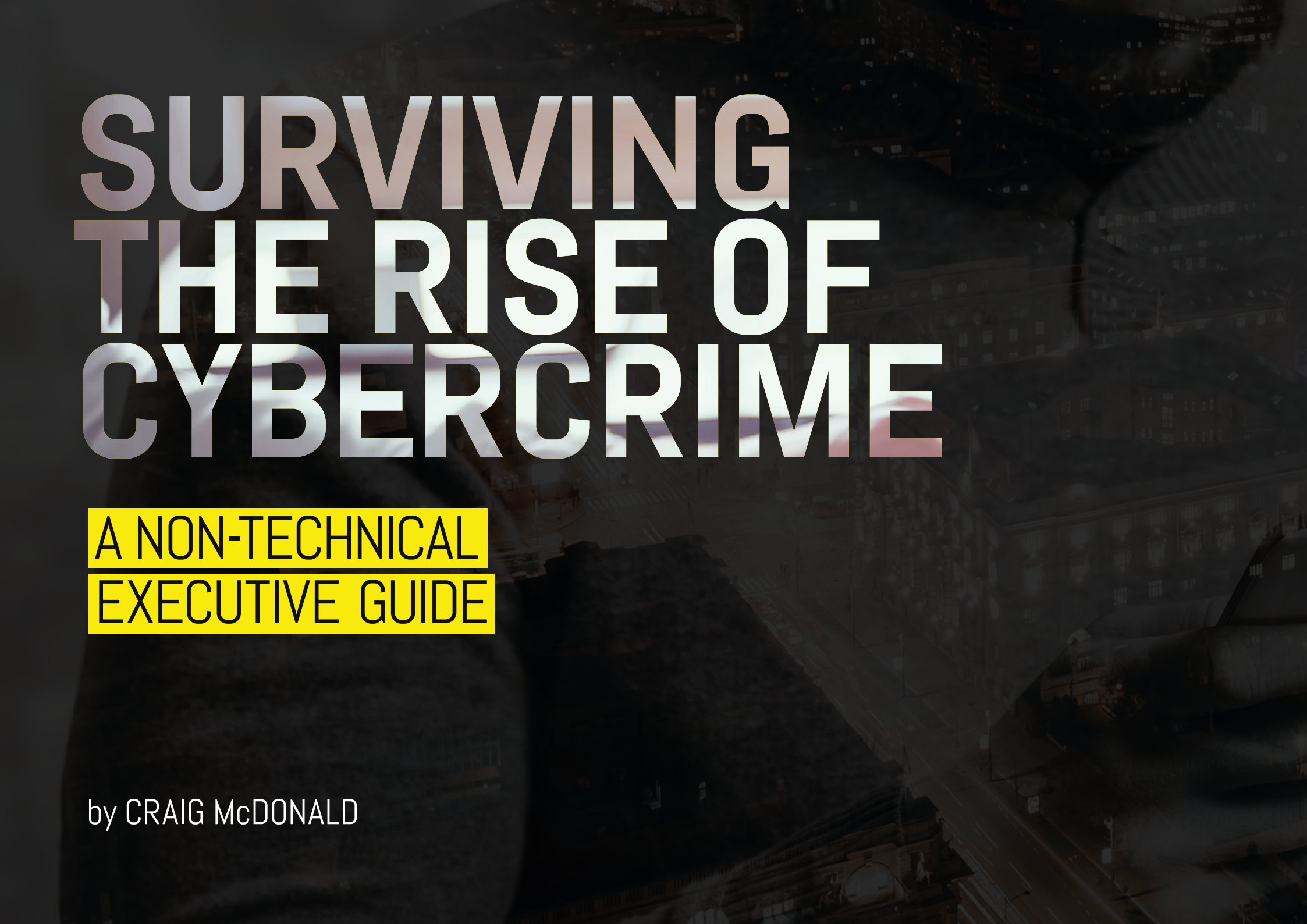


SURVIVING THE RISE OF CYBERCRIME

A NON-TECHNICAL EXECUTIVE GUIDE

by CRAIG McDONALD

YOUR KEY TAKEAWAYS

This guide aims to provide a non-technical insight into cybersecurity for time-poor executives who are new to the threats emerging in this space.

In less than 60 minutes, I aim to provide you with an understanding of cybersecurity and what it means for your organisation, to highlight some real-world examples, and to make you familiar with some industry jargon and terminology.

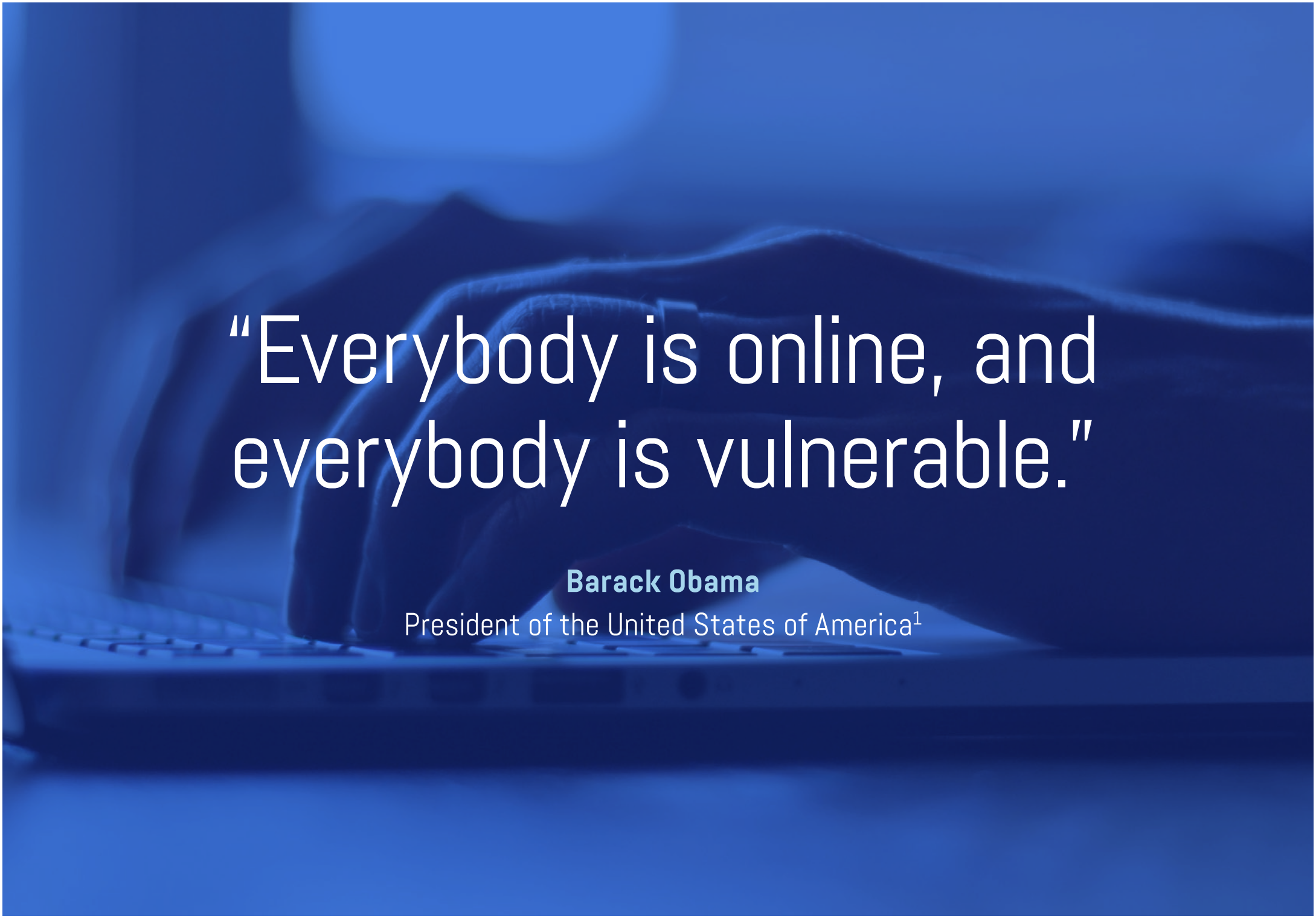
I'm Craig McDonald, CEO & Founder of MailGuard.

A cloud-based email and web security business since 2001, MailGuard was recently commended as a "world-leading" innovator by the Australian Prime Minister, The Hon. Malcolm Turnbull MP.

- Identifying the threats to your business
- Finding out why cybercriminals are targeting your business and staff
- Understanding why your IT team is struggling to prevent these threats
- Knowing your role and responsibilities as a C-level executive or business leader, and
- How to educate and empower your managers and teams as the frontline in your cyber-defence.

"[MailGuard is] among the leading cloud and email security solutions anywhere in the world."

The Hon Malcolm Turnbull MP,
Prime Minister of Australia


“Everybody is online, and everybody is vulnerable.”
Barack Obama
President of the United States of America[1]

WHY WRITE ANOTHER GUIDE ON CYBERSECURITY?

Every day I meet with successful C-level business leaders who are charged with the responsibility of steering their organisations to success. To many, the sphere of cybersecurity is relatively new and unfamiliar.

There is a plethora of extensive texts and guides that have been commissioned by experts in the cybersecurity space, however despite their thoroughness, in my experience they are rarely read. They are simply too detailed, and too technical, and as a result they often ask too much of their audience.

In cybersecurity, the human factor is the greatest vulnerability for any organisation, and a large part of the challenge is generating awareness and educating those who are in harm's way. This is particularly the case with C-level executives who are time-poor and often feel that there's too much to consider. **Some executives take the view that it's somebody else's problem – most commonly a member of their IT team. In today's climate such attitudes are outdated and plain dangerous.**

I am not alone in calling for business leaders to be more proactive tackling the rise of cybercrime. Inside this guide is a collection of thoughts, opinions and quotes from some of our most informed and respected leaders, including Australia's Prime Minister, The Hon. Malcolm Turnbull MP, Barack Obama, President of the United States, Robert S. Mueller III, Director of the FBI, and business visionaries including Bill Gates, Elon Musk and Jeff Bezos.


“Cybersecurity is a leadership issue, not an IT issue"
Craig McDonald
Founder & CEO, MailGuard²

ABOUT THE AUTHOR

CRAIG MCDONALD

CEO & FOUNDER MAILGUARD

Over 15 years ago, an email-borne virus caused havoc for one of my businesses. I was astounded that something as simple as an email could have such a devastating effect, especially when that business was protected by all the latest antivirus software.

As a non-technical business professional I struggled to reconcile the fact that my business had for years been paying for a service that didn't do what it said on the box.

Those events in 2001 inspired me to start MailGuard, and I have made it my mission ever since to provide a service that delivers on its promise.

Not only a businessman and entrepreneur, I am also a family man, a husband and a father. I am dedicated to protecting the state of the nation we live in, and the state of the global digital economy, so that my children grow up in a digital age that is safe and secure.

An Australian company, MailGuard has grown to become the world's largest private email Software as a Service [SaaS] security provider, and now delivers business email and web security worldwide.

MailGuard applies immediate protection to thousands of businesses, stopping fast-breaking, zero-day email threats 2-48 hours ahead of the market. With advanced AI (artificial intelligence) threat-detection engines, MailGuard is uniquely positioned to predict and stop emerging threats before they reach your network.

Today, MailGuard has partnerships with some of the world's largest email hosting providers, and works collaboratively alongside industry leaders including Microsoft, KPMG, Deakin University and Xero. MailGuard is a member of the Centre for Cyber Security Research (CCSR) and is CSA STAR accredited. MailGuard was recognised by ANZIA, at the Australia & New Zealand Internet Awards, as the 2016 Security Award winner.

CONTENTS

01 LEARNING THE HARD LESSONS FROM OTHERS

Let's start by taking a look at some high-profile breaches


"Your brand is what other people say about you when you're not in the room"
Jeff Bezos
CEO & Founder Amazon[19]

01
LEARNING THE HARD LESSONS FROM OTHERS

Let's start by taking a look at some high-profile breaches

Yahoo!

In late 2014, Yahoo! suffered one of the world's largest breaches of public information.

It wasn't until two years later, **in September 2016, that Yahoo! revealed user information – including names, email addresses, phone numbers, dates of birth, passwords and even the answers to encrypted security questions – had been stolen from at least 500 million accounts.**

The resultant damage could be far more than just reputational. Just months before the breach was revealed, Verizon had reportedly agreed to pay $4.83 billion for Yahoo's core business.

As part of the negotiations, Yahoo! made a regulatory filing with the US Securities and Exchange Commission which reportedly stated it did not have knowledge of "any incidents of, or third-party claims alleging ... unauthorised access" of personal data of its customers that could have a material adverse effect on Verizon's acquisition.[56]

But Verizon said in October it had "reasonable basis" to believe Yahoo's massive data breach of email accounts represented a material impact that could allow Verizon to withdraw from the deal to buy the technology company.

As of December 2016, the deal was still in negotiation.

"The individuals who planned the attempted Times Square bombing in May 2010 used public web cameras for reconnaissance. They used file-sharing sites to share sensitive operational details. They deployed remote conferencing software to communicate. They used a proxy server to avoid being tracked by an IP address. And they claimed responsibility for the attempted attack – on YouTube.

To date, terrorists have not used the internet to launch a full-scale cyber attack. But we cannot underestimate their intent. In one hacker recruiting video, a terrorist proclaims that cyber warfare will be the warfare of the future."

Robert S. Mueller, III

Director, Federal Bureau of Investigation (FBI)[20]

01
LEARNING THE HARD LESSONS FROM OTHERS

Let's start by taking a look at some high-profile breaches

eBay

In May 2014, cybercriminals obtained the log-in credentials of three eBay corporate employees.

The credentials gave cybercriminals access to the personal data of 145 million eBay customers.

The crime was so sophisticated that eBay Global Marketplaces Chief, David Weng, said at the time: "For a very long time we did not believe that there was any eBay customer data compromised."[57]

Subsequent investigations confirmed the extent of the breach.

The credentials gave cybercriminals access to the personal data of 145 million eBay customers.

"Our connectivity brings extraordinary benefits to our daily lives, but it also brings risks. And when companies get hacked, Americans' personal information, including their financial information, gets stolen. Identity theft can ruin your credit rating and turn your life upside-down. In recent breaches, more than 100 million Americans had their personal data compromised, including, in some cases, credit card information. We want our children to go online and explore the world, but we also want them to be safe and not have their privacy violated.

So **this is a direct threat to the economic security of American families, not just the economy overall, and to the wellbeing of our children, which means we've got to put in place mechanisms to protect them."**

Barack Obama

President of the United States of America[21]

Target

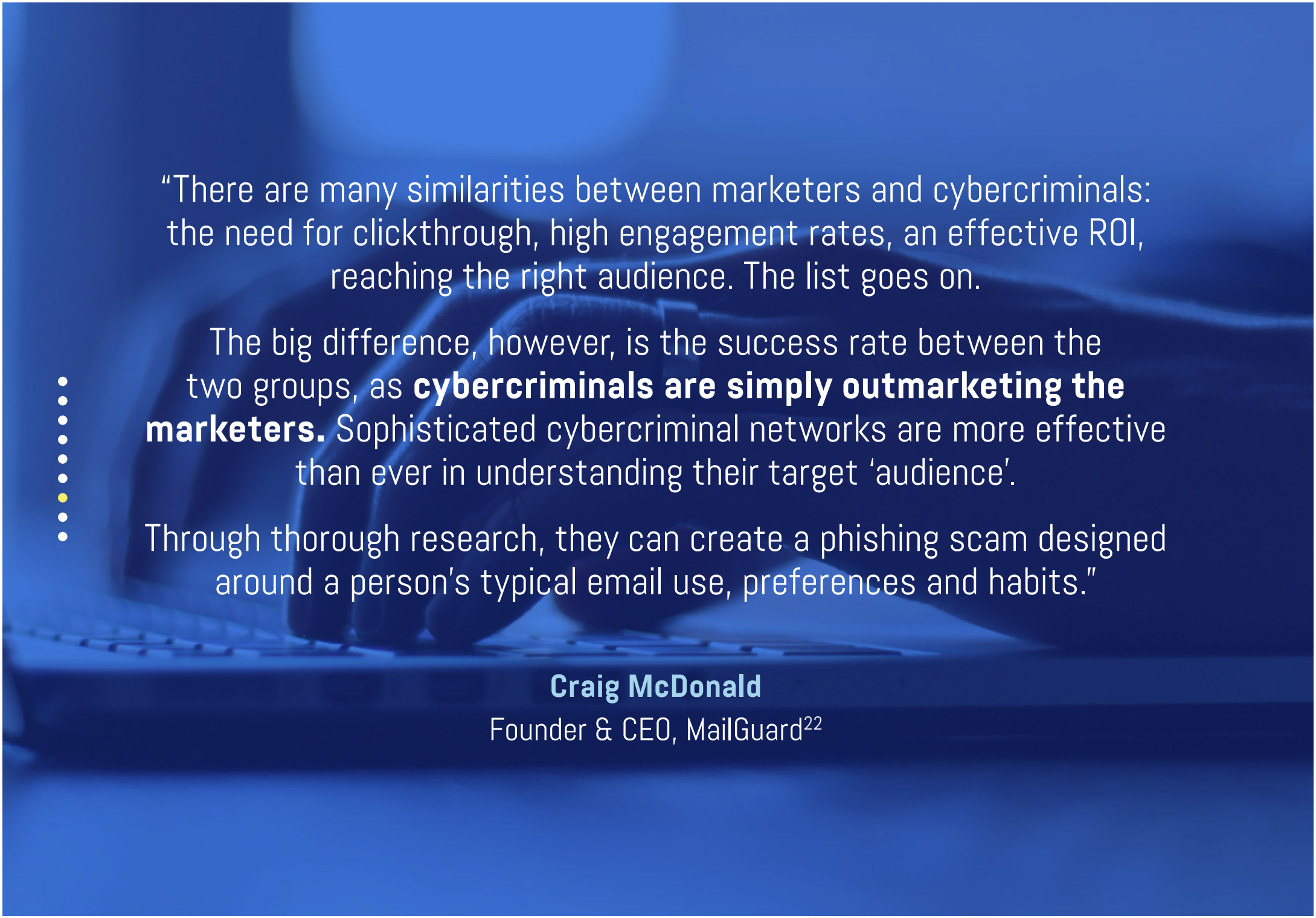
In 2013, attackers lifted an estimated 40 million credit and debit cards from the retail mega-chain's point of sale systems in the United States. The breach has been attributed to an unwary business partner.

Investigators suspect attackers gained access to Target's network credentials from an air-conditioning and ventilation subcontractor who fell prey to a phishing email containing the Citadel Trojan.

The attack hit the headlines, followed by a Congressional Enquiry, executive firings, and a lawsuit against the board of directors.[58]

Investigators suspect attackers gained access to Target's network credentials from an air-conditioning and ventilation subcontractor who fell prey to a phishing* email containing the Citadel Trojan.

*See dictionary defintion on page 124



"There are many similarities between marketers and cybercriminals: the need for clickthrough, high engagement rates, an effective ROI, reaching the right audience. The list goes on.

The big difference, however, is the success rate between the two groups, as **cybercriminals are simply outmarketing the marketers.** Sophisticated cybercriminal networks are more effective than ever in understanding their target 'audience'.

Through thorough research, they can create a phishing scam designed around a person's typical email use, preferences and habits."

Craig McDonald

Founder & CEO, MailGuard[22]

01
LEARNING THE HARD LESSONS FROM OTHERS

Let's start by taking a look at some high-profile breaches

Ubiquiti

In June 2015, Ubiquiti Networks, a Silicon Valley computer networking company, was scammed of nearly $47 million by cyber thieves.

The company fell prey to a “CEO fraud” email phishing scam.

In a statement, Ubiquiti cited that it was “the victim of ‘criminal fraud’ involving "employee impersonation and fraudulent requests from an outside entity targeting the company's finance department".

The scam led to the transfer of $46.7 million held by a Ubiquiti subsidiary incorporated in Hong Kong to other overseas accounts held by third parties, the company said.[59]

The company fell prey to a “CEO fraud” email phishing scam.

"American companies are being targeted, their trade secrets stolen, intellectual property ripped off. The North Korean cyber attack on Sony Pictures destroyed data and disabled thousands of computers, and exposed the personal information of Sony employees.

And these attacks are hurting American companies and costing American jobs. So this is also a threat to America's economic security."

Barack Obama

President of the United States of America[23]

02 THERE'S NO STOPPING PROGRESS

The speed of change


"It is the most important piece of infrastructure ever created by mankind and yet it has not been created, as most infrastructure is, by governments.
A free and open internet supports our democratic rights of freedom – of speech, religious expression, political thought and choice."
The Hon. Malcolm Turnbull MP
Prime Minister of Australia[3]

02
THERE'S NO STOPPING PROGRESS

The speed of change

As leaders, the enormous challenge we face is anticipating what the future will bring.

Which trends will take hold?

Which technologies will transform the way we live, and the way we do business?

02
THERE'S NO STOPPING PROGRESS

The speed of change

Many who have harnessed the possibilities of the internet have ridden the wave to commercial success.

We've seen the newspaper, publishing, music, movie and advertising industries be swept aside by the internet.[53] Fortunes, careers, and industries have been lost as outdated business models have failed.

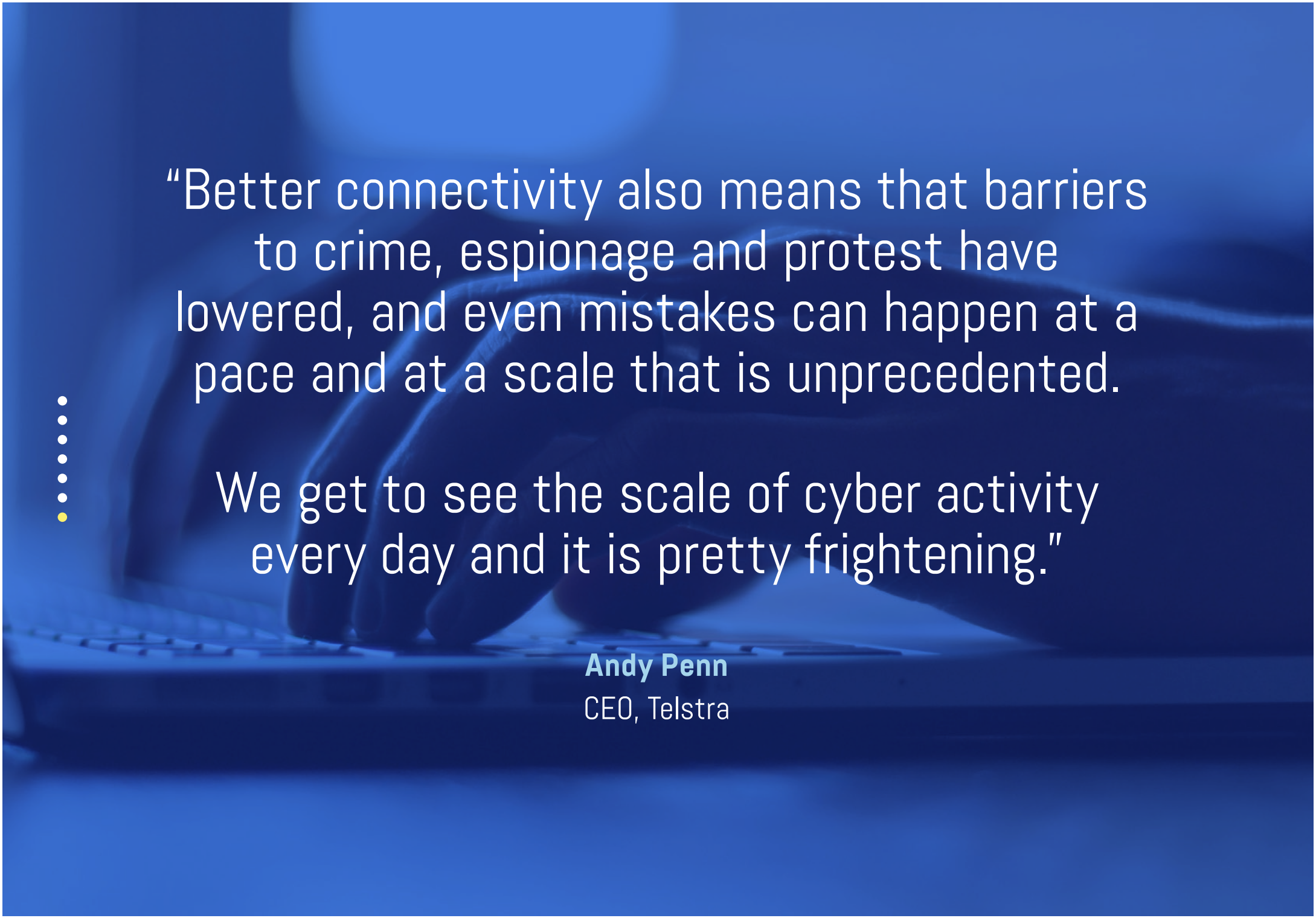

"...we have to preserve one of the greatest engines for creativity and innovation in human history."
Barack Obama
President of the United States of America[7]

Are you, your business, and your leadership team ready for what the future holds?

As technology evolves, global commerce is accelerating in the digital realm.

A new way of doing business is now upon us. All successful businesses innovate. The task now is to do so faster than ever before.


"We are working to keep the net safe for our citizens and their businesses, to protect the infrastructure on which we all rely and to elevate the safe use of cyberspace in our trading partners.
This digital century is a time of remarkable opportunity.
Our response to those opportunities and to the threat of people using it criminally and maliciously will come to define the future of our societies."
The Hon. Malcolm Turnbull MP
Prime Minister of Australia[6]


"Better connectivity also means that barriers to crime, espionage and protest have lowered, and even mistakes can happen at a pace and at a scale that is unprecedented.
We get to see the scale of cyber activity every day and it is pretty frightening."
Andy Penn
CEO, Telstra

03

AN EXPLOSION OF EASY-ACCESS DATA

The new norm in the digital economy

03
AN EXPLOSION OF EASY-ACCESS DATA

The new norm in the digital economy

As technical innovation and global commerce accelerate, an explosion of data is occurring. This 'virtual Big Bang' manifests as a proliferation of detailed personal and business information in the cyber sphere.

03
AN EXPLOSION OF EASY-ACCESS DATA

The new norm in the digital economy

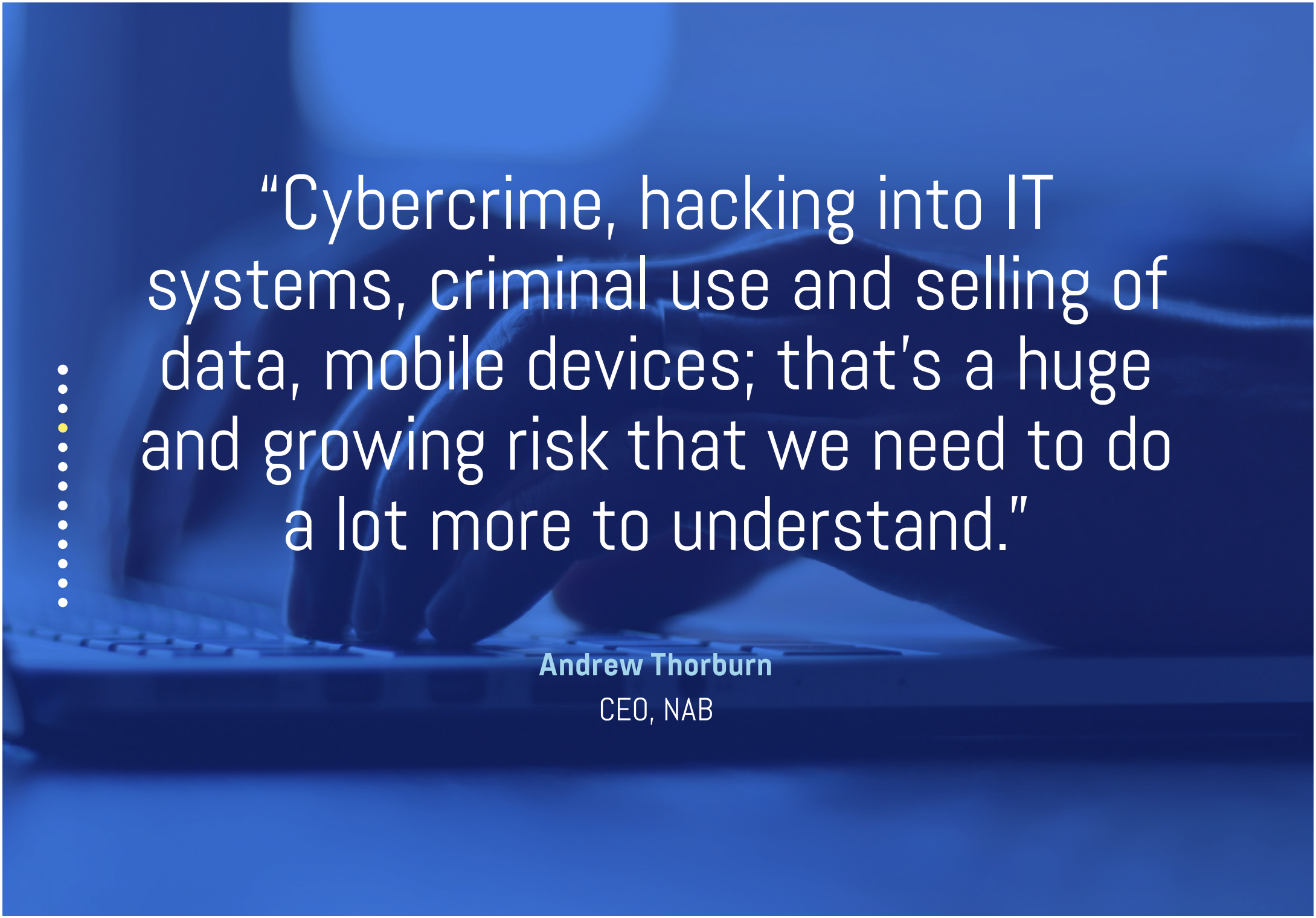
The statistics are mind-boggling. More than 205 billion emails are sent and received throughout the world every single day, according to market researchers Radicati.[40]

That's more than 1 trillion email messages each week – and growing.

03
AN EXPLOSION OF EASY-ACCESS DATA

The new norm in the digital economy

Combine those messages with the global explosion in social media engagement: there are now 2.307 billion[41] active social media users around the world, among 3.631 billion internet users globally, according to Internet World Stats.


“Cybercrime, hacking into IT systems, criminal use and selling of data, mobile devices; that’s a huge and growing risk that we need to do a lot more to understand.”
Andrew Thorburn
CEO, NAB

03
AN EXPLOSION OF EASY-ACCESS DATA

The new norm in the digital economy

Consider the volume of data across email, search engines and social networks every minute. By the end of 2016, the volume of global IP data transferred is forecast to exceed 1.1 zettabytes (ZB)*.[42]

The global availability of masses of easily-accessible data, combined with the cultural norm of sharing personal information online, creates a potential hotbed for cybercrime.

*A zettabyte is roughly 1000 exabytes. According to Cisco, an exabyte is equal to about one billion gigabytes and has the capacity to hold over 36,000 years worth of HD-quality video, or stream the entire Netflix catalogue more than 3,000 times.

03
AN EXPLOSION OF EASY-ACCESS DATA

The new norm in the digital economy

It's alarmingly simple for cybercriminals to engage in identity fraud using your data. In just minutes, with little investment, cybercriminals can design a campaign to scam those close to you, by adopting your identity. Generally speaking, this is referred to as 'social engineering.'

'Social engineering' is the foundation for many forms of attack, including phishing and ransomware scams, but the most dangerous may be highly-targeted spear-phishing attacks.

The attacks can take many names, from CEO fraud, to whaling and Business Email Compromise. Whichever name you choose, spear-phishing attacks impersonating influential executives continue to be a big problem for businesses of all sizes.

03
AN EXPLOSION OF EASY-ACCESS DATA

The new norm in the digital economy

It happens this simply. Before an email is sent, the cybercrime network behind the attack conducts thorough reconnaissance to research the targeted organisation and the individual executives involved.

Often much of the information that attackers require is easily available from company websites and social networks such as LinkedIn.

Scammers can ascertain the contact details, location and role titles of executives and employees, as well as researching the victim's colleagues within the target organisation. Depending on the profile of the executives involved, together with their social media activity, it may be possible to determine if they will be offsite at business roundtables, conferences or other speaking engagements.

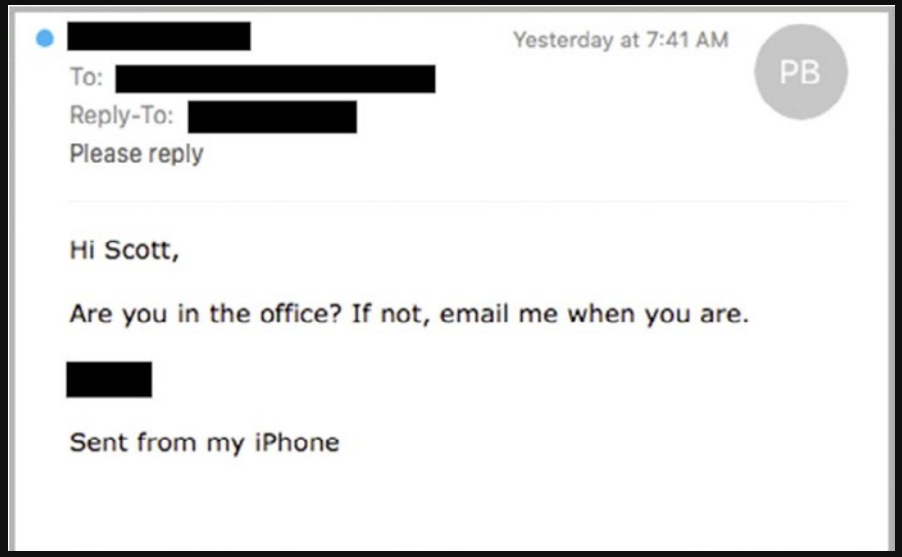

“Every minute matters”
Craig McDonald
Founder & CEO, MailGuard10

Here is a real-life example targeting the managing director of an ASX-listed mining and resources company.

It's a very casual, simple first approach, attempting to determine if the individual required to make a cash transfer is at his desk.

It's from the iPhone of the managing director, thereby avoiding the need to mimic an email signature, and is likely to capture the target's attention.

It is also early in the morning – 7.40am – so there's a good chance there aren't many people around to verify if the request is legitimate.



Here's another example. This time it purports to be from the CEO of a large financial services business.

It's shortly before lunch, and the sender makes it quite clear that he is seeking to converse over email only. Nonetheless, it is quite casual and personal in nature.

How would your team respond to a personal request for a favour from the managing director, CEO or other senior executives in the business?

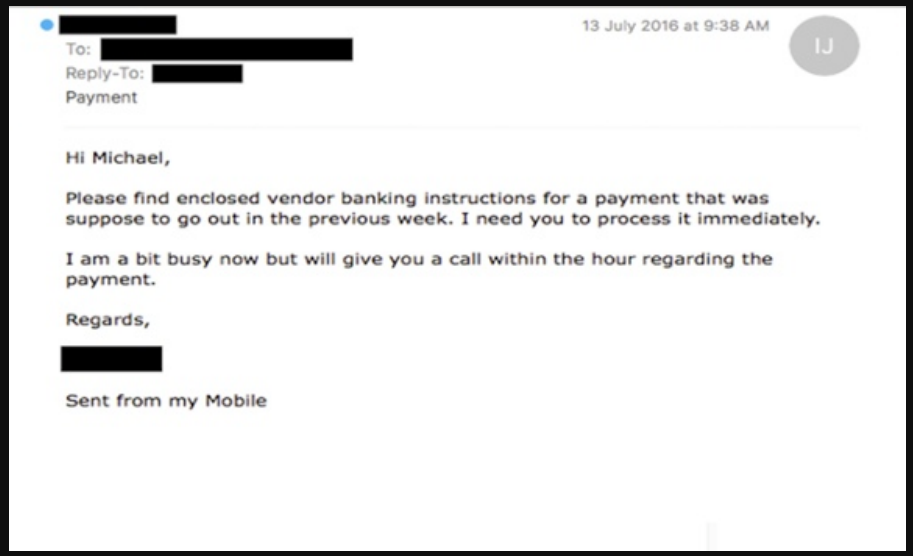
03
AN EXPLOSION OF EASY-ACCESS DATA

The new norm in the digital economy

Having established a connection and that the person is available, the following example purports to be from another managing director in yet another ASX-listed business.

It provides details for the payment and makes clear that the payment is overdue so there is some urgency.

The request is from the mobile phone of the MD, making clear he is not in the office so there is no point trying to speak with him in person.


[redacted]
13 July 2016 at 9:38 AM
IJ
To: [redacted]
Reply-To: [redacted]
Payment

Hi Michael,

Please find enclosed vendor banking instructions for a payment that was suppose to go out in the previous week. I need you to process it immediately.

I am a bit busy now but will give you a call within the hour regarding the payment.

Regards,

[redacted]

Sent from my Mobile

You can see how simple these scams are, yet they are extremely effective. With little time and cost invested, a cybercrime network can easily assume the identity of a high-profile executive to pressure employees in the business to make a payment.

As simple as they may seem, these attacks are happening all too regularly, and with devastating effect.

04 THE EMERGENCE OF A NEW GLOBAL INDUSTRY

A sophisticated network of cybercriminals


"The cost impact of cyber attacks on companies is complex, and not limited to just a loss of shareholder value, although this can be, as we've seen, significant."
The Hon. Malcolm Turnbull MP
Prime Minister of Australia[8]

04
THE EMERGENCE OF A NEW GLOBAL INDUSTRY

A sophisticated network of cybercriminals

With so much data at the disposal of cybercriminals, online users are easy prey.

Cybersecurity Ventures predicts cybercrime will cost the world $6 trillion annually[43] by 2021. Many corporations are hesitant to announce they've suffered a breach – or their security budgets – for fears of reputational damage.

04
THE EMERGENCE OF A NEW GLOBAL INDUSTRY

A sophisticated network of cybercriminals

Just as with cybercrime, cybersecurity is a burgeoning industry. Cybersecurity Ventures projects $1 trillion will be spent globally on cybersecurity from 2017 to 2021.[44]

Rob Owens, senior research analyst at Pacific Crest Securities, recently told Investor's Business Daily that companies still aren't spending enough on security.

"I think security has been an under-spend area for decades. You're spending about 3% of your capex (capital expenditures) that's focused on IT on security. That's relatively low."[45]


“Ignorance is a dangerous option”
Craig McDonald
Founder & CEO, MailGuard10

04
THE EMERGENCE OF A NEW GLOBAL INDUSTRY

A sophisticated network of cybercriminals

While defences are growing, so is criminals' sophistication.

"A service-based criminal industry is developing, in which specialists in the virtual underground economy develop products and services for use by other criminals. This 'Crime-as-a-Service' business model drives innovation and sophistication, and provides access to a wide range of services that facilitate almost any type of cybercrime," said Owens.[46]

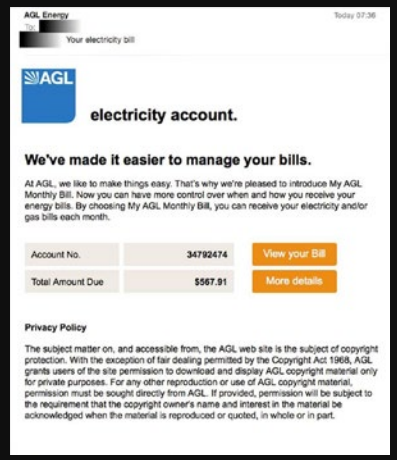
04
THE EMERGENCE OF A NEW GLOBAL INDUSTRY

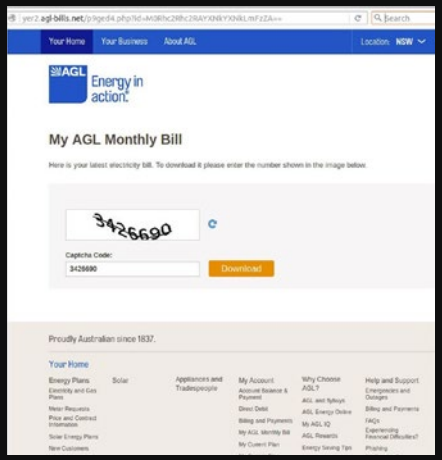
A sophisticated network of cybercriminals

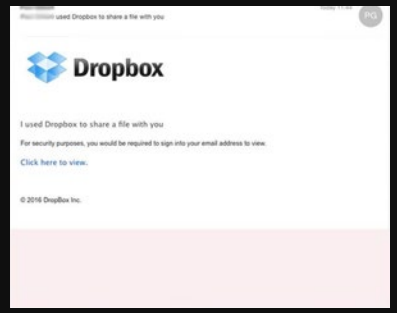
Cleverly employing consumer psychology, cybercriminals leverage brands we know and trust to drive engagement.

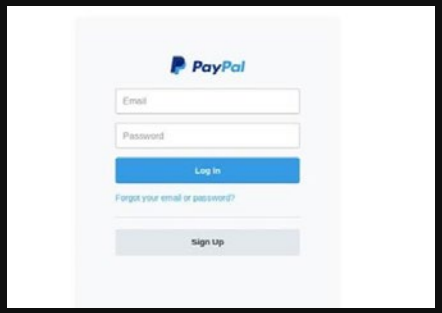
Email is their preferred entry point, with more than nine out of 10 attacks delivered via inboxes. It's simple, low-cost and most email users are flooded with messages so the time spent considering each request is relatively brief.

All it takes is for an unsuspecting staff member to click on a single email, and the impact can be devastating.










"It's one of the great paradoxes of our time that the very technologies that empower us to do great good can also be used to undermine us and inflict great harm."
Barack Obama
President of the United States of America[11]

04
THE EMERGENCE OF A NEW GLOBAL INDUSTRY

A sophisticated network of cybercriminals

iOCTA, the Internet Organised Crime Threat Assessment, highlights that barriers into cybercrime are being lowered as those lacking technical expertise – including traditional organised crime groups – venture in by purchasing the skills they lack.[47]

iOCTA says the best responses include:

- awareness raising,
- international and cross-border co-operation,
- development of adequate legislation, and
- the dismantling of the criminal infrastructures behind illicit online services.[48]

Darknets are often used by criminals for illicit online trade. Here are some important definitions:

Deep web: Hidden parts of the web whose contents are not indexed by standard search engines. Not necessarily illicit content, but undiscoverable via a public link. It might be information behind a paywall, or search results within a travel website.

Dark web: A small portion of the deep web that has been intentionally hidden and is inaccessible through standard web browsers. The most famous content that resides here is found in the TOR network, which is only accessed with a special web browser. In cybersecurity circles, the dark web is well known as a marketplace for the proceeds of cybercrime, and a safe haven for information exchange, co-ordination and discussions.

Surface web: Anything a search engine can access on the internet that is available to the general public.


"Let me begin with cyber threats to our national security.
Terrorists are increasingly cyber-savvy. Much like every other multi-national organisation, they are using the internet to grow their business and to connect with like-minded individuals. And they are not hiding in the shadows of cyberspace."
Robert S. Mueller, III
Director, Federal Bureau of Investigation (FBI)[12]

04
THE EMERGENCE OF A NEW GLOBAL INDUSTRY

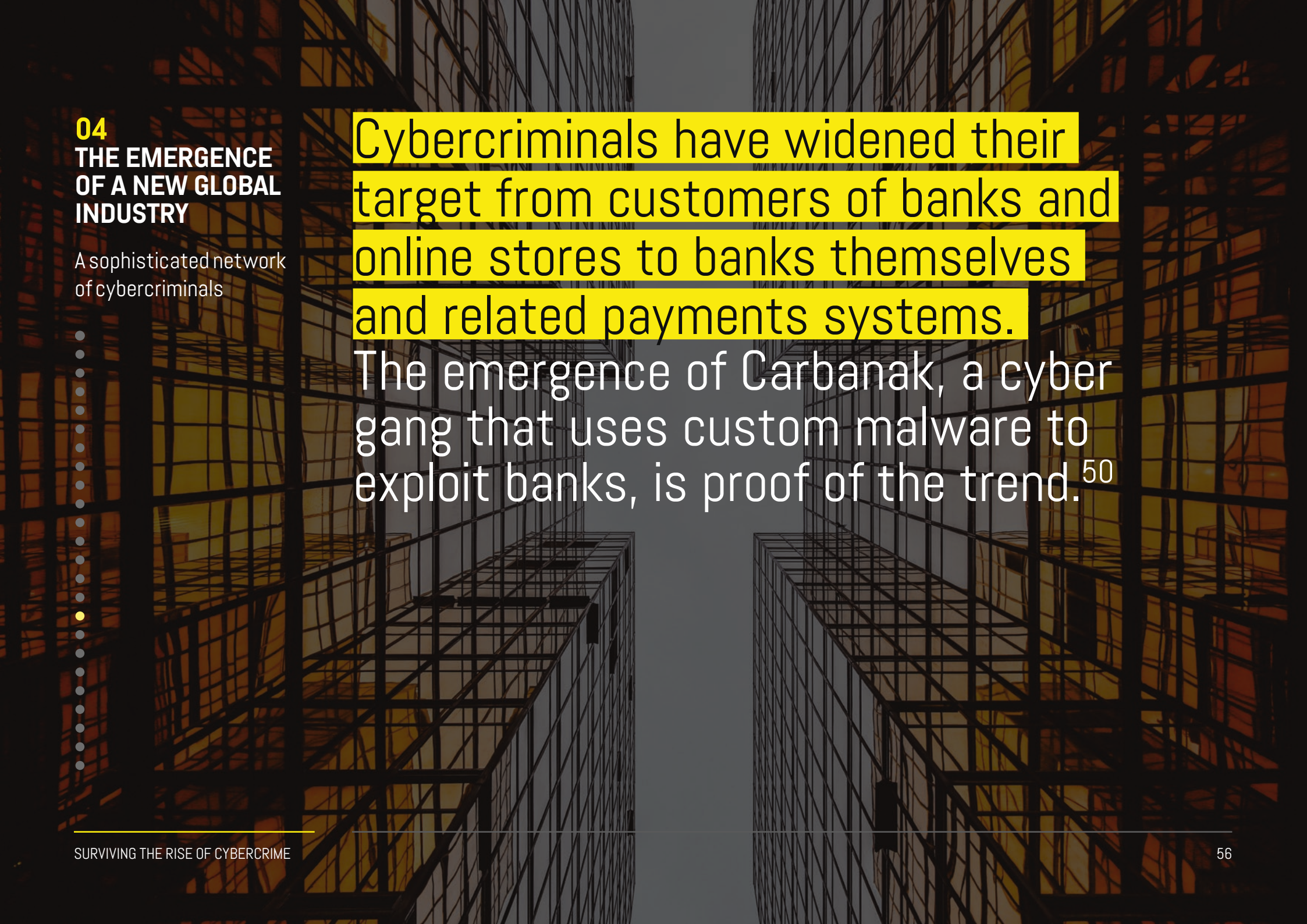
A sophisticated network of cybercriminals

Cybercrime networks using the dark web often trade from jurisdictions unlikely to prosecute, such as Russia and China. For buyers, the menu of options is staggering: social security numbers, stolen credit card details and full identity information can be as cheap as a few dollars each. Many malware authors offer both software for sale and malware-as-a-service. Additional services, such as zero-day vulnerability information, are even more lucrative.

A sophisticated network of cybercriminals

Each country has a speciality on the dark web[55]

According to security vendor Kaspersky Lab, Russian criminal organisations stole about $790 million from 2012 to 2015 – most from victims outside Russia.[49]



Cybercriminals have widened their target from customers of banks and online stores to banks themselves and related payments systems. The emergence of Carbanak, a cyber gang that uses custom malware to exploit banks, is proof of the trend.[50]

Cybercriminal recruitment is itself a growing industry.

By advertising “real” job vacancies, cybercriminals often seek employees from the remote regions of Russia and neighbouring countries such as Ukraine

Cybercriminal recruitment is itself a growing industry. Skilled hackers are drafted by Russian gangs for programming, virus creation, web designing for phishing pages, and testing.[55]

Cryptographers, or ‘cryptors’ specialise in packing malicious code to evade malware detection. By advertising “real” job vacancies, cybercriminals often seek employees from the remote regions of Russia and neighbouring countries such as Ukraine, where employment opportunities and salaries for IT specialists are lacking.

Prices for stolen credit card data are highly volatile

Exploit kits are available for $500-$1000; malware source code could be $800 to $4000 depending on the type. Many even come complete with full customer support and SLAs to ensure success.[55]

Prices for **stolen credit card data** are highly volatile, and depend on the card origin, balance and expiration date. CVV security codes could go for $3-25; a card dump – the unauthorised copying of the information contained on a card's magnetic strip – might be $20-$60.[55]

A 'fullz' – scammer slang for **full personal information** – could net $25-125.[55]

The Arbor Security Engineering & Response Team (ASERT) estimates **a DDoS* attack** could be launched for under US$60 per day, or $400 per week.[55]

*See dictionary definition on page 120

Cybercrime networks move at pace, outsmarting prevailing technologies and techniques. What people often fail to understand is that cybercriminals have access to the same publicly available software that many businesses rely upon, especially signature-based software such as antivirus, allowing them to test and iterate on attacks to bypass those signatures.

"Unlike state-sponsored intruders, hackers for profit do not seek information for political power – they seek information for sale to the highest bidder. These once-isolated hackers have joined forces to create criminal syndicates. Organised crime in cyberspace offers a higher profit with a lower probability of being identified and prosecuted.

Unlike traditional crime families, these hackers may never meet, but they possess specialised skills in high demand.

They exploit routine vulnerabilities. They move in quickly, make their money, and disappear. No company is immune, from the Fortune 500 corporation to the neighborhood "mom and pop" business."

Robert S. Mueller, III

Director, Federal Bureau of Investigation (FBI)[14]

Many businesses have a false sense of security, thinking up-to-date antivirus software will protect them.

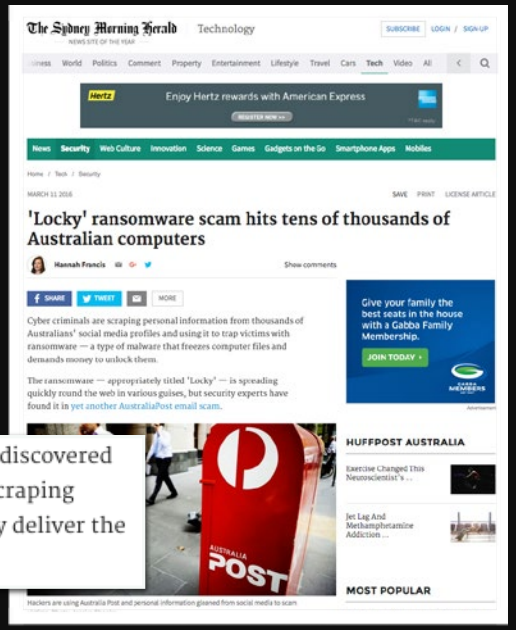
Antivirus software is signature based. This means that after an attack has occurred, the characteristics of the attack are coded into a signature, or a rule, to prevent future breaches.

Antivirus alone is not the answer. When a threat is known, antivirus can stop it, but cybercriminals move quickly, relying upon the element of surprise. In minutes an attack can be executed, yet it takes hours or days for traditional antivirus vendors to push out updates to customers.

What this means for the cybercriminal is that there is a window of opportunity (or window of vulnerability) between the time the attack is detected, and when a new signature is designed and deployed to stop those threats. This window of vulnerability can be hours or even days.

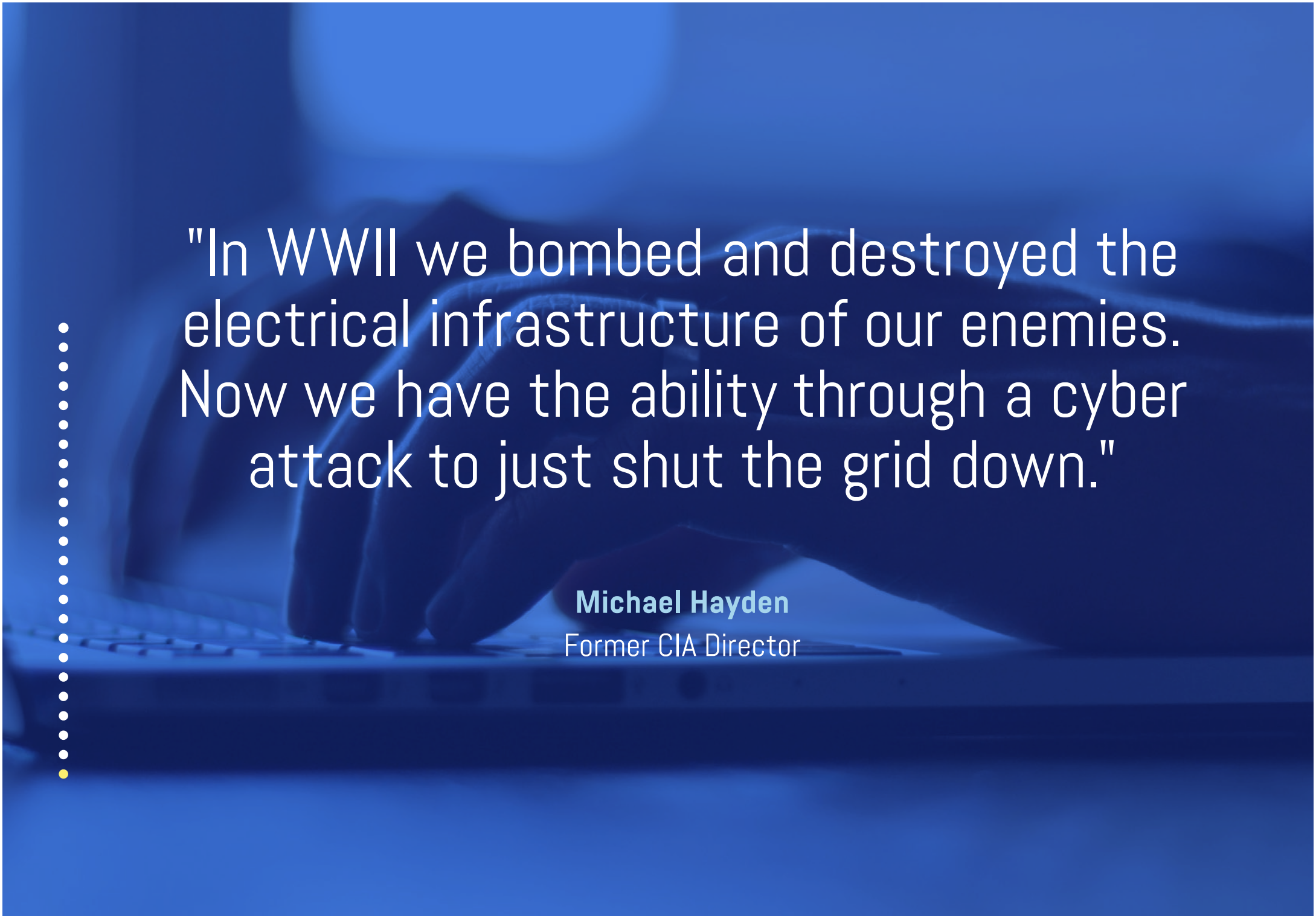
During that window of vulnerability, criminals continue to iterate on attacks to avoid detection.

In March 2016, within the first two hours of an Australia Post 'Locky' ransomware email scam being blocked by my team, we observed more than 160+ variations, all designed to stay ahead of signatures.



MailGuard, the anti-virus and security company which discovered the scam, said hackers were using "highly advanced" scraping software to scan social media profiles and automatically deliver the malicious email to tens of thousands of victims.

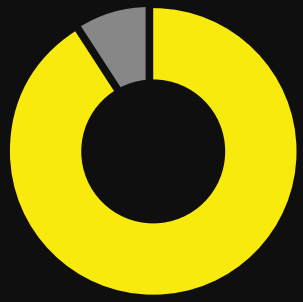
The next-generation of protection is email filtering that is predictive by design, using machine learning and artificial intelligence to scan tens of thousands of email attributes in milliseconds, to anticipate and stop new and emerging threats.


"In WWII we bombed and destroyed the electrical infrastructure of our enemies. Now we have the ability through a cyber attack to just shut the grid down."
Michael Hayden
Former CIA Director

05 LET'S TALK NUMBERS

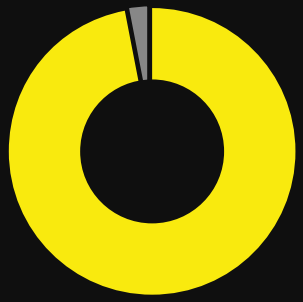
Quantifying the impact

The human cybersecurity challenge



91% of all cybercrime is initiated by email.[52]

CXO financial 'whaling' attacks are on the rise.

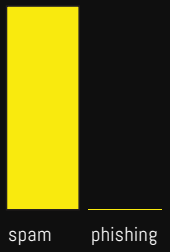


97% of people cannot identify a phishing email.[60]

05
LET'S TALK NUMBERS

Quantifying the impact

60% of hacked SMEs go out of business within six months of a cyber attack[62]



It's estimated that 100 billion spam emails are sent daily worldwide, and 500 million phishing emails make it into inboxes.[64]

The average cost of cyber attack to a business is $276,323 and takes an average time of 23 days to resolve[63]

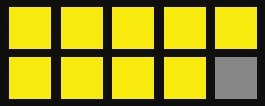
05
LET'S TALK NUMBERS

Quantifying the impact

1/4 (23%) of email users click malicious content.[61]

Cybercrime has skyrocketed, increasing by 300% since 2015.[65]

Two out of three emails circulating the globe contain unwanted content.[66]



Nine out of 10 businesses report being impacted by spear-phishing.[67]


"Denial of service, hacking, phishing and malware, are disruptive to our economies, our social interactions, and – through their unwavering persistence – our sense of security.
This undermining of our online confidence means we are not fully leveraging the digital economy."
The Hon. Malcolm Turnbull MP
Prime Minister of Australia[25]

06 THE CHANGING SECURITY LANDSCAPE

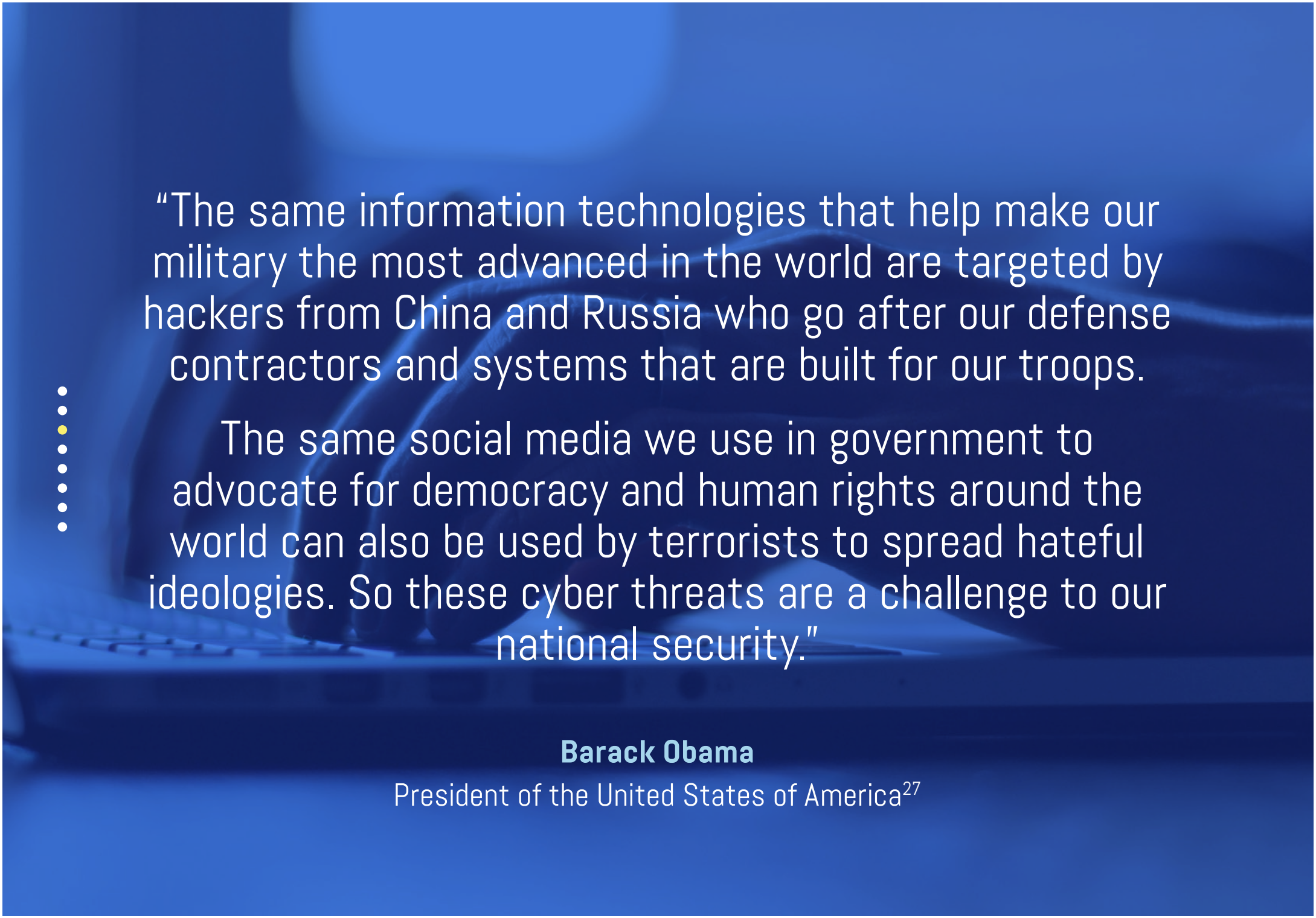
Security in depth

As an executive, it's important to be familiar with potential risks to help guide your organisation's cybersecurity plan. It is vital to protect your computer hardware, software, data and customers from unauthorised access.

While it is almost impossible to prevent all risks, basic security practices can make an enormous difference.

Cyber attacks typically target your business' information, personal data for your staff and customers, IT infrastructure and equipment.

Cybercriminals' preferred entry point is email: it's cheap, easy and potential targets are plentiful. For the scammers, information is valuable. Commonly-stolen data includes client lists, transaction information, databases, financial details, pricing information and personal data.



"The same information technologies that help make our military the most advanced in the world are targeted by hackers from China and Russia who go after our defense contractors and systems that are built for our troops.

The same social media we use in government to advocate for democracy and human rights around the world can also be used by terrorists to spread hateful ideologies. So these cyber threats are a challenge to our national security."

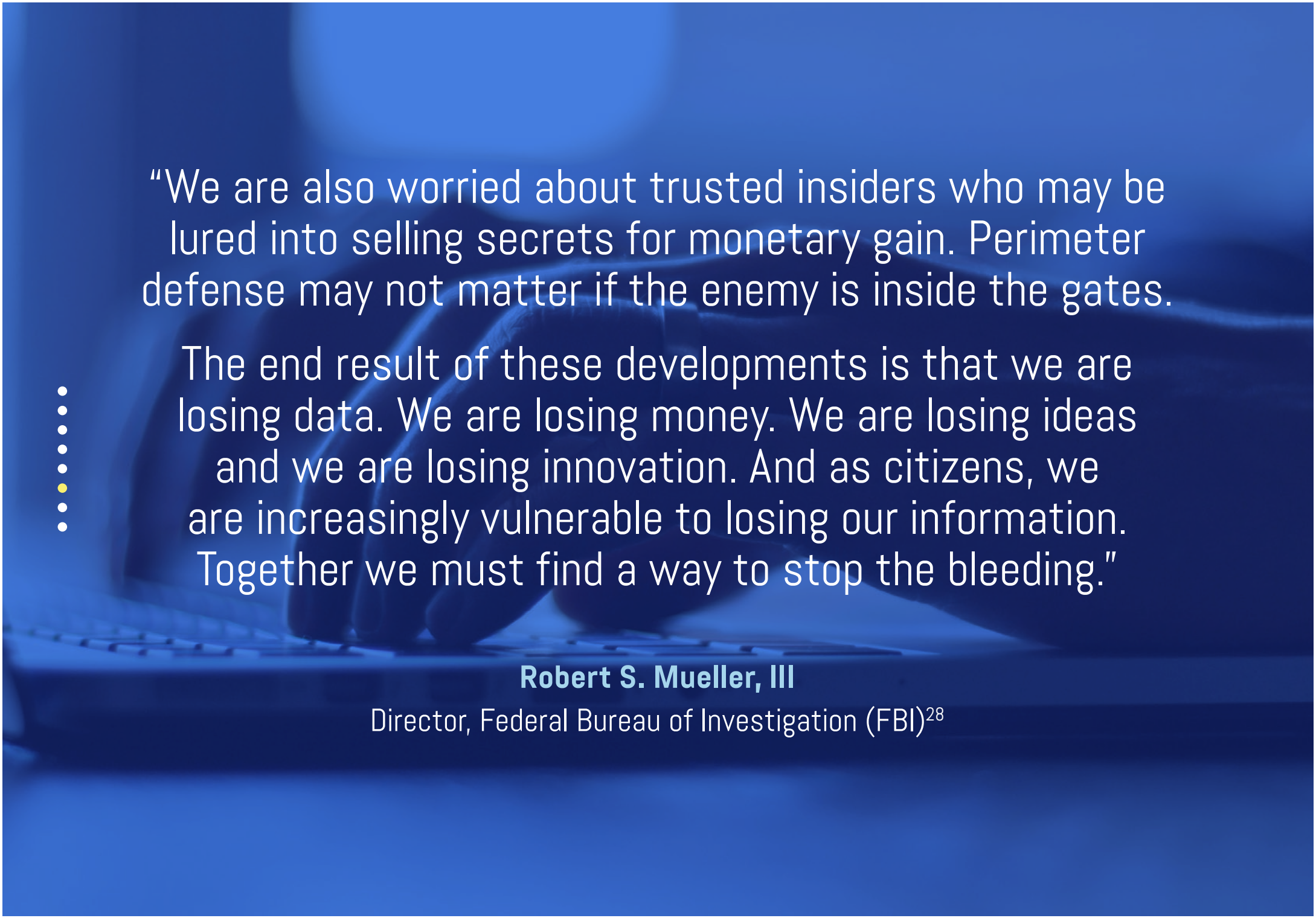
Barack Obama

President of the United States of America[27]

There are many ways an attack or breach can occur: theft, unauthourised access to equipment, remote attacks on your IT system or website, or attacks on information held by third-parties, such as a cloud-based system or vendor.

It's not just criminals or competitors who might steal from or disrupt your business: current or former employees could also pose a threat.

Employees have access to privileged information and can compromise it by accident, through negligence or with malicious intent. Leaving a laptop unattended for just a few minutes can pose a threat.


"We are also worried about trusted insiders who may be lured into selling secrets for monetary gain. Perimeter defense may not matter if the enemy is inside the gates.
The end result of these developments is that we are losing data. We are losing money. We are losing ideas and we are losing innovation. And as citizens, we are increasingly vulnerable to losing our information. Together we must find a way to stop the bleeding."
Robert S. Mueller, III
Director, Federal Bureau of Investigation (FBI)[28]

The consequences of an attack can be devastating.

A single attack – perhaps an employee falls victim to a phishing link and ransomware locks your entire system – could seriously damage your business.

If bank or financial details are taken, everyday business can be disrupted.

Customers might look elsewhere and your reputation will suffer.

There are also significant costs involved with a successful cyber attack, such as cleaning up and restoring equipment, IT systems, networks and websites.

There is a risk of breaching privacy or data protection legislation too, which can lead to costly fines.

Attacks can also damage other companies you are associated with, such as suppliers or business partners.

Best-practice suggests engaging multiple forms of security.

Often referred to as 'layered security' or 'defence in depth', it means employing complementary controls sufficient to detect and deter infiltration and exploitation of an organisation, its information systems and facilities.

07 YOUR ACTION PLAN

What to consider


"There are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again."
Robert S. Mueller, III
Director, Federal Bureau of Investigation (FBI)[29]

07
YOUR ACTION PLAN

What to consider

When considering a plan for your organisation, begin by asking yourself these simple questions:

1. What information or revenue-generating assets are critical to your business? What kind of risks could they be exposed to? Think about customer records, financial data or other IP critical to your business.
2. Are resources allocated based on risk appetite and strategic assets?
3. Is a risk management framework in place, incorporating cybersecurity and reporting?
4. What technical capabilities does the company have in place to identify malicious events in real-time?
5. Is there a response plan in the event of a breach or attack? Is the response plan tested and how often?
6. What relationships does the company have with supply chain, government and other third-party organisations to respond effectively to a breach? What relationships need to be developed?
7. Are there legal and compliance requirements relating to your business? How are these being managed and reviewed?
8. Could you continue to conduct business as usual if you were taken offline for any period of time?
9. Does your cyber insurance policy cover your business for first and/or third party?

To request a 1-page cybersecurity framework that we use at MailGuard go to www.mailguard.com.au/policyframework

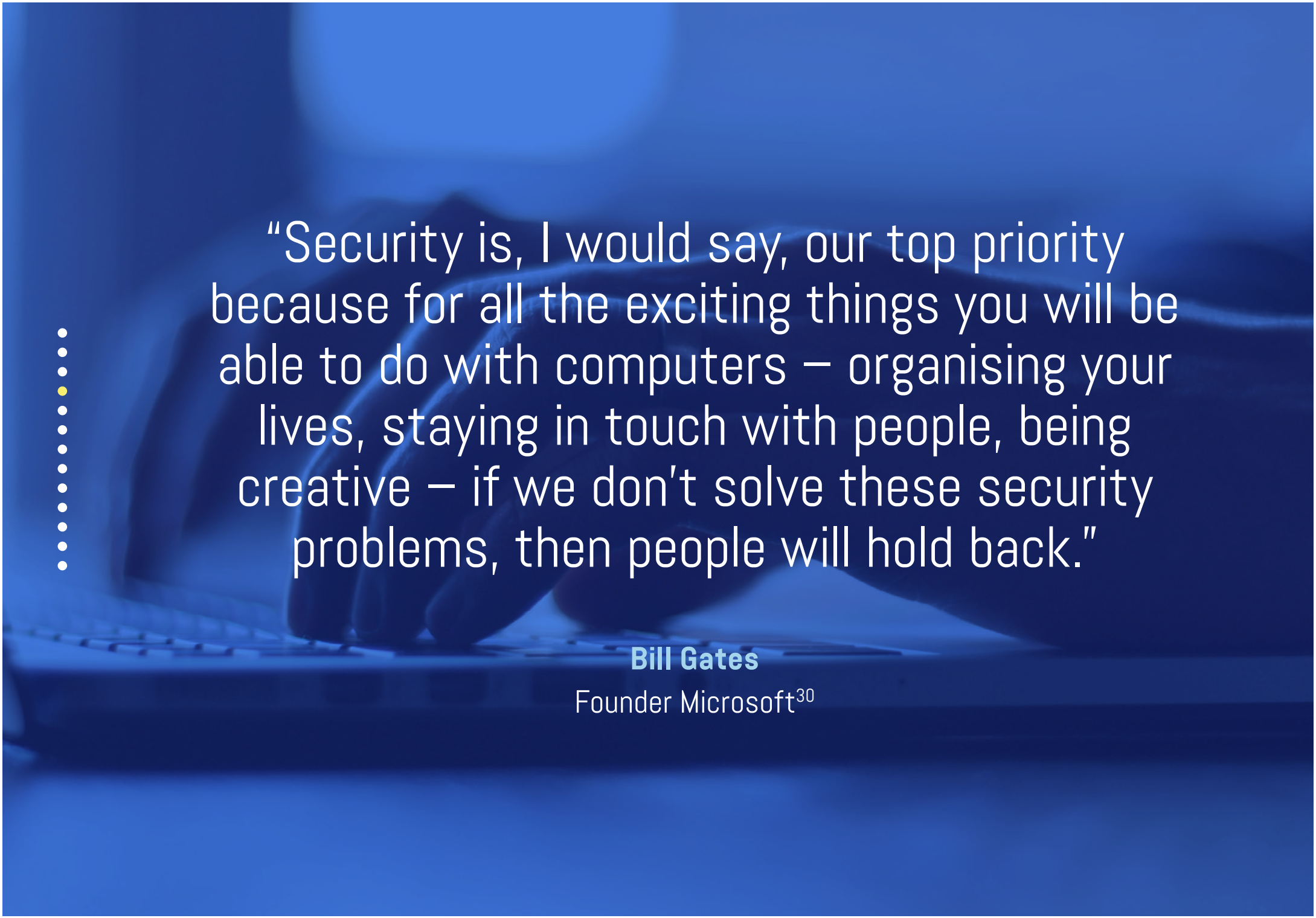
07
YOUR ACTION PLAN

What to consider

The unfortunate reality is that every business is a target for an attack. Whether that's a targeted spear-phishing campaign, or an indiscriminate attack like the delivery of CryptoLocker or other ransomware.

Commonly reported attacks target accounting firms and those in financial services, shipping or delivery, or companies that deal with transfers of large sums of money.

Networking is vital. Ask if your suppliers, major customers or similar businesses in your industry have been attacked. It may be an early indicator that cybercriminals are targeting your network.


“Security is, I would say, our top priority because for all the exciting things you will be able to do with computers – organising your lives, staying in touch with people, being creative – if we don't solve these security problems, then people will hold back.”
Bill Gates
Founder Microsoft[30]

Do you know the regulatory and legislative obligations for your organisation?

Does your organisation need to comply with **personal data protection legislation**, such as the Data Protection Act and Payment Card Industry compliance?

Are there regulations specific to your sector, such as the Healthcare Identifiers Act 2010 (HI Act) which imposes data quality and data security obligations for healthcare providers, or the Telecommunications Act 1997 for ISPs and telecommunications carriers in Australia.

Do you operate in different jurisdictions, and if so how does that change your obligations? In the United States healthcare providers must also consider HIPAA. (the Health Insurance Portability and Accountability Act of 1996)

What are your obligations for privacy, say under the Privacy Act 1988 in Australia, the Data Protection Act 1998 (DPA) in the United Kingdom? As a 'Data Controller', what are your obligations under the Data Protection Directive of the European Commission?

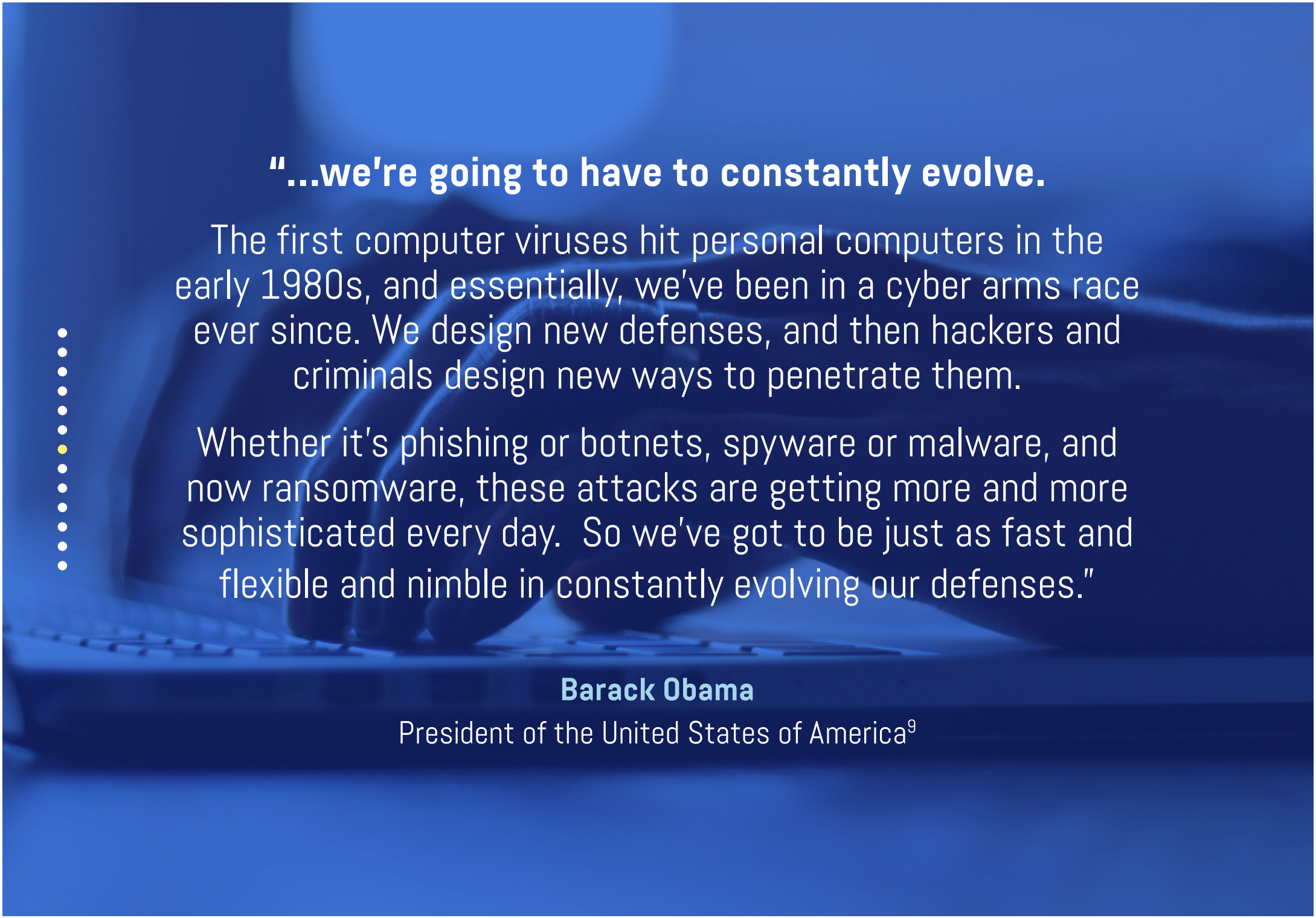
Across the US, regulations vary. In California there is the Online Privacy Protection Act (OPPA) 2003, and the proposed Right to Know Act.

07
YOUR ACTION PLAN

What to consider

Identify financial and information assets critical to your business, along with essential IT services, such as online payments.

What infrastructure, IT equipment and devices, such as mobiles, laptops and tablets, are critical to your business?



"...we're going to have to constantly evolve.

The first computer viruses hit personal computers in the early 1980s, and essentially, we've been in a cyber arms race ever since. We design new defenses, and then hackers and criminals design new ways to penetrate them.

Whether it's phishing or botnets, spyware or malware, and now ransomware, these attacks are getting more and more sophisticated every day. So we've got to be just as fast and flexible and nimble in constantly evolving our defenses."

Barack Obama

President of the United States of America[9]

Understand potential risks by considering how they are currently managed and stored, and who has access to them.

What happens if an unforeseen attack shuts down your operations indefinitely?

Assess the level of password protection required to access equipment and online services by staff, third parties and customers.

Determine whether your security can be strengthened. Instead of traditional passwords, use passphrases that contain numbers and characters to help prevent automated 'dictionary attacks'. Enforce two-factor authentication where possible and use password-management software to keep sensitive information secure.

07
YOUR ACTION PLAN

What to consider

- Ensure regular staff training. Do your employees understand their role in cybersecurity?
- Is ongoing education provided to make staff aware of threats and risks to your business?
- Do you have an information security policy that all staff must sign?
- Do you conduct social engineering tests to identify staff training development areas?

Are you confident that your organisation has access to the necessary level of cybersecurity expertise?

Decide whether additional investment or expert advice is needed to protect your business. If so, seek professional advice. Engage a reputable security company to help find the weaknesses in your environment.


"The Australian Crime Commission estimates the annual cost of cybercrime to Australia is over $1 billion in direct costs, but some estimates put the real costs to be as high as one per cent of GDP a year - or about $17 billion."
The Hon. Malcolm Turnbull MP
Prime Minister of Australia[33]

Who will provide assistance if your organisation experiences a breach, if you are attacked or if online services are disrupted?

Define recovery procedures and plan how to keep your business running in the event of an attack.

08

HAVING THE RIGHT TEAM IN PLACE.

Roles & responsibilities

All too often when I am speaking with C-level executives and boards, they tell me: “We have people for that. I pay someone to take care of cybersecurity.”

Cybersecurity is the responsibility of everyone in your organisation, and that must start from the top.

"We must convince leaders, at board level and corporate sector and government levels, that cyber is one of their essential functions. That means people must be cyber ambassadors and carry that message.

Many companies have Chief Technology Officers and Chief Information Security Officers. Both have technical knowledge and business acumen.

The most obvious reason to value the role of a Chief Information Security Officer in board-level decision-making is the risk of cyber threat to your budget bottom line. As we are all acutely aware, a cyber attack or data leak from even a mundane business system like email can have a dramatic impact on an enterprise.

In fact, to properly recognise the convergence of online and offline threats, consideration should probably be given to now replacing the title of CISOs with the more appropriate Chief Security Officer."

The Hon. Malcolm Turnbull MP

Prime Minister of Australia[34]

08
HAVING THE RIGHT TEAM IN PLACE

Roles & responsibilities

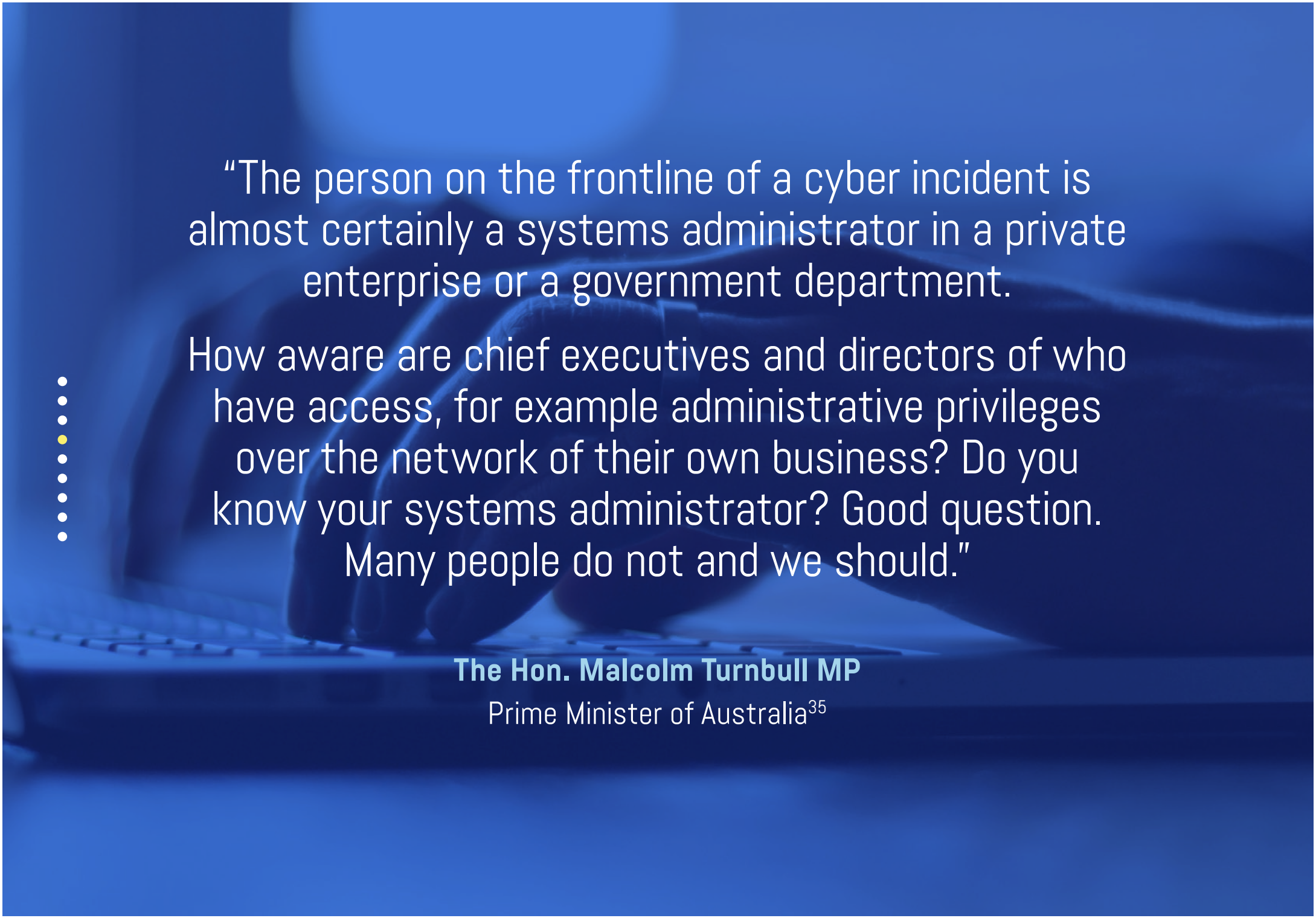
With the convergence of online and offline threats, many leading organisations are now considering a combined Chief Security Officer role to take the lead.

Responsibility for cybersecurity often sits at an executive level with a CIO, CTO, or a CISO.

Sometimes it even resides with a CFO given the risk of fraudulent payments.

With the convergence of online and offline threats, many leading organisations are now considering a combined Chief Security Officer role to take the lead.

In smaller businesses without the luxury of technical or security specialists, this responsibility will often reside with company directors, who must work closely with external IT and security consultants to truly understand the risks.



"The person on the frontline of a cyber incident is almost certainly a systems administrator in a private enterprise or a government department.

How aware are chief executives and directors of who have access, for example administrative privileges over the network of their own business? Do you know your systems administrator? Good question. Many people do not and we should."

The Hon. Malcolm Turnbull MP

Prime Minister of Australia[35]

08
HAVING THE RIGHT TEAM IN PLACE

Roles & responsibilities

While it can sometimes be the case, it is unwise to assume that your IT manager is a cybersecurity expert.

Consider the expertise within your organisation supporting the executive team in strategic decisions, and importantly, executing against that security strategy every day.

Who are your IT managers and systems administrators? What is their role? Do they have the skills and experience necessary?

While it can sometimes be the case, it is unwise to assume that your IT manager is a cybersecurity expert.

In the spirit of 'layered security' and 'defence in depth', it takes an entire team to defend your organisation.

"A forward-thinking government knows it will always be intertwined with industry in the field of cybersecurity.

That's why we must work together – private sector and nation states – to secure the internet. The challenges the internet faces are greater than can be solved by any of us alone.

For all my enthusiasm for government's responsibilities in cyberspace, good cyber policy requires the co-operation and creativity of academia and industry."

The Hon. Malcolm Turnbull MP

Prime Minister of Australia[36]

Your organisation should have an information security policy that is signed off and understood by your executive team and all staff.

Best practice is to base your information security policy on ISO 27001, which is a specification for an information security management system (ISMS). This is a framework of policies and procedures incorporating legal, physical and technical controls relating to information risk.

Regardless of how confident you are in your internal team, it is always prudent to engage a reputable security company to provide advice and oversight, and to help find and protect against the weaknesses in your environment.


"Risk comes from not knowing what you're doing."
Warren Buffet
Businessman, Investor & Philanthropist[37]

09 SO WHAT'S NEXT?

Looking forward

Are you confident that you have the answers to all of the questions posed in this guide?

From my experience, you're not alone if your answer is 'no.' What's important is what you do next. My advice: review those questions in Chapter 7 as they relate to your organisation.

I recommend that you put the same challenge to the executives on your organisation's senior leadership team.

Speak to the team members within your organisation who manage your cybersecurity strategy on a day-to-day basis: your Chief Security Officer, IT managers and systems administrators. Consider getting their opinions.


"There's a tremendous
bias against taking risks.
everyone is trying to
optimise their ass-covering"
Elon Musk
CEO & Founder, Tesla and Space-X[38]

Contrast internal opinions with those of external advisers and consultants. I encourage you to form your own view.

When you are confident that you are well-informed about the risks to your organisation and the strategy, plans and resources that are in place to respond, ensure that your organisation is periodically conducting reviews to respond to changes or any problems that are identified.


"People also need to take responsibility for their own cybersecurity and **there are simple steps we can all take to protect our personal and financial information online.**"
Hon. Dan Tehan MP
Minister Assisting the Prime Minister for Cyber Security[39]

Security is by nature, a constantly changing environment. There is always a new threat, and a new method being trialled to break through your defences.

Make sure your team stays informed about new developments and threats by collaborating with peers, and being active in security and industry forums.

Don't wait. Here are six immediate steps to start mitigating the risk today!

I encourage you to engage a professional services partner to do the following.

1. Use a cloud-based email and web security service that can predict and prevent criminal-intent threats (you will know you don't have a leading provider in place by the fact you are still getting emails you don't want)
2. Ensure your files are secured with a cloud-based back-up, to protect your business in the event of a ransomware attack. This will allow you to reinstall critical business files and information.
3. To prevent fraudulent payments, implement a tight internal third-party payment policy for your accounts team. No payment to a new third party is ever that critical that a few checks can't be conducted.
4. Ensure all hardware touch points to the internet are using up-to-date antivirus protection.
5. Implement a cybersecurity policy that every employee must read and sign, and
6. Protect your business with a comprehensive cybersecurity insurance policy that matches your circumstances.

09
SO WHAT'S NEXT?

Looking forward

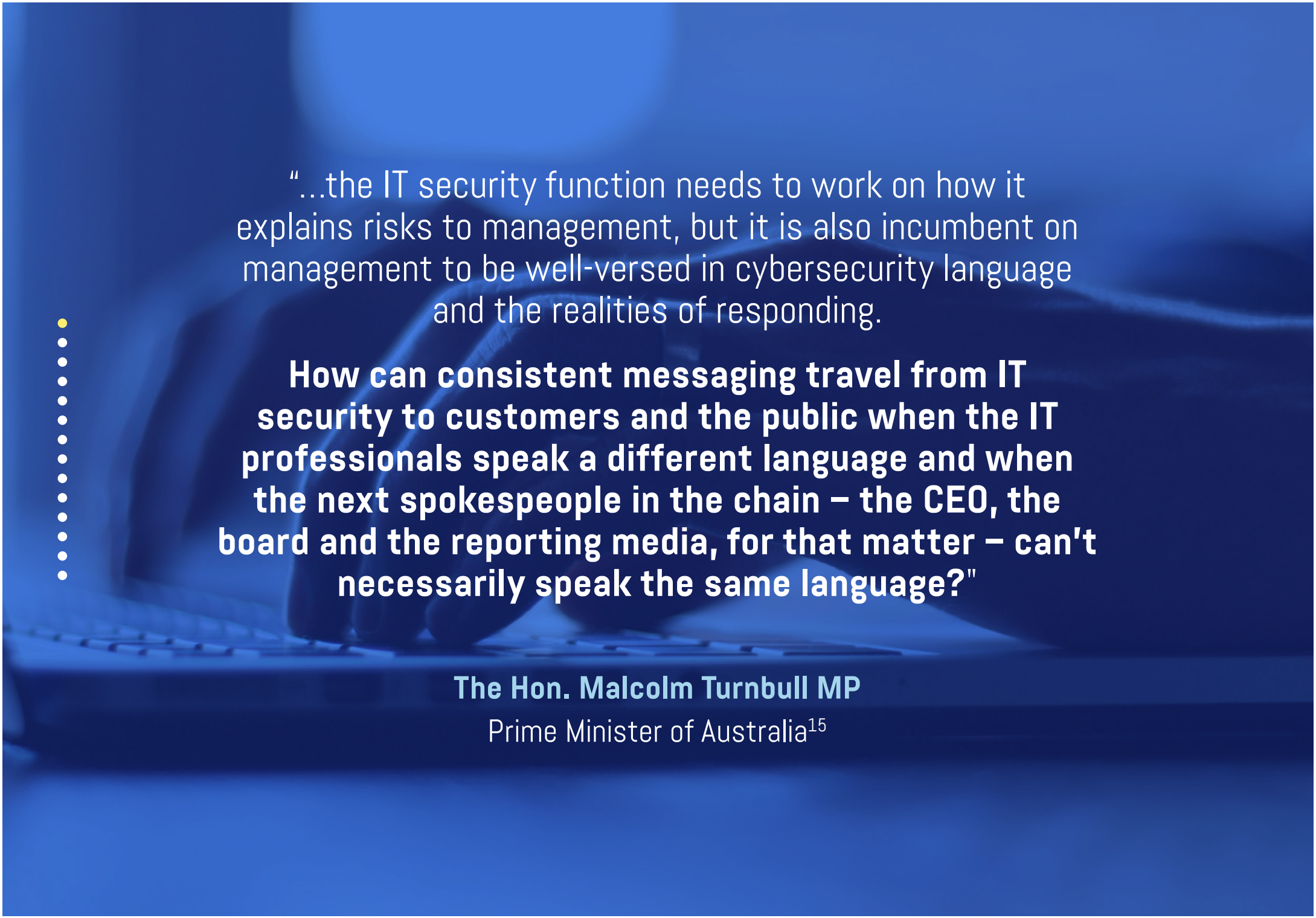
In the final pages of this guide, I have included a glossary of commonly-used cybersecurity terms to help prepare you for the discussion ahead of you. There are also some links to additional resources and references.

If you would like to discuss the cybersecurity readiness of your organisation, please reach out to my team to talk to one of our cybersecurity specialists at **expert@MailGuard.com.au**

Alternatively, please connect with me on LinkedIn. You can find me at **linkedin.com/in/craigmcdonaldcloud**

10 TALKING THE TALK

The beginnings of a cybersecurity lexicon



"...the IT security function needs to work on how it explains risks to management, but it is also incumbent on management to be well-versed in cybersecurity language and the realities of responding.

How can consistent messaging travel from IT security to customers and the public when the IT professionals speak a different language and when the next spokespeople in the chain – the CEO, the board and the reporting media, for that matter – can't necessarily speak the same language?"

The Hon. Malcolm Turnbull MP

Prime Minister of Australia[15]

10
TALKING THE TALK

The beginnings of a cybersecurity lexicon

Commenting on the failure of security professionals to effectively communicate cybersecurity issues to boards and C-suite leaders, Australian Prime Minister, Malcolm Turnbull, challenged business leaders to be 'well-versed in cybersecurity language,' and said we need to develop a common cybersecurity lexicon.

To start you on that journey, here are some commonly-used terms, courtesy of **staysmartonline.gov.au/glossary**, with some additions from my team at MailGuard.

10 TALKING THE TALK

The beginnings of a cybersecurity lexicon

A
Account Harvesting
ADSL
Adware
Antivirus

B
Bitcoin and crypto-currencies
Bot
Botnet
Botnet master
Browser hijacking

C
Catfish
Cookie

D
Denial-of-service attack (DoS)
Dictionary attack
Digital certificate
Distributed denial-of-service attack (DDoS)
Domain Name System (DNS)
Drive-by-download

E
Encryption

F
Firewall
Freeware

H
Hacker
Hardware
Hotspot

I
Identity Theft
Internet Service Provider (ISP)

K
Keystroke logger

L
Like farming

M
Malicious software (Malware)
Modem

P
Padlock
Password
Patches
Peer-to-peer file sharing network (P2P)
Pharming
Phishing (email/ website)
Pop-up
Privacy settings

R
Ransomware
Remote access
Rootkit
Router

S
Scam
Scareware
Security symbols
Service Set Identifiers (SSID)
Secure Socket Layer (SSL)
Social engineering
Spam
Spear phishing
Spyware

T
Trojan horse

U
URL
USB stick

V
Virus
VoIP

W
Whaling
Wi-Fi
Worm

Z
Zombie

10
TALKING THE TALK

The beginnings of a cybersecurity lexicon

A

Account harvesting

The illegal practice of collecting email accounts from information in the public domain or by using software to search for email addresses stored locally on a computer. Account harvesting is one of the foundations for spamming.

ADSL

Asymmetric Digital Subscriber Line (ADSL) is a data communications technology that enables faster data transmission over copper telephone lines than a conventional dial-up modem can provide.

Adware

Software that is covertly installed on your computer and designed to deliver advertisements or other content which encourages you to purchase goods or services.

Antivirus

Software that is designed to prevent infection from computer viruses.

B

Bitcoin and crypto-currencies

A type of digital currency which uses encryption techniques to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank.

Bot

A single compromised computer (a robot computer), sometimes called a zombie.

Botnet

A network of compromised computers, also called a zombie network.

Botnet master

The individual (or group) who controls a botnet remotely, also called a bot-herder.

Browser

A software application that enables the retrieval and presentation of websites and other internet resources.

"Increasing the capacity for security staff to engage in conversations with senior decision-makers is absolutely critical when it comes to responding to a cyber incident.

...without ongoing good communications and a working knowledge of cyberspace, your capacity to respond is hampered.

In one study, 80 per cent of organisations said they don't frequently communicate with executive management about potential cyber attacks against their organisations."

The Hon. Malcolm Turnbull MP

Prime Minister of Australia[16]

10 TALKING THE TALK

The beginnings of a cybersecurity lexicon

Browser hijacking

A symptom of a malware infection (particularly ransomware and scareware) in which your browser persistently redirects to fraudulent websites, usually in an attempt to extort money.

C

Catfish

Internet predators who create fake online identities to lure people into emotional or romantic relationships for personal or financial gain.

Cookie

A string of text stored by your web browser enabling a website to remember you and your personal settings.

D

Denial-of-service attack (DoS)

An attack that 'floods' a system with useless data or requests for data in order to overload it.

Dictionary attack

A technique used for finding a password by attempting a search with a large volume of words from a specialized dictionary of commonly used passwords and normal words.

Digital certificate

A way for browsers to verify the identity and authenticity of a website. A digital certificate is issued to a website by a trusted third party certificate authority.

Distributed denial-of-service attack (DDoS)

A denial of service attack coming from multiple sources at once.

Domain Name System (DNS)

A hierarchical naming system for resources connected to the internet. The DNS translates domain names to numerical identifiers (IP addresses) which are readable to networking equipment, allowing the routing of data from one point on the internet to another.

10 TALKING THE TALK

The beginnings of a cybersecurity lexicon

Drive-by-download

A program that is automatically dowloaded to your computer, often without your consent or even your knowledge.

E

Encryption

The process of transforming documents and files for safe transmission over a public network. The information is then converted or deciphered back into its original format.

F

Firewall

Hardware or software which monitors information going in and out of your computer or network.

Freeware

Copyrighted computer software which is made available for use free of charge, for an unlimited time.

H

Hacker

Someone who attempts to gain unauthorised access to a computer system, often for fraudulent purposes.

Hardware

The mechanical parts of a computer system, including the central processing unit, monitor, keyboard, and mouse, as well as other equipment like printers and speakers and mobile devices such as tablets and smart phones.

Hotspot

An area in which wi-fi is available to the general public as a wireless local area network, as in a coffee shop.

I

Identity theft

Use of personal details by someone else to deceive, to support some type of crime, or even just to play a joke. Identity theft is a form of identity crime (where somebody uses a false identity to commit a crime).

10 TALKING THE TALK

The beginnings of a cybersecurity lexicon

Internet Service Provider (ISP)

A company that provides access to the internet.

K

Keystroke logger

A malware program hidden on a computer that records and 'logs' each key you press. It is used to record your personal data, e.g. usernames, passwords, credit card and bank account numbers which is then sent to the malware operator without your knowledge.

L

Like farming

Use of social engineering, such as compelling stories or photos, to persuade large number of users to 'like' a social networking page. Many of the stories are fake, and are part of a scam which makes money from the exposure generated by people liking and hence sharing the page.

M

Malicious software (Malware)

A catch-all term used to describe software designed to be installed into a computer system for the purpose of causing harm to you or others. This would include viruses, spyware, trojans, worms, etc.

Modem

A device that is used to connect your computer to a network (such as the internet) over a long distance.

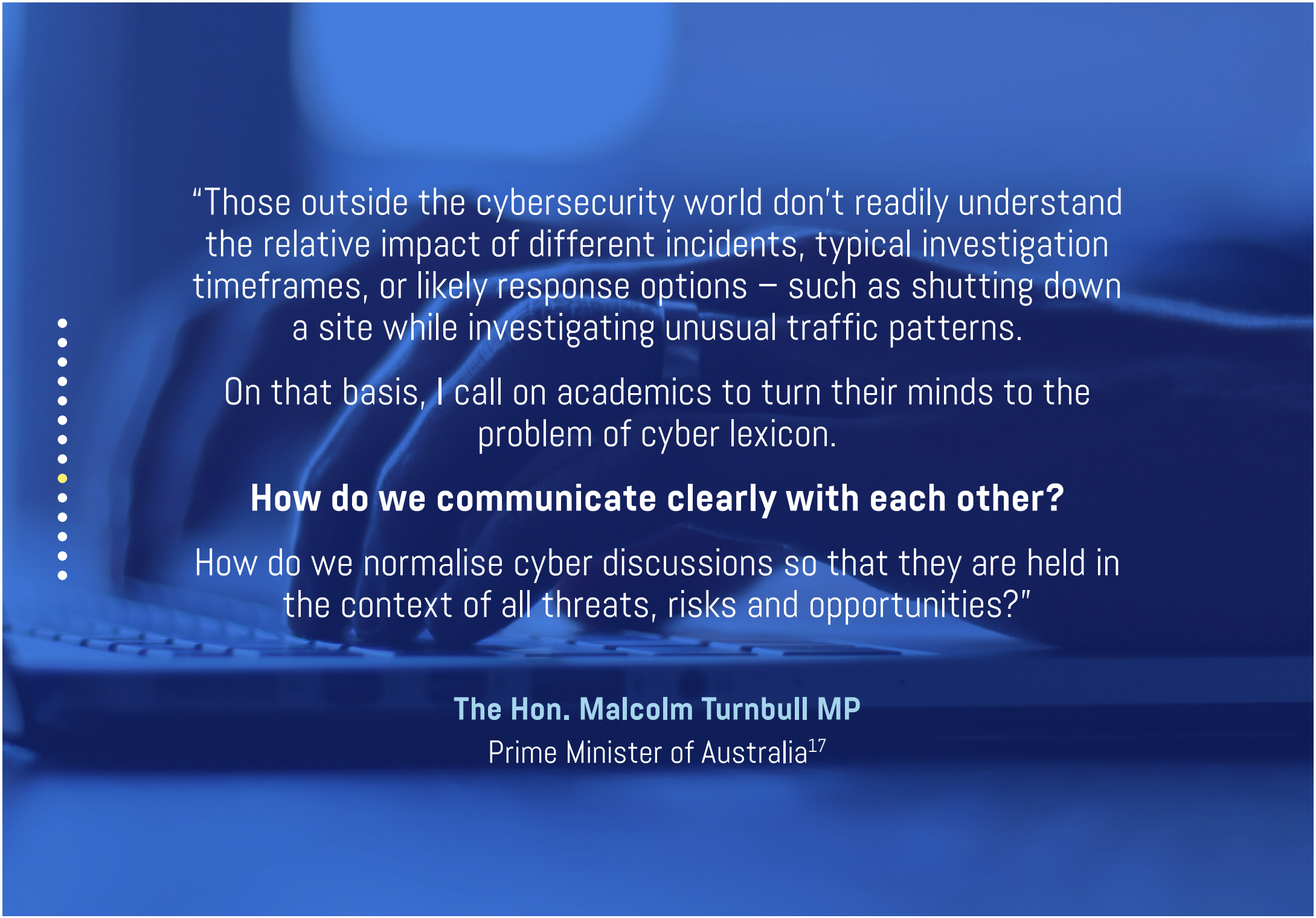
P

Padlock

A padlock display in a browser is intended to indicate a secure connection or website, although it may not always be a reliable indicator. Users should look instead for 'HTTPS' at the beginning of the address bar and check the website's SSL certificate.

Password

A secret word, phrase or series of characters that is used for authentication.



"Those outside the cybersecurity world don't readily understand the relative impact of different incidents, typical investigation timeframes, or likely response options – such as shutting down a site while investigating unusual traffic patterns.

On that basis, I call on academics to turn their minds to the problem of cyber lexicon.

How do we communicate clearly with each other?

How do we normalise cyber discussions so that they are held in the context of all threats, risks and opportunities?"

The Hon. Malcolm Turnbull MP

Prime Minister of Australia[17]

10 TALKING THE TALK

The beginnings of a cybersecurity lexicon

Patches

A fix for a software program, also known as a software update.

Peer-to-peer file sharing network (P2P)

A decentralised file sharing system. Files are stored on and served by the personal computers of the users.

Pharming

A way of harvesting personal information, where a hacker puts a malicious code on your computer that redirects you to a fake site.

Phishing (email/website)

Fraudulent email messages or websites used to gain access to personal information for illegal purposes such as transferring funds or purchasing goods over the internet.

Pop-up

A small window, which suddenly appears (pops-up) in the foreground of the normal screen.

Privacy settings

Settings which control how a user's data is shared with other people or systems. Privacy settings apply to web browsers and social networking services.

R

Ransomware

Malware which handicaps computer functionality, e.g. through browser hijacking or encrypting personal data, and offers to restore the functionality for a fee.

Remote access

Communication with a computer or network from a remote location through a link such as the internet or mobile phone.

Rootkit

A software system that consists of one or more programs designed to obscure the fact that a system has been compromised.

10 TALKING THE TALK

The beginnings of a cybersecurity lexicon

Router

A device that connects a local network to the internet and converts a public IP address to private addresses on the local network.

S

Scam

A commonly-used term to describe a confidence trick, relying on email or a website to deliver the trick to unsuspecting users.

Scareware

Malware that causes frightening messages to appear (for example, that your computer is infected with malware or that you are guilty of a crime), and attempts to extort money from you to resolve the alleged issue. Similar to ransomware.

Security symbols

A secure webpage will have two symbols - a closed padlock image at the top or bottom of the browser window (although this may not be visible on a mobile device), and 'https://' in the address bar. Modern browsers also colour code the address bar to provide a visual cue that the page is secure. These signs help to indicate the presence of a digital certificate, which can provide a way for you to verify the identity and authenticity of a website.

Service Set Identifiers (SSID)

The Service Set Identifier (SSID) is the name given to identify a particular wi-fi network. The SSID is broadcast by the wireless access point (wireless router) and can be detected by other wireless-enabled devices in range of the wireless access point. In some cases SSIDs are hidden, making them invisible to wi-fi clients.

Secure Socket Layer (SSL)

The most widely used security protocol on the internet, used for online banking and shopping sites. Website digital certificates are commonly implemented through SSL. The presence of 'https' in the browser address bar demonstrates that the connection between your computer and the website is encrypted. However, 'https' can still be present when connecting to a website with an invalid digital certificate.


"It takes 20 years to build a reputation and five minutes to ruin it. If you think about that, you'll do things differently."
Warren Buffet
Businessman, Investor & Philanthropist[18]

10 TALKING THE TALK

The beginnings of a cybersecurity lexicon

Social engineering

Psychological manipulation of people in order to achieve a hidden goal. A wide variety of social engineering techniques are used in activities such as fraud, phishing and like farming.

Spam

Unsolicited email. Most spam is commercial advertising, often for dubious products, get-rich-quick schemes, or illegal services. Users are advised that if an offer in an email appears too good to be true then it probably is and should not be actioned in any way.

Spear phishing

An email spoofing fraud attempt (phishing) that targets a specific organisation, seeking unauthorised access to confidential data.

Spyware

Software that is covertly installed on a computing device and takes information from it without your consent or the knowledge of the user.

T

Trojan horse

Malicious code that is hidden in a computer program or file that may appear to be useful, interesting, or at the very least harmless to you when using your computer. When this computer program or file is run, the malicious code is also triggered, resulting in the set up or installation of malware.

U

URL

Universal Resource Locator. The technical term for the address (location) of an internet resource on the internet such as a website or image within a website.

USB stick

Universal Serial Bus. A small piece of hardware that stores data, sometimes called a jump drive, thumb drive or flash drive.

10
TALKING THE TALK

The beginnings of a cybersecurity lexicon

V

Virus

Malware designed to infect and corrupt a computer and to copy itself. Viruses can disrupt programs installed on a computer.

VoIP

The routing of real-time voice conversations (telephone calls) over the internet rather than over an analogue or circuit-switched network.

W

Whaling

Whaling is a type of email fraud targeting high-profile end users like C-level corporate executives.

Wi-fi

A set of wireless communication protocols that can transmit traffic to wi-fi-enabled devices within a local area. A wi-fi-enabled device such as a laptop or mobile device can connect to the internet when within range of a wireless network connected to the internet. An area covered by one or more wi-fi access points is commonly called a hotspot.

Worm

A self-replicating virus that does not alter files but resides in active memory and duplicates itself.

Z

Zombie

A compromised computer. See Bot.

MailGuard	MailGuard.com.au MailGuard.com.au/blog MailGuard.com.au/cybersecuritychecklist
Australian Government Bodies & Resources	www.acsc.gov.au www.scamwatch.gov.au www.cert.gov.au www.staysmartonline.gov.au www.acorn.gov.au www.moneysmart.gov.au/scams www.afp.gov.au
International Associations	www.isaca.org www.enisa.europa.eu


"MailGuard has developed world leading cloud and email security"
The Hon. Malcolm Turnbull MP
Prime Minister of Australia[17]

About my company, MailGuard

MailGuard is one of Australia's leading technological innovators and the world's foremost cloud email and web security service, providing complete protection for businesses around the world against email and web security threats such as malware, ransomware, spyware, phishing, spear-phishing, whaling, viruses, spam and similar malicious scams.

MailGuard is different to traditional antivirus. A cloud-based email and web solution, it partners with smart Hybrid AI threat-detection engines that predict, learn and anticipate new threats as they're emerging. This cloud-based layer of security means MailGuard can apply immediate protection against emerging threats. MailGuard is 2-48 hours ahead of the market preventing fast-breaking zero-day attacks.

Because cybercrime never stops evolving, MailGuard continues to invest more than 40% of its revenues back into research and development every year. MailGuard will shortly release the next-generation Artificial Neural Network (ANN), a new frontier in threat detection, developed in collaboration with Deakin University and the Centre for Cyber Security Research.

MailGuard has partnerships with some of the world's largest email hosting providers, and works collaboratively alongside industry leaders including Microsoft, KPMG, Deakin University and Xero. MailGuard is a member of the Centre for Cyber Security Research (CCSR) and is CSA STAR accredited. MailGuard was recognised by ANZIA at the Australia & New Zealand Internet Awards, as the winner of the 2016 Security Award.

www.MailGuard.com.au

Referencing

1, 4, 7, 9, 11, 21, 23, 27, 31. Barack Obama, President of the United States of America. Remarks by the President at the Cybersecurity and Consumer Protection Summit at Stanford University, 13 February 2015, in San Francisco, CA.

2, 10. Craig McDonald, CEO & Founder, MailGuard. www.MailGuard.com.au/blog, 4 October 2016

22. Craig McDonald, CEO & Founder, MailGuard. www.MailGuard.com.au/blog, 1 August 2016

3, 5, 6, 8, 15, 16, 17, 25, 33, 34, 35, 36. The Hon. Malcolm Turnbull MP, Prime Minister of Australia. Keynote address at the Australia-US Cyber Security Dialogue Center for Strategic and International Studies on 22 September 2016 in Washington D.C.

12, 13, 14, 20, 28, 29. Robert S. Mueller, III, Director, Federal Bureau of Investigation (FBI). Speaking at the RSA Cyber Security Conference on 1 March 2012 in San Francisco, CA.

18, 37. Warren Buffet, Businessman, Investor & Philanthropist. Attributed to Warren Buffet by forbes.com in the article 'The Three Essential Warren Buffett Quotes To Live By' on 20 April 2014.

19. Jeff Bezos, CEO & Founder, Amazon. Attributed to Jeff Bezos by forbes.com in the article 'The Most Damaging Myth About Branding' on 6 September 2016.

38. Elon Musk, CEO & Founder, Tesla and SpaceX. Article in www.wired.com entitled 'Elon Musk's Mission to Mars' on 21 October 2012.

30. Bill Gates, Founder of Microsoft. ABC News interview. One-on-One with Bill Gates, Redmond, Wash., 16 February 2005.

Referencing

39. Hon. Dan Tehan MP, Minister Assisting the Prime Minister for Cyber Security. Speaking at the launch of 2016 Stay Smart Online Week at the National Library of Australia on 10 October 2016.

40. www.radacati.com. Email statistics report 2015-2019.

41. www.wearesocial.com. Digital in 2016 report published 27 January 2016.

42. Cisco VNI 2016.

43, 44, 45. www.cybersecurityventures.com Cybersecurity Ventures Report, 2016.

46, 47, 48. Extract from the Internet Organised Crime Threat Assessment (IOCTA), published by Europol's European Cybercrime Centre (EC3), describing the commercialisation of cybercrime.

49, 50. www.darkreading.com article and the Kaspersky Lab 2015 report, listed on 20 November 2015.

52. www.wired.com article 'Hacker Lexicon: What are phishing and spear phishing?' published 7 April 2015

53. http://theemergingfuture.com/disruptive-technology.htm

55. http://resources.infosecinstitute.com/cyber-criminal-ecosystems-in-the-deep-web/

56. http://www.reuters.com/article/yahoo-cyber-questions-idUSL2N1BZ1X3

Referencing

57. http://www.businessinsider.com/cyber-thieves-took-data-on-145-million-ebay-customers-by-hacking-3-corporate-employees-2014-5?IR=T

58. http://www.darkreading.com/attacks-and-breaches/target-breach-phishing-attack-implicated/d/d-id/1113829

59. http://fortune.com/2015/08/10/ubiquiti-networks-email-scam-40-million/

60. http://www.businessinsider.com/97-of-consumers-cant-always-identify-email-scams-2015-6?IR=T

61. http://gizmodo.com/the-number-of-people-who-fall-for-phishing-emails-is-st-1697725476

62. https://blog.knowbe4.com/paychex-60-of-hacked-smbs-are-out-of-business-6-months-later

63. https://www.communications.gov.au/sites/g/files/net301/f/Cost%20of%20cybercrime_INFOGRAPHIC_WEB_published_08102015.pdf

64. https://blog.digicert.com/dont-get-caught-phishing-scams/

65. http://www.riskmanagementmonitor.com/ransomware-threats-jump-300/

66. https://securelist.com/analysis/monthly-spam-reports/66297/spam-in-july-2014/

67. https://blog.cloudmark.com/2016/01/13/survey-spear-phishing-a-top-security-concern-to-enterprises/

A non-technical insight into cybersecurity for time-poor executives. In less than 60 minutes, McDonald provides an understanding of cybersecurity and what it means for your organisation, highlighting real-world examples and the risks facing every organisation.

"Knowledge of cybersecurity issues is essential for all executives irrespective of the business they are in. This guide puts the current state of cybersecurity into perspective with deep insights from visionaries in government and commerce, and offers practical advice on defining and protecting critical assets."

Bradley Bastow
Chief Technology Officer, Department of Prime Minister and Cabinet

"Being aware of cybersecurity threats and legal obligations is an essential consideration for all businesses. Craig's book is a must-read for all business owners and senior executives, and helps simplify a significant and little-understood risk to business."

Erhan Karabardak
Director, Cooper Mills Lawyers

"Effective cybersecurity has become a key foundation for the digital transformation initiatives of government and businesses. This guide provides a clear assessment of the threat, while providing a set of very practical steps that executive leaders can take to build a modern, resilient platform for their business innovation."

James Kavanagh
National Technology Officer, Microsoft Australia

"Outstanding. This book is a must-read for every executive. Cybercrime poses a serious threat to every business, large and small. No longer just an IT problem; all executives must comprehend the risks. Cyber attacks lead to serious business disruption, reputational damage and financial loss. It's the responsibility of every executive, and this book provides a thorough foundation for understanding the cybersecurity landscape."

Pip Marlow
Managing Director, Microsoft

"Gone are the days when cybercrime was simply a matter for IT professionals. In today's world, cybersecurity is an important issue for all leaders and managers at all levels of all organisations. If you value business continuity and strategic growth for your organisation, then *Surviving the Rise of Cybercrime* is a must-read for all executives."

Professor Gary Martin FAIM FACE
Chief Executive Officer, Australian Institute of Management, Western Australia.

ISBN 978-0-646-96612-0
9 780646 966120

RRP $29.95

survivingcybercrime.com