humanIT

Cyber Security

Reduce Risk
while Increasing Impact

humanIT

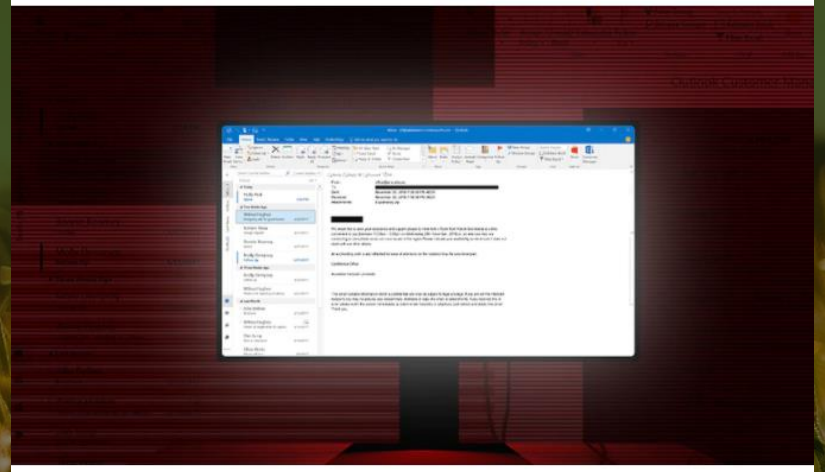
What's happing in the Cyber Security space?

Notable Events

What is a cyber attack, what are the targets and who is behind them? Inside the hacking attacks bombarding Australia

By Catherine Taylor

Posted Mon 29 Jun 2020 at 5:00am, updated Tue 30 Jun 2020 at 8:57am



Who are the hackers targeting Australia — and can we do anything to stop them? *(ABC News: Emma Machan)*

June 2020 – ABC News

a "sophisticated state-based cyber actor" had launched attacks earlier this month on "all levels of government, industry, political organisations, education, health, essential service providers and operators of other critical infrastructure".

the most significant and coordinated cyber-targeting against Australian institutions to date.

Australian corporations hit by massive Microsoft Server hack

Australia's cyber security watchdog has urgently warned Aussie corporations using Microsoft Exchange products to urgently patch their software after it was compromised by hackers.

CYBER ATTACK | 11:17am Mar 10, 2021

March 2021 - ABC News

7000 Australian Servers potentially compromised

Are Australians at a 'turning point' on cybersecurity or still unprepared?

By business reporter Nassim Khadem

Posted Mon 11 Jan 2021 at 5:52am

Australia is facing more frequent and sophisticated cyber attacks. *(ABC: Four Corners)*

January 2021 – ABC News

Federal Government launches $1.7 billion cybersecurity strategy aimed at preparing the nation against highly-sophisticated threats targeting critical networks to less-sophisticated but still damaging activities targeting small businesses and individuals.

humanIT

Cyberattacks are increasing in frequency and sophistication

An average of 164 cybercrime reports are made by Australians every day. ***1 every 10 minutes***

Between July 1, 2019 and June 30, 2020, the ACSC responded to 2,266 cybersecurity incidents and received 59,806 cybercrime reports. The most common category of cybercrime reported was fraud, which relates to criminals obtaining benefit through deception, such as investment, shopping, or romance scams.

Ransomware has become the biggest threat, used by criminals to lock up people's systems and data and then demand a ransom in return for their release

humanIT

Source: Australian Cyber Security Centre (ACSC)

The Real Cost of Data Breaches

Penalties aside, the cost of data breaches to reputation and lost revenue are significant

Brand Reputation Costs

94% of Australian Consumers believe Trust is more important than Convenience[1]

89% of Consumers would avoid doing business with companies that they think **do not** protect the privacy online[2]

60% of Australians have decided **not to deal with** a company due to Privacy concerns[3]

Lost Revenue

A single data breach costs[4]

An average of $158 USD per record compromised in administration and remedial services

An average of 23% customer churn after each privacy breach

1. Deloitte Australian Privacy Index 2016
2. PwC Outlook June 2014
3. OAIC Community Attitude to Privacy Survey 2013
4. IBM Cost of Data Breach Study, 2016

humanIT

Who are the Cyber Criminals?

Essentially there are two types of Cybercriminals

Lone actors, motivated by financial gain

- bounty hunters, who scour the dark web for paid opportunities. There are markets for illegal cyber information. A message on the dark web might offer a bounty for a piece of specific information.
- look to look to take small sums from thousands of credit cards
- use Ransomware to lockup your systems and demand a ransom.

Advanced Persistent Threats

- Cyber espionage is being linked more and more frequently to named groups with links to specific nations such as Ireland, Iran, China and Russia.
- State backed, well resourced groups, seeking to wreak havoc on our government, institutions, and private sector

humanIT

What do Cybercriminals want?

At one end of the spectrum, there are opportunistic cybercriminals who target Australia and Australian companies for financial gain, the Bounty Hunters.

And at the other end of the same spectrum, there are sophisticated and very well-resourced state-based actors who are seeking to interfere in our nation, the Advanced Persistent Threats.

1. **Your Trust Relationships**
   The average person can become collateral damage in the cyber spy's search for information. They are not after you. They are after your ‘trust relationship’ with someone higher up. They use you as a pivot point to leapfrog through the system with relative impunity."

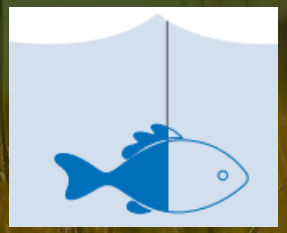
2. Some of the bounty hunters out there want to take small sums from thousands of credit cards and make a killing.

   There are also cyber criminals who will dump ransomware on a computer in order to destroy a small-to-medium-sized company unless they pay up.

humanIT

What do cyberattacks look like?

Attacks typically rely heavily on phishing emails to get a toehold in the network. They take advantage of timely topics, such as healthcare enrollment or climate change, to increase the chances someone will click a link or open an attachment and download a Trojan, ransomware, or other malware.



Phishing

Remains an effective method for criminals to capture credentials and other sensitive data

A hacker gains access to a person's email and takes over a legitimate conversation, then forwards it to one of that person's friends or colleagues with a malicious payload attached.

The email is likely to get through any email filtering, and the recipient is likely to open it, since the conversation details are convincing.

humanIT

What do cyberattacks look like?

Malware / Ransomware

Malware
Malicious code designed to compromise computer systems usually delivered by an email attachment or clicking on a link to an unsafe website

Malware has become a favorite tool of nation-states, which employ (and, occasionally, lose control over) highly advanced, zero-day exploits to wreak havoc on businesses, governments, and organizations in general

Ransomware
Ransomware is a type of malware that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid.

Attackers are focusing their efforts on learning about a company and its infrastructure, including critical servers and backup locations. That way, they know which malware and exploits to use to increase the likelihood of success. These types of recon attacks are especially effective when targeting small and medium-sized businesses (SMBs) who are less prepared (i.e. no contingency plans, risk assessment structures, cyber insurance, etc.)

The average ransom amount is increasing. Many cases are now in excess of $40,000

humanIT

What do attacks look like?

Business Email Compromise (BEC)

This type of email fraud targets commercial, government, and nonprofit organisations by fraudulently representing a senior colleague or a trusted customer.

The email typically contains instructions to send money (especially via wire transfer) or release client data. BEC relies heavily on the inherent trust of employees in their senior executives and valued customers.

With patience, the random hack of someone's email account can lead to contacts and passwords that could deliver access to an entire company's network or — in the case of the 2019 attack on Australia, access into the heart of Government and key infrastructure.

Publishing giant Nikkei lost roughly $29 million after an employee of the Nikkei America subsidiary was tricked by scammers into sending funds to a bank account they controlled (Nov 2019).

AIG Insurance claims that BEC has overtaken ransomware and data breaches as the main reason companies filed a cyber-insurance claim last year.

humanIT

Source: 2020 Webroot Threat Report

humanIT

Building your Cyber Resilience

What actions do you need to take?

There is no silver bullet, there never has been, and there never will be.

But by implementing security layers that protect users and data though all the stages of an attack, it's possible to achieve a state of "cyber resilience"

– 2020 Webroot Threat Report

1

Cyber Security
Makes it much harder for adversaries to compromise systems.

2

Safe Data Practices
Protect your data and systems from human error
Detect and respond to security breaches

3

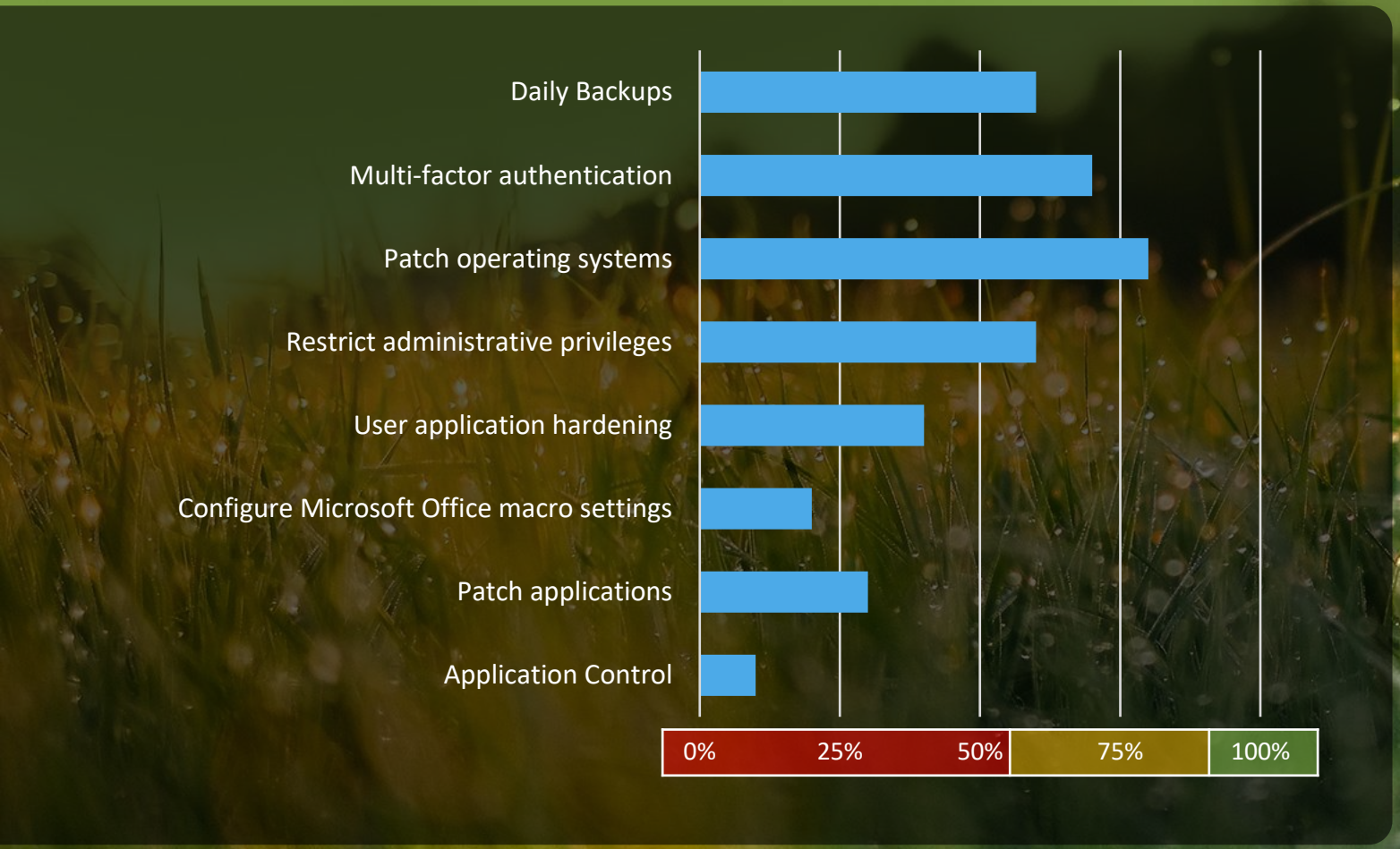
Information Security Governance
Oversight and Risk Management

humanIT

1

Cyber Security

Makes it much harder for adversaries to compromise systems



ACSC Australian Cyber Security Centre

The Essential Eight

No single mitigation strategy is guaranteed to prevent cyber security incidents.

The Australian Cyber Security Centre recommends organizations implement eight essential mitigation strategies as a baseline.

This baseline, known as the Essential Eight, makes it much harder for adversaries to compromise systems.

- Maturity Level One: Partly aligned with the intent of the mitigation strategy.
- Maturity Level Two: Mostly aligned with the intent of the mitigation strategy.
- Maturity Level Three: Fully aligned with the intent of the mitigation strategy.

humanIT

2

Safe Data Practices

Protect your data and systems from human error
Detect and respond to security breaches

Social engineering, such as phishing, are often the starting point for serious breaches. *Phishing URLs grew by 640% throughout 2020* (2020 Webroot Threat Report)

Security Awareness Training is key

The first line of defense are trained individuals to help protect sensitive data, intellectual property, and the viability of your organisation. This type of training is especially relevant in combatting *Business Email Compromise*

The OAIC received 539 data breach notifications from July to December 2020, an increase of 5% on the previous six months. Nearly two in five breaches were attributed to human error.

Source: Australian Cyber Security Centre (ACSC)

Running 11 or more short security awareness training sessions over 4-6 months reduces phishing click-through rates by 65%

(2020 Webroot Threat Report)

humanIT

3

Information Security Governance

Oversight and Risk Management

1. Embedded Cybersecurity into your risk management framework
2. Develop appropriate policies around Privacy, Information Security, Data Loss Prevention, Backup and Recovery, Business Continuity and Disaster Recovery, and a Data Breach Response Plan
3. Put Cyber Insurance in place
4. Ensure the identity and value of your systems, applications and information is determined and documented, especially Personally Identifiable Information Datasets
5. Apply to join the ACSC Partnership Program to receive threat alerts and advice to strengthen cyber defenses.

humanIT

Steps to take today

1. Start with the Essential Eight
2. Deliver Security Awareness Training
3. Develop your safe data practices
4. Build out your policies and governance practices

FREE TOOL

humanIT

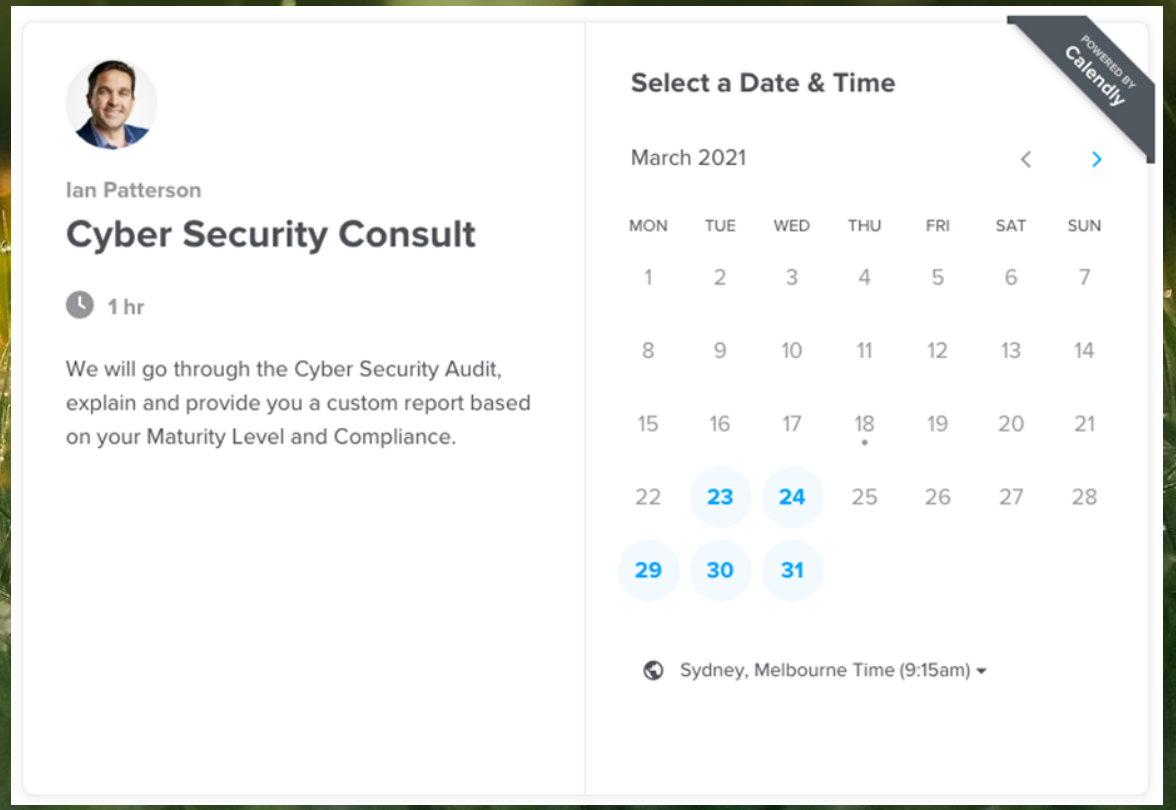
Essential Eight Self Assessment Tool

humanIT

Unsure what your next steps are?

Book a 15 minute no obligation call with our team

Click here to book your call



humanIT

Steps you should take if you have been compromised

- Identify if your organisation has been caught in the breach by using the Domain Search function on the Have I Been Pwned website.
- Reset passwords for affected users as a precaution.
- We recommend that you notify your users of the breach as they may have reused those passwords.
- Advise users that they can check if their accounts and passwords have been compromised via the Have I Been Pwned website.
- Your organisation should have multi-factor authentication enabled.
- We recommend you implement a policy whereby staff do not use their corporate credentials on public websites, and follow their workplace's security posture regulations.
- Check the Protecting Web Applications and Users and Secure Administration webpages contain a wealth of information that may be of assistance in securing your systems and networks.
- Review and implement the ACSC's Essential Eight Strategies to Mitigate Cyber Security Incidents where applicable.
- We also recommend you review any available logs for ongoing malicious activity.
- We strongly encourage ICT security staff to check Pastebin and similar password dumping sites on a regular basis for potential compromises of corporate credentials.

humanIT

Source: Australian Cyber Security Centre (ACSC)

humanIT

It is imperative Cyber Security forms part of your Technology Strategy

Increasing sustainability and driving greater social impact

Good technology governance is achieved through a set of practices that direct, measure and evaluate the use of IT resources to ensure strategic and operational outcomes are achieved and risk is well managed

Protect your brand reputation and client data by developing specific frameworks and practices that meet federal, state and international data protection and information security standards such as the NDB Scheme, VPDSS and GDPR.

Inform and empower your leaders to better manage sustainability and increase social impact by having on-demand access to integrated reports across the organisation

Ensure applications are fit-for-purpose, modernised, and integrated to create operational efficiencies and maximise your investment into service delivery

Enable your team to store, share and search for information from anywhere, and provide a platform for the team to communicate, collaborate and share ideas while reducing use of paper

Educate your team to use the technology well and stay productive; provide great support to get them back to work quickly when things do go wrong

Use technology to create awareness and connect with more people who need your services; engage funders, supporters, volunteers and attract talented and passionate staff

Step up the use of technology and digital assets in driving your purpose, vision and mission; increase your impact, boost customer engagement and create great experiences

Re-align your IT platform to support a cloud first strategy; proactively manage your IT platform to minimise service disruptions, keep IT secure, reliable, well performing and agile; mature your security practices to protect your data, your customers privacy, your brand reputation and enable compliance with increasing data security requirements

humanIT

Thank you

Ian Patterson
Director | Technology Strategist
m: 0412 959 998 head office: 1300 13 80 40
w: www.humanit.com.au e: ian.patterson@humanit.com.au