November 2016

Cybersecurity

Threats
Challenges
Opportunities

Preview

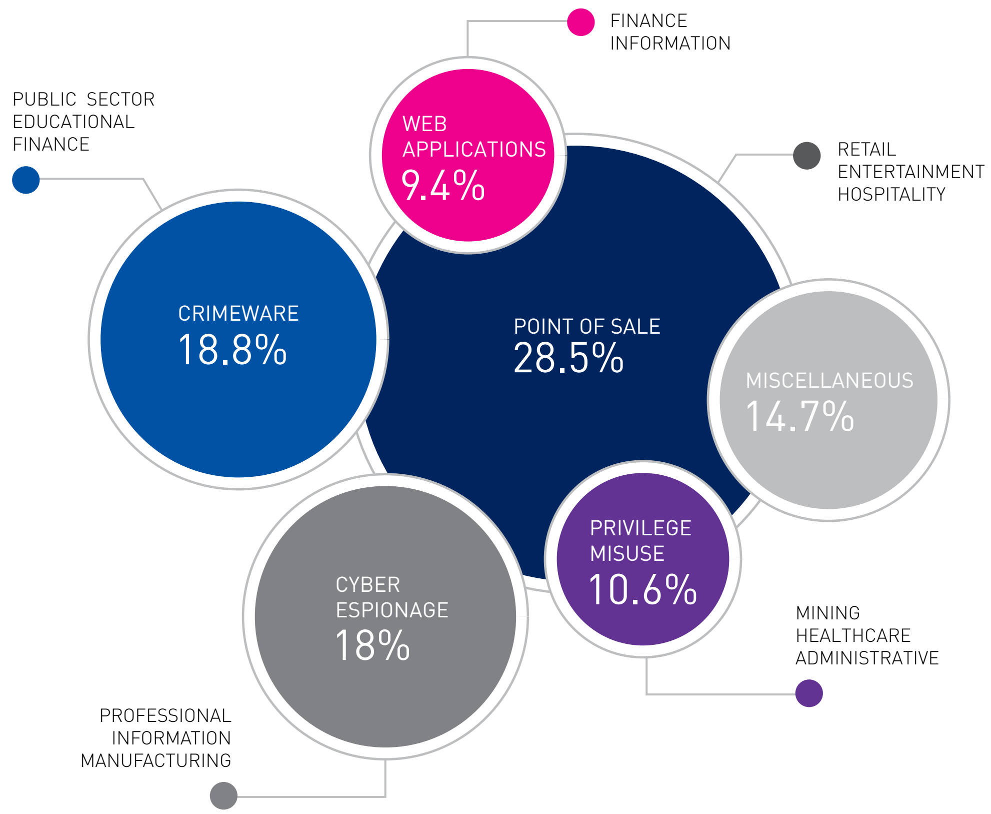
Download the full version at:
acs.org.au/insightsandpublications/publications.html

46%

OF THE WORLD'S POPULATION IS CONNECTED TO THE INTERNET

THREAT VECTORS BY INDUSTRY

The vectors by which industries are compromised.
Source: Verizon 2015 Data Breach Investigations Report



What is cybersecurity?

As with any technological advance throughout history, whenever new opportunities are created, there will always be those that exploit them for their own gain.

Despite the threat of viruses and malware almost since the dawn of computing, awareness of the security and sanctity of data with computer systems didn't gain traction until the explosive growth of the internet, whereby the exposure of so many machines on the web provided a veritable playground for hackers to test their skills – bringing down websites, stealing data, or committing fraud. It's something we now call **cybercrime**.

Since then, and with internet penetration globally at an estimated 3.4 billion users (approximately 46% of the world's population), the opportunities for cybercrime have ballooned exponentially.

Combating this is a multi-disciplinary affair that spans hardware and software through to policy and people – all of it aimed at both preventing cybercrime occurring in the first place, or minimising its impact when it does. This is the practice of **cybersecurity**.

There is no silver bullet, however; cybersecurity is a constantly evolving, constantly active process just like the threats it aims to prevent.

What happens when security fails? While what frequently makes the news are breaches of user accounts and the publication of names and passwords – the type that the Ashley Madison hack publicly exemplified – it's often financial gain, or the theft of critical business or government intelligence, that drives the cyber underworld.

One fact remains clear: it's only going to increase. As we integrate technology further into our lives, the opportunities for abuse grow. So too, then, must the defences we employ to stop them through the education and practice of cybersecurity.

The increasing prevalence and severity of malicious cyber-enabled activities... constitute an unusual and extraordinary threat to the national security, foreign policy and economy of the United States. I hereby declare a national emergency to deal with this threat.

Barack Obama,
President of the United States

Through the looking glass

The following is a snapshot – just a sample – of the stories that made the news during the production of this guide. These headlines give you an insight to the ongoing, every day, occurrences of what happens in the absence of cybersecurity.

The US government has increased its annual cybersecurity budget by 35%, going from $14 billion budgeted in 2016 to $19 billion in 2017. This is a sign of the times and there's no end in sight. Incremental increases in cybersecurity spending are not enough. We expect businesses of all sizes and types, and govern-ments globally, to double down on cyber protection.

Cybersecurity Ventures

'LINKEDIN USER? YOUR DATA MAY BE UP FOR SALE'

'EASYDOC MALWARE ADDS TOR BACKDOOR TO MACS FOR BOTNET CONTROL'

'LIZARDSTRESSER BOTNETS USING WEBCAMS, IOT GADGETS TO LAUNCH DDOS ATTACKS'

'DDOS ATTACK TAKES DOWN US CONGRESS WEBSITE FOR THREE DAYS'

'HACKERS FIND 138 SECURITY GAPS IN PENTAGON WEBSITES'

'HACKER STEALS 45 MILLION ACCOUNTS FROM HUNDREDS OF CAR, TECH, SPORTS FORUMS'

'10 MILLION ANDROID DEVICES REPORTEDLY INFECTED WITH CHINESE MALWARE'

'THIEVES GO HIGH-TECH TO STEAL CARS'

'CROOKS ARE WINNING THE 'CYBER ARMS RACE', ADMIT COPS'

'A HACK WILL KILL SOMEONE WITHIN 10 YEARS AND IT MAY HAVE ALREADY HAPPENED'

'CHINA HACKED US BANKING REGULATOR'

'APPLE DEVICES HELD FOR RANSOM, RUMOURS CLAIM 40M ICLOUD ACCOUNTS HACKED'

'RESEARCHERS DISCOVER TOR NODES DESIGNED TO SPY ON HIDDEN SERVICES'

'RESEARCHERS FOUND A HACKING TOOL THAT TARGETS ENERGY GRIDS ON THE DARK WEB'

'CITING ATTACK, GOTOMYPC RESETS ALL PASSWORDS'

'POLITICAL PARTY'S VIDEO CONFERENCE SYSTEM HACKED, ALLOWED SPYING ON DEMAND'

'ONLINE BACKUP FIRM CARBONITE TELLS USERS TO CHANGE THEIR PASSWORDS NOW'

'ANDROID RANSOMWARE HITS SMART TVS'

'HACKERS CAN USE SMART WATCH MOVEMENTS TO REVEAL A WEARER'S ATM PIN'

'IDENTITY FRAUD UP BY 57% AS THIEVES 'HUNT' ON SOCIAL MEDIA'

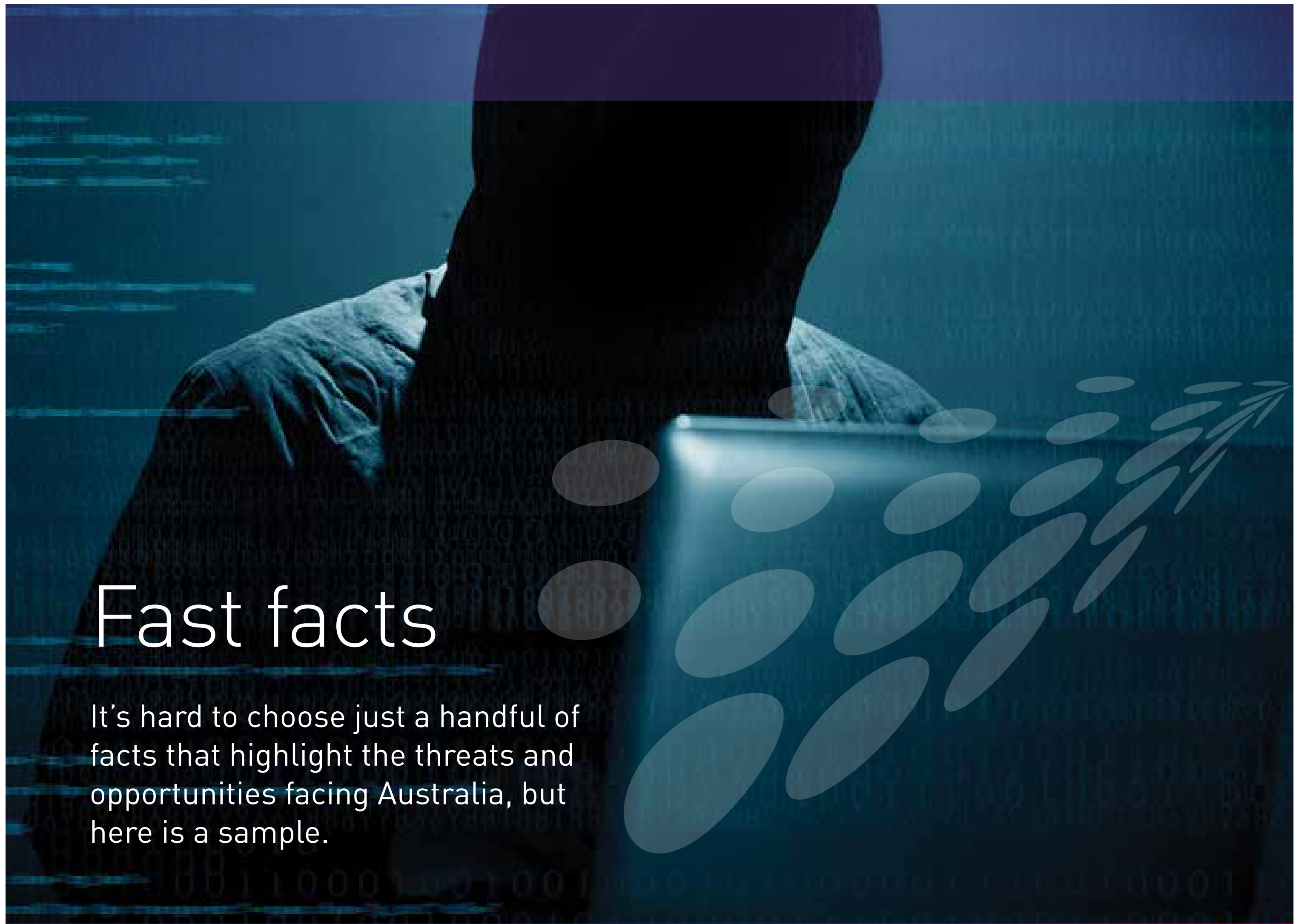
'WHY YOU SHOULD DELETE THE ONLINE ACCOUNTS YOU DON'T USE ANYMORE – RIGHT NOW'

'MASSIVE DDOS ATTACKS REACH RECORD LEVELS'

'HACKER DEMONSTRATES HOW VOTING MACHINES CAN BE COMPROMISED'

'FTC WARNS CONSUMERS OF RENTAL CAR DATA THEFT RISK'

'YAHOO CONFIRMS MASSIVE DATA BREACH, 500 MILLION USERS IMPACTED'



Fast facts

It's hard to choose just a handful of facts that highlight the threats and opportunities facing Australia, but here is a sample.

THREATS

IN 2014-15 CERT (COMPUTER EMERGENCY RESPONSE TEAM) AUSTRALIA RESPONDED TO

11,733

INCIDENTS, 218 OF WHICH INVOLVED SYSTEMS OF NATIONAL INTEREST OR CRITICAL INFRASTRUCTURE. OF THESE, ENERGY, BANKING AND FINANCE, AND COMMUNICATIONS WERE THE TOP THREE TARGETS.

THE AUSTRALIAN GOVERNMENT DEPARTMENT OF COMMUNICATIONS HAS REPORTED THAT THE AVERAGE COST OF A CYBERCRIME ATTACK TO A BUSINESS IS AROUND

$276,000

THE WORLD ECONOMIC FORUM'S GLOBAL RISKS 2015 REPORT HIGHLIGHTED CYBERATTACKS AND THREATS AS ONE OF THE MOST LIKELY HIGH-IMPACT RISKS. IN THE UNITED STATES, FOR EXAMPLE, CYBER CRIME ALREADY COSTS AN ESTIMATED

$US100

BILLION A YEAR.

IOT SENSORS AND DEVICES ARE EXPECTED TO EXCEED MOBILE PHONES AS THE LARGEST CATEGORY OF CONNECTED DEVICES IN 2018, GROWING AT A

23%

COMPOUND ANNUAL GROWTH RATE (CAGR) FROM 2015 TO 2021. SOLID CYBERSECURITY POLICY MUST BE IN PLACE FOR THIS FUTURE.

CYBERSECURITY IS A BUSINESS ISSUE, NOT JUST A TECHNOLOGY ONE. IN A SURVEY OF CLOSE TO

4,000

COMPANY DIRECTORS IN AUSTRALIA, ROUGHLY ONLY HALF REPORTED TO BE CYBER LITERATE, AND OF CO-DIRECTORS ONLY

FIFTEEN

PERCENT CLASSED AS CYBER LITERATE. THERE IS A LACK OF KNOWLEDGE ABOUT CYBERSECURITY AT THE EXECUTIVE LEVEL IN MANY BUSINESSES IN AUSTRALIA.

OPPORTUNITIES

IN 2003 THE CYBERSECURITY INDUSTRY WAS TAGGED AT

$US2.5

BILLION TODAY THE GLOBAL CYBERSECURITY MARKET TOTALS MORE THAN $US106 BILLION. SOME ESTIMATES PEG THE SECTOR WILL BE WORTH $US639 BILLION BY 2023.

BY 2030 IT'S ESTIMATED DATA ANALYTICS, MOBILE INTERNET, CLOUD AND IOT COULD GENERATE $US625

BILLION

IN SALES PER YEAR IN APAC.

THE UK PUBLISHED ITS CYBER-SECURITY STRATEGY IN 2011 – SINCE THEN THE SECTOR ALMOST DOUBLED FROM TEN BILLION POUNDS TO

SEVENTEEN

BILLION POUNDS AND IS NOW RESPONSIBLE FOR EMPLOYING 100K PEOPLE.

THERE ARE

1,404

CYBERSECURITY VENDORS IN THE WORLD TODAY. AUSTRALIA SPORTS ONLY FIFTEEN. VENDORS BY COUNTRY: USA 827, ISRAEL 228, UK 76, INDIA 41, AUSTRALIA 15.

JOB ADVERTISEMENTS FOR CYBER-SECURITY ALONE HAVE GROWN

57%

IN THE LAST 12 MONTHS ACCORDING TO JOBS WEBSITE SEEK. NETWORK SECURITY CONSULTANTS WERE THE

SIXTH

MOST ADVERTISED ICT OCCUPATION ON LINKEDIN IN 2015.

SECURING AUSTRALIA'S FUTURE

At ACS we are passionate about the ICT profession being recognised as a driver of productivity, innovation and business – able to deliver real, tangible outcomes.

This year ACS celebrates 50 years of advancing ICT in Australia. Our founders and pioneers worked on the first innovative computers in government, academia and industry, and our members now work at the coalface of technology development across every industry.

In 2011, ACS brought together its own Cyber Taskforce from our 23,000 members to respond to the Federal Government's new cyber discussion paper, 'Connecting with Confidence', where we highlighted the need for ongoing co-ordination and a focus on developing the pipeline of cyber professionals.

To play our part in securing Australia's future, we continue to perform the role of trusted advisor to government, and deliver services to develop and identify ICT professionals you can trust, including through the Professional Standards Scheme that ensures professionals have the specialist skills business can rely upon.

ACS is part of the global federation of professional ICT societies, the International Federation for Information Processing (IFIP), and the first professional body to receive accreditation under the International Professional Practice Partnership (IP3) – providing a platform for accreditation for ICT professionals and mutual recognition across international boundaries. The ACS currently chairs IP3 and plays a leading role in the professionalism of the ICT workforce.

IP3 has since gained global attention after successful engagements at the World Summit on the Information Society (WSIS) Forum in Geneva and the United Nations in New York, where the importance of ICT professionalism was acknowledged by the UN General Assembly President in 2015.

In May 2016 the President of IFIP participated in the European Foresight Cyber Security Meeting where he advocated that professionalism of the ICT workforce is "a key element in building trustworthy and reliable systems" and that it is important to ensure that "cyber security and cyber resilience is also a duty of care of the individual ICT professional, in all stages of a system lifecycle".

As we move forward another 50 years, ACS will be there at the forefront meeting the challenges and opportunities of ICT, and supporting the growth and potential of ICT professionals in Australia.

ACS
Level 11
50 Carrington Street
Sydney NSW 2000

P: 02 9299 3666
F: 02 9299 3997
E: info@acs.org.au
W: www.acs.org.au