Essential Eight Makeover

How to marry E8 with contemporary Australian threats

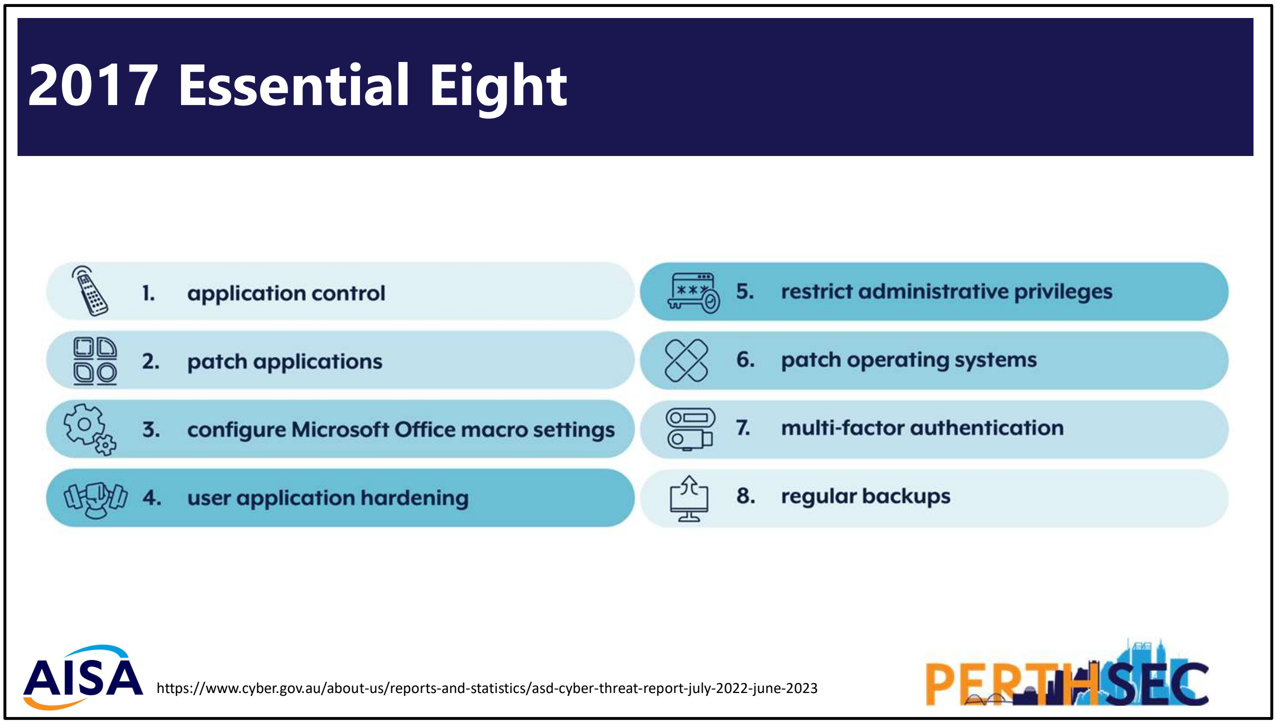
Shana Uhlmann CISO Minderoo Foundation & Tattarang
John Uhlmann Security Researcher Engineer @ Elastic

AISA
Cyber | smart · safe · secure

PERTHSEC

The Essential Eight is due, arguably overdue, for a refresh. So today we're going to look at some contemporary Australian statistics and compromises – and have a dinner-time conversation about how the E8 stacks up. It's a rare glimpse into how most nights pass in our household ;)

John was part of the ACSC working group that reviewed the Essential Eight *Maturity Model* in 2021, and Shana was responsible for implementing the E8 on ACSC systems. She now tackles E8, alongside risk management frameworks, in the real world. So hopefully this unique pairing of perspectives makes for an enjoyable session and helps you identify best value for money on a cyber roadmap, given the threats in the Australian eco-system today.



2017 Essential Eight

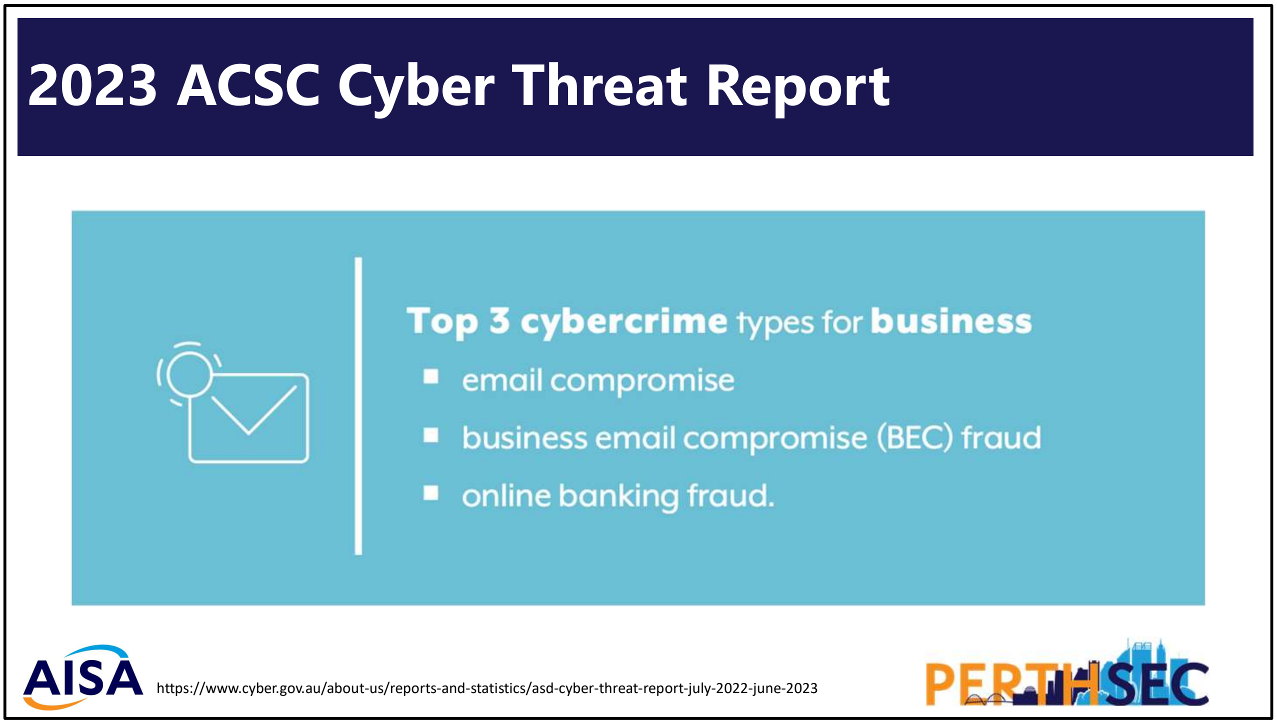
1. application control
2. patch applications
3. configure Microsoft Office macro settings
4. user application hardening
5. restrict administrative privileges
6. patch operating systems
7. multi-factor authentication
8. regular backups

AISA https://www.cyber.gov.au/about-us/reports-and-statistics/asd-cyber-threat-report-july-2022-june-2023 PERTHSEC

2010 – Strategies to Mitigate Cyber Security Incidents. Original Top 4 was App Control, Patch, Patch & Restrict Admin. The contemporary threat to government was internet to the workstation exploitation. (Internet Explorer, Flash, Java, Adobe).
2014 – Refresh to Strategies. No change to Top Four.
2017 – Refresh to Strategies. Essential Eight – added App Hardening (& Macros), MFA and backups.
2021 – No review of E8 composition. Only the Maturity Model was updated – to align with adversary maturity.

So, in 2023 we're working on 2017 advice where the primary threat was internet to the workstation – and especially Office Macros. Let's see what has changed in the environment since then and how E8 stacks up.

It's also worth noting that E8 was developed for your Enterprise Windows networks only. Not Mac. Not Linux. Not mobile. Not cloud. Not OT. Not customer-facing services. Not SMB. Not software developers.



2023 ACSC Cyber Threat Report

Top 3 cybercrime types for **business**

- email compromise
- business email compromise (BEC) fraud
- online banking fraud.

https://www.cyber.gov.au/about-us/reports-and-statistics/asd-cyber-threat-report-july-2022-june-2023

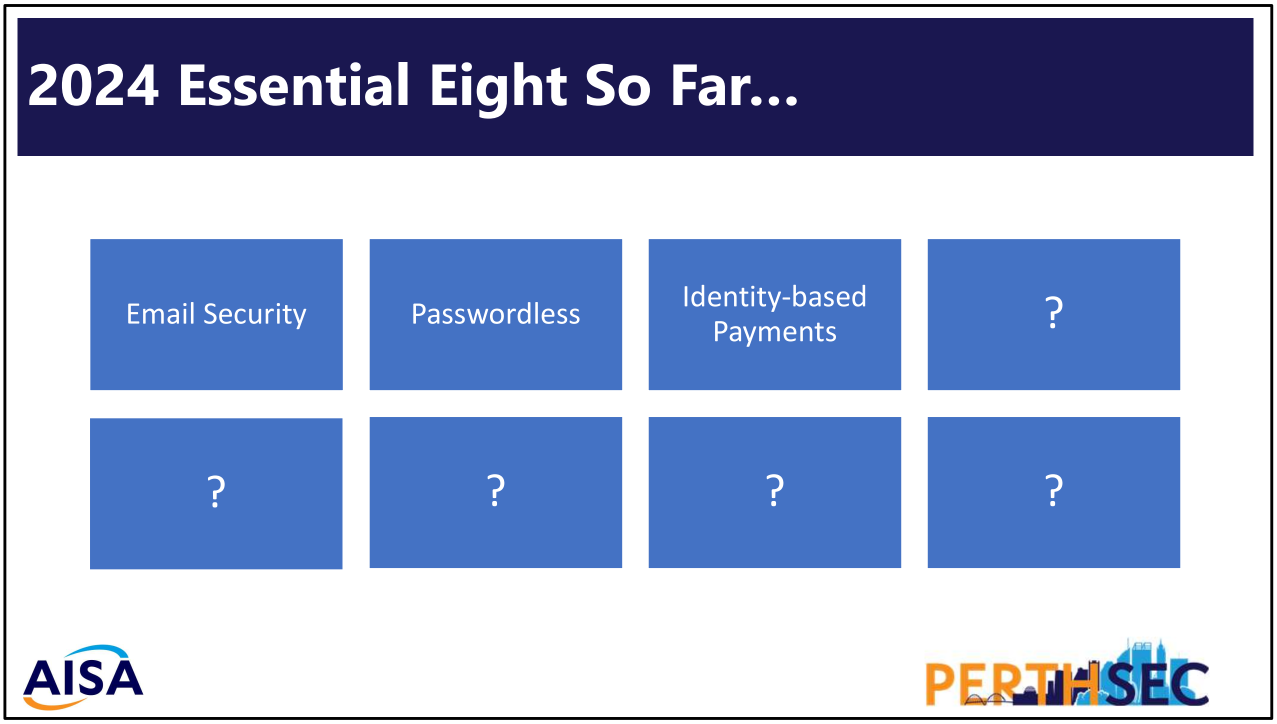
These are the top 3 reported cybercrimes for business in order of volume - which is not necessarily the same thing as impact.

For volume we want to knock these out quickly and preferably easily. It can be distracting noise. In right-sizing cyber security and choosing which locks to fit to your windows, a piece of dowel is acceptable if it effectively manages your risk to a suitable size value and is in budget. We shouldn't be aiming to stop everything, just reduce volume and big impact items.

The primary attacker technique is credential phishing. So, implement phishing-resistant authentication (aka passwordless). All modern laptops and mobile devices are already FIDO platform authenticators. Windows Hello for Business, FaceID, TouchID. Unfortunately, passwordless doesn't work for small business because of the password recovery process. We need Government to step in with appropriate digital identity. This is a key capability gap for Australia at the moment.

Secondly, you want to block spoofed emails – so SPF, DKIM and DMARC checks. This is table stakes for an Email Security product. Next, you want account takeover detection logic running over email authentication logs and you probably want an Email Security product that flags behavioural anomalies that might be BEC or other social engineering.

For BEC, you should strongly prefer to pay supplier invoices using an identity-based mechanism such as PayID via ABN. Secondly, you want to ensure that your supplier's email can't be hijacked – so phishing-resistant authentication and device hygiene. Did you catch the E8 nuance. You need your suppliers – not you – to be secure.



2024 Essential Eight So Far…

Email Security	Passwordless	Identity-based Payments	?
?	?	?	?

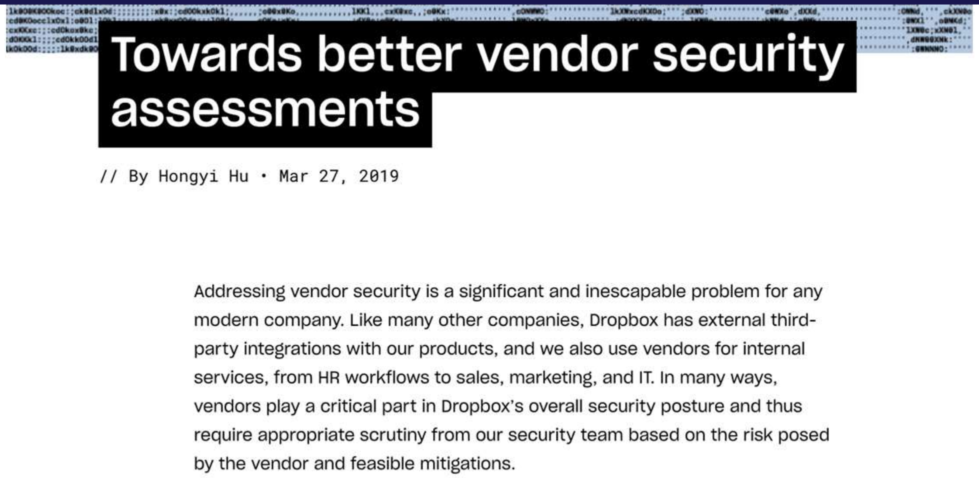
AISA

PERTHSEC

Essential controls so far:
Phishing resistant passwordless (aka MFA evolution)
Modern email security tool with behavioral analysis.
Identity-based payments especially ABN PayID for invoices.

Email Security is first – because it is simpler to implement.

Vendor Security?



Towards better vendor security assessments

// By Hongyi Hu • Mar 27, 2019

Addressing vendor security is a significant and inescapable problem for any modern company. Like many other companies, Dropbox has external third-party integrations with our products, and we also use vendors for internal services, from HR workflows to sales, marketing, and IT. In many ways, vendors play a critical part in Dropbox's overall security posture and thus require appropriate scrutiny from our security team based on the risk posed by the vendor and feasible mitigations.

https://dropbox.tech/security/towards-better-vendor-security-assessments

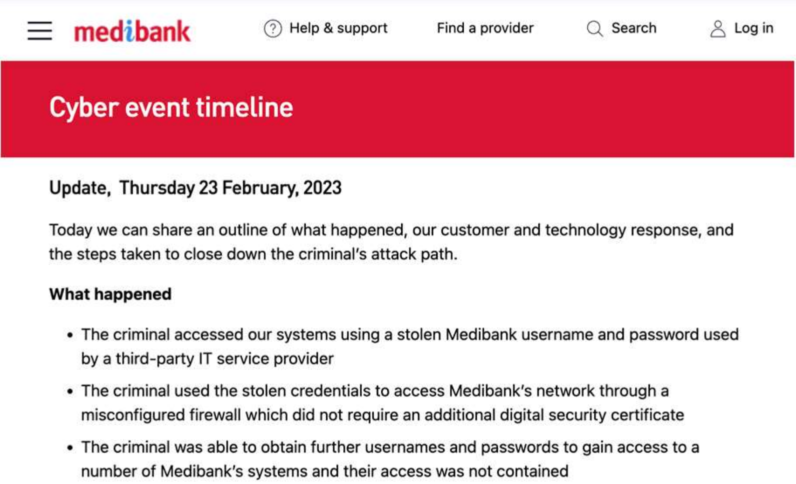
What remains exposed though in these top 3? There's only so much you can do about BEC when it manifests in your supply chain. So how to influence vendor security?

If your business model makes you a critical supply chain risk for your customers, then be like DropBox – and strongly vet all of your vendors.

If you are a larger organisation, consider adding super basic security hygiene requirements to all of your vendor contracts. (PayID, Passwordless, user device hygiene).

If you are a smaller organisation, hope that your vendors are too small to be targeted – or that they took a larger contract that required good hygiene.

Case Study: Medibank



Cyber event timeline

Update, Thursday 23 February, 2023

Today we can share an outline of what happened, our customer and technology response, and the steps taken to close down the criminal's attack path.

What happened

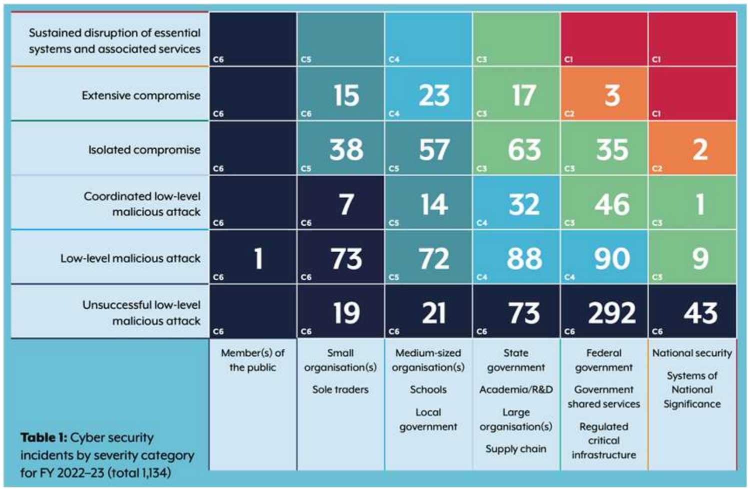
- The criminal accessed our systems using a stolen Medibank username and password used by a third-party IT service provider
- The criminal used the stolen credentials to access Medibank's network through a misconfigured firewall which did not require an additional digital security certificate
- The criminal was able to obtain further usernames and passwords to gain access to a number of Medibank's systems and their access was not contained

https://www.medibank.com.au/health-insurance/info/cyber-security/timeline

Because what's worse that your supplier being compromised and sending you fraudulent invoices?
Your IT service provider being compromised... and not having basic security practices in place.
In Medibank, the third-party IT service provider was not using pMFA for remote access.

We've just covered volume, now let's look at big impact ticket items.

2023 ACSC Cyber Threat Report



Sustained disruption of essential systems and associated services	C6	C5	C4	C3	C1	C1
Extensive compromise	C6	15 C6	23 C4	17 C3	3 C2	C1
Isolated compromise	C6	38 C5	57 C5	63 C3	35 C3	2 C2
Coordinated low-level malicious attack	C6	7 C6	14 C5	32 C4	46 C3	1 C3
Low-level malicious attack	1 C6	73 C6	72 C5	88 C4	90 C4	9 C3
Unsuccessful low-level malicious attack	C6	19 C6	21 C6	73 C6	292 C6	43 C6
Table 1: Cyber security incidents by severity category for FY 2022–23 (total 1,134)	Member(s) of the public	Small organisation(s) Sole traders	Medium-sized organisation(s) Schools Local government	State government Academia/R&D Large organisation(s) Supply chain	Federal government Government shared services Regulated critical infrastructure	National security Systems of National Significance

AISA https://www.cyber.gov.au/about-us/reports-and-statistics/asd-cyber-threat-report-july-2022-june-2023 PERTHSEC

The ACSC responded to over 1100 incidents in FY22/23 with C3 or above incidents remaining at about 15%, year on year. Let's break that down.

500 unsuccessful low-level attacks – okay, that's reporting kids riding on skateboards

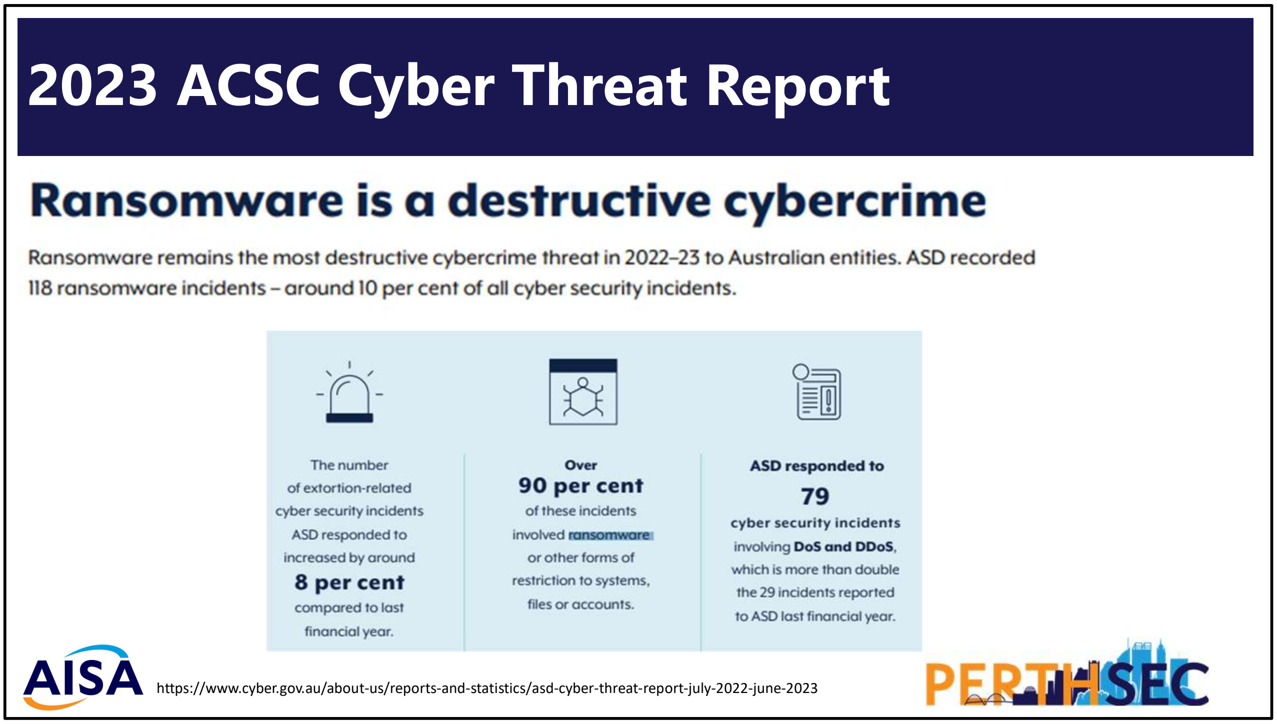
300 low-level malicious attacks – now we're reporting shoplifters and kids with spraycans.

100 coordinated low-level malicious attacks – now the kids are in street gangs.

200 isolated compromises – this is a great statistic. These organisations did everything right. Someone broke in through a window, but the alarm went off before further impact.

60 extensive compromises – this is where we need to focus our lessons learned. This is where our defence-in-depth failed.

All we have so far from the ACSC here is a single sentence - "Common activities leading to C3 incidents included exploitation of public–facing applications (20% or 34) and phishing (17% or 29)."



2023 ACSC Cyber Threat Report

Ransomware is a destructive cybercrime

Ransomware remains the most destructive cybercrime threat in 2022–23 to Australian entities. ASD recorded 118 ransomware incidents – around 10 per cent of all cyber security incidents.

The number of extortion-related cyber security incidents ASD responded to increased by around **8 per cent** compared to last financial year.

Over **90 per cent** of these incidents involved ransomware or other forms of restriction to systems, files or accounts.

ASD responded to **79** **cyber security incidents** involving **DoS and DDoS**, which is more than double the 29 incidents reported to ASD last financial year.

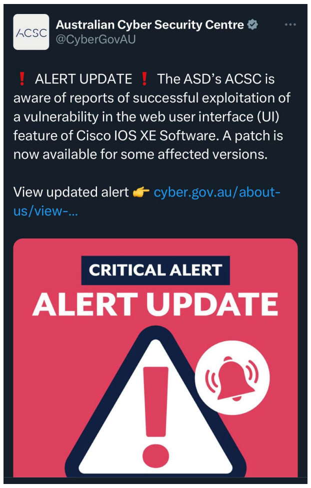
AISA https://www.cyber.gov.au/about-us/reports-and-statistics/asd-cyber-threat-report-july-2022-june-2023 PERTHSEC

The ACSC did not share a figure for ransomware impact. However, they recorded 118 r/ware incidents and notified 158 entities of r/ware activity on their networks.
The global average cost of a ransomware incident calculated by IBM is AUD$7 million. We don't have an Australian figure, but we can still estimate an upper bound on the impact as $800 million. So, as a nation, ransomware likely has the largest impact amongst the pure cybercrime types ($3Bn scam losses is cyber-enabled crime). But that's skewed by some very large organisations, and Australia is 2% of global ransomware.
The global average is 3 weeks of lost revenue. What does that mean to your organisation, and what business continuity plans can you put in place? You need to ask questions like these to determine which is the larger threat for you.

So, it's important enough to warrant some essential controls.
41% of data breaches was credential abuse (to access cloud services, local systems, entire networks), commonly using brute-force attacks on bad passwords or phishing.
This is covered already.

Next was remote exploitation (34% of data breaches), with known vulnerabilities often exploited.
Let's take a quick look at how these manifest – remote exploitation, users installing stuff, through case studies.

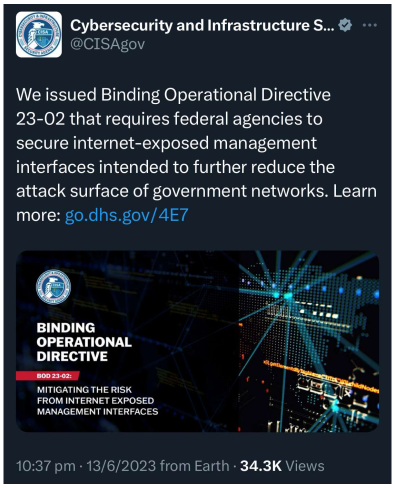
Case Study: Cisco IOS XE Vulnerability



Australian Cyber Security Centre
@CyberGovAU

❗ ALERT UPDATE ❗ The ASD's ACSC is aware of reports of successful exploitation of a vulnerability in the web user interface (UI) feature of Cisco IOS XE Software. A patch is now available for some affected versions.

View updated alert 👉 cyber.gov.au/about-us/view-...



Cybersecurity and Infrastructure S...
@CISAgov

We issued Binding Operational Directive 23-02 that requires federal agencies to secure internet-exposed management interfaces intended to further reduce the attack surface of government networks. Learn more: go.dhs.gov/4E7

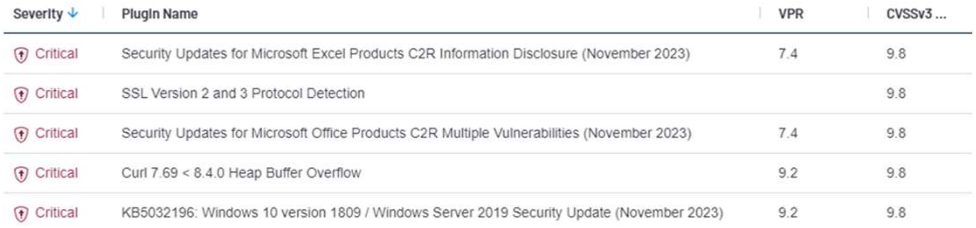
10:37 pm · 13/6/2023 from Earth · **34.3K** Views

https://twitter.com/CyberGovAU/status/1717076490368762173
https://twitter.com/CISAgov/status/1668628546338820096

Let's start with the current go to initial access technique for many ransomware families - exploitation of public–facing applications – especially via a known vulnerability. Basically, if you are on Shodan you're at risk.
The ACSC advice to you always to Patch, Patch and Patch some more. Patching is literally a quarter of the E8. It is also often the wrong advice, so we won't be starting with that control. Last month's vulnerability was in Cisco's management Web UI. That's not customer-facing… so why is it exposed on the internet at all?

According to the ACSC annual report, last FY saw a 25% increase in the number of publicly reported software vulnerabilities with 1/5 exploitable within 48 hours. Clearly a patch, patch, patch mentality isn't going to stack up. It isn't affordable, it creates severe user frustration, and most businesses don't have the capability to keep current. Is patching really the best answer? Quick sidestep to why patching doesn't work…

Case Study: Patching - Audience Participation



Severity ↓	Plugin Name	VPR	CVSSv3 ...
Critical	Security Updates for Microsoft Excel Products C2R Information Disclosure (November 2023)	7.4	9.8
Critical	SSL Version 2 and 3 Protocol Detection		9.8
Critical	Security Updates for Microsoft Office Products C2R Multiple Vulnerabilities (November 2023)	7.4	9.8
Critical	Curl 7.69 < 8.4.0 Heap Buffer Overflow	9.2	9.8
Critical	KB5032196: Windows 10 version 1809 / Windows Server 2019 Security Update (November 2023)	9.2	9.8

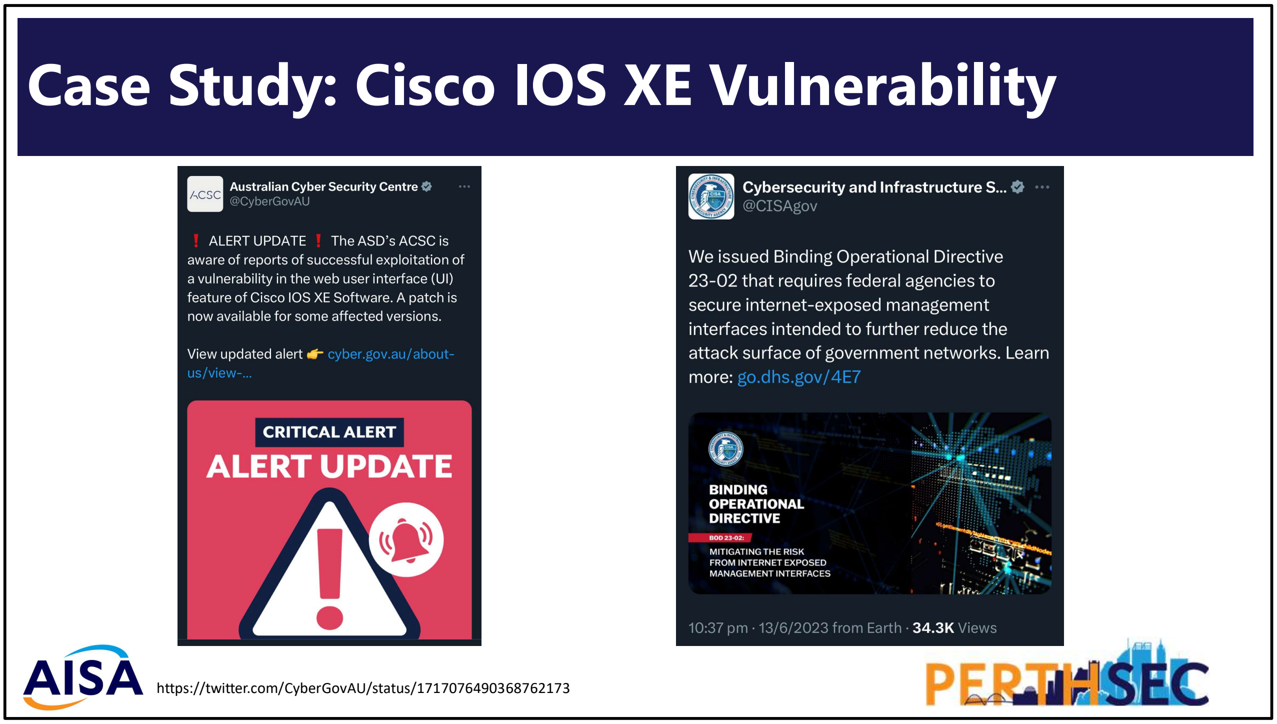
Reports like this are BaU for IT. What would you do with this?
TL;DR – none of these are 'drop everything and patch now' critical.

It's not that patching doesn't have any value – it's that the value does not scale linearly as more effort is applied.

We want people to patch. We just want them to patch at a healthy, sustainable cadence.

Of note, instances of exploitation of user applications (browsers & productivity suite) is currently low. But this is *because* we're patching (and because of sandboxing and other software quality improvements) – so keep doing this. So, focus patching only on software that is commonly exploited.

Let's call this control Focused Patching. Look at CISA's Known Exploited Vulnerability Catalog to see what products to include. In addition to browsers & productivity suite, we also need to consider network edge devices…
Which neatly brings us back to the Cisco Case Study…



Case Study: Cisco IOS XE Vulnerability

Australian Cyber Security Centre
@CyberGovAU

❗ ALERT UPDATE ❗ The ASD's ACSC is aware of reports of successful exploitation of a vulnerability in the web user interface (UI) feature of Cisco IOS XE Software. A patch is now available for some affected versions.

View updated alert 👉 cyber.gov.au/about-us/view-...

Cybersecurity and Infrastructure S...
@CISAgov

We issued Binding Operational Directive 23-02 that requires federal agencies to secure internet-exposed management interfaces intended to further reduce the attack surface of government networks. Learn more: go.dhs.gov/4E7

10:37 pm · 13/6/2023 from Earth · **34.3K** Views

https://twitter.com/CyberGovAU/status/1717076490368762173

As a counterpoint, CISA's advice here is more nuanced.
Step 1 is to reduce your internet-exposed attack surface.
And, specifically, management interfaces should never be internet-exposed.
Three low-cost options –
1. Place your management interfaces on an unguessable IPv6 address.
2. Use a modern WireGuard-based VPN. There is no discoverable service until after a cryptographic UDP port knock.
3. Place the management interface behind an identity aware proxy. This is the Zero Trust approach.

Step 2 is to increase the cost of exploitation. In general, SaaS products are more secure than COTS ones – because the adversary can't just buy a copy of the software and look for vulnerabilities. PaaS is just someone else's computer and doesn't necessarily offer security benefits. But the cloud is an excellent DMZ. You definitely want these devices in a DMZ. That's the network segmentation bit. It buys you time to detect if you haven't patched quickly enough.

Step 3 is then to consider patching cadence for exposed COTS software and disaster recovery as part of the total cost of ownership of an internet exposed service.
If it's a static website hosted in a container in the cloud – then who cares if I don't patch it that often. I can rebuild it at will.

Let's call this control Reduce Internet Exposure.

Case Study: Royal Ransomware

TLP: CLEAR

Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

2023-01: ACSC Ransomware Profile - **Royal**

24 January 2023

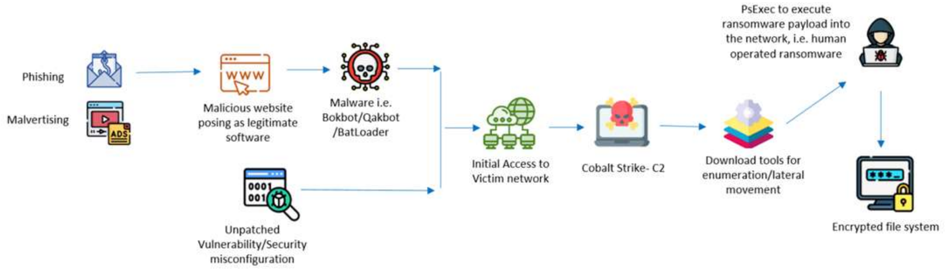

Phishing
Malvertising
ADS
WWW
Malicious website posing as legitimate software
Malware i.e. Bokbot/Qakbot /BatLoader
Unpatched Vulnerability/Security misconfiguration
0001
001
Initial Access to Victim network
Cobalt Strike- C2
Download tools for enumeration/lateral movement
PsExec to execute ransomware payload into the network, i.e. human operated ransomware
Encrypted file system

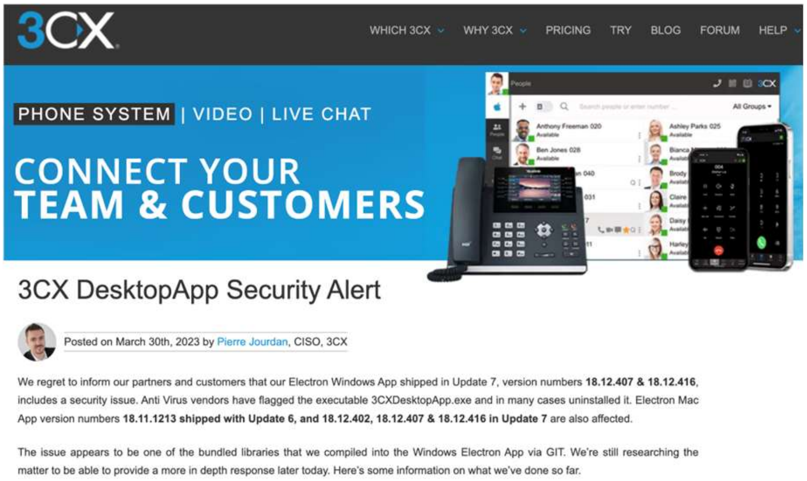
Figure-1: Royal Ransomware Infection Chain

https://www.cyber.gov.au/sites/default/files/2023-02/2023-01 - ACSC Ransomware Profile - Royal.pdf

The second initial access technique used for ransomware currently is tricking a user to download and run software.
The effectiveness of email security products is pushing actors to new delivery vectors – such as callback requests.
So, a vector agnostic approach of blocking **standard** users from downloading and/or double-clicking certain file types goes a very long way here.

Combine this 'just enough application control' with EDR for a more effective mitigation and blended user experience. More on EDR in a minute.
The gold standard, however, is still for standard users to only be able to run installed applications.
This is Application Control ML1 – not a full implementation. Just blocking (or even sandboxing) unauthorised software.

Case Study: 3CX


3CX
WHICH 3CX
WHY 3CX
PRICING
TRY
BLOG
FORUM
HELP
PHONE SYSTEM | VIDEO | LIVE CHAT
CONNECT YOUR TEAM & CUSTOMERS

3CX DesktopApp Security Alert

Posted on March 30th, 2023 by Pierre Jourdan, CISO, 3CX

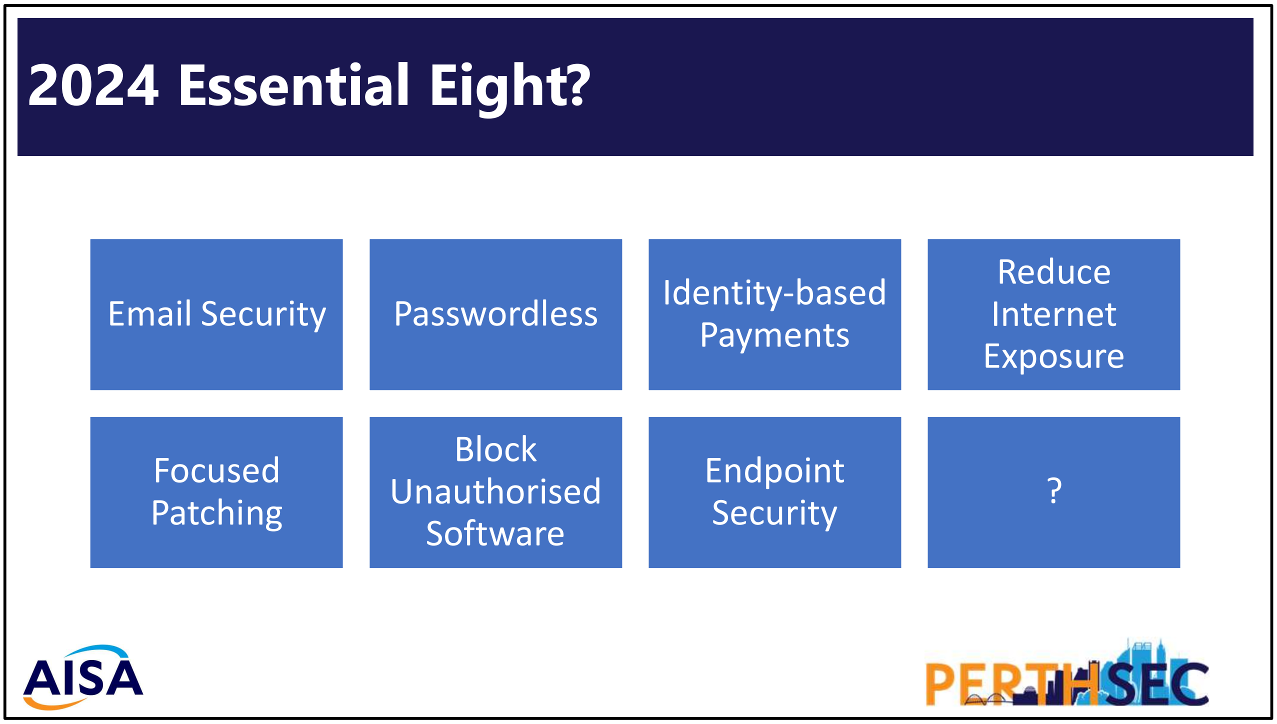
We regret to inform our partners and customers that our Electron Windows App shipped in Update 7, version numbers **18.12.407 & 18.12.416**, includes a security issue. Anti Virus vendors have flagged the executable 3CXDesktopApp.exe and in many cases uninstalled it. Electron Mac App version numbers **18.11.1213 shipped with Update 6, and 18.12.402, 18.12.407 & 18.12.416 in Update 7** are also affected.

The issue appears to be one of the bundled libraries that we compiled into the Windows Electron App via GIT. We're still researching the matter to be able to provide a more in depth response later today. Here's some information on what we've done so far.

https://www.3cx.com/blog/news/desktopapp-security-alert/

The final category to consider here is your supply chain – either via a managed service provider (Kayesa/Medibank) or privileged applications (3CX).
3CX customers that installed the "legitimate" software update were compromised.
The subsequent abnormal behaviour was then detected by endpoint security – not currently one of the E8, though arguably implied by the logging requirements in the 2021 maturity model update.
Literally none of the current E8 were relevant here. In fact, E8's aggressive patch recommendations would exacerbate exposure.
The mitigation here was to … not patch?
To be honest, patching anything that's not Microsoft, Google or Apple is always a business risk – hence focused patching.
I don't know your business – so I can't make that risk call for you.

So, our 7th Essential Control becomes Endpoint Security on enterprise IT assets.
From an investment perspective, Endpoint Security provides features across multiple risk management frameworks, it aids in prevention, detection, response and recovery activities… and if used properly, it helps enable users to do what they need to do while maintaining visibility and protection.

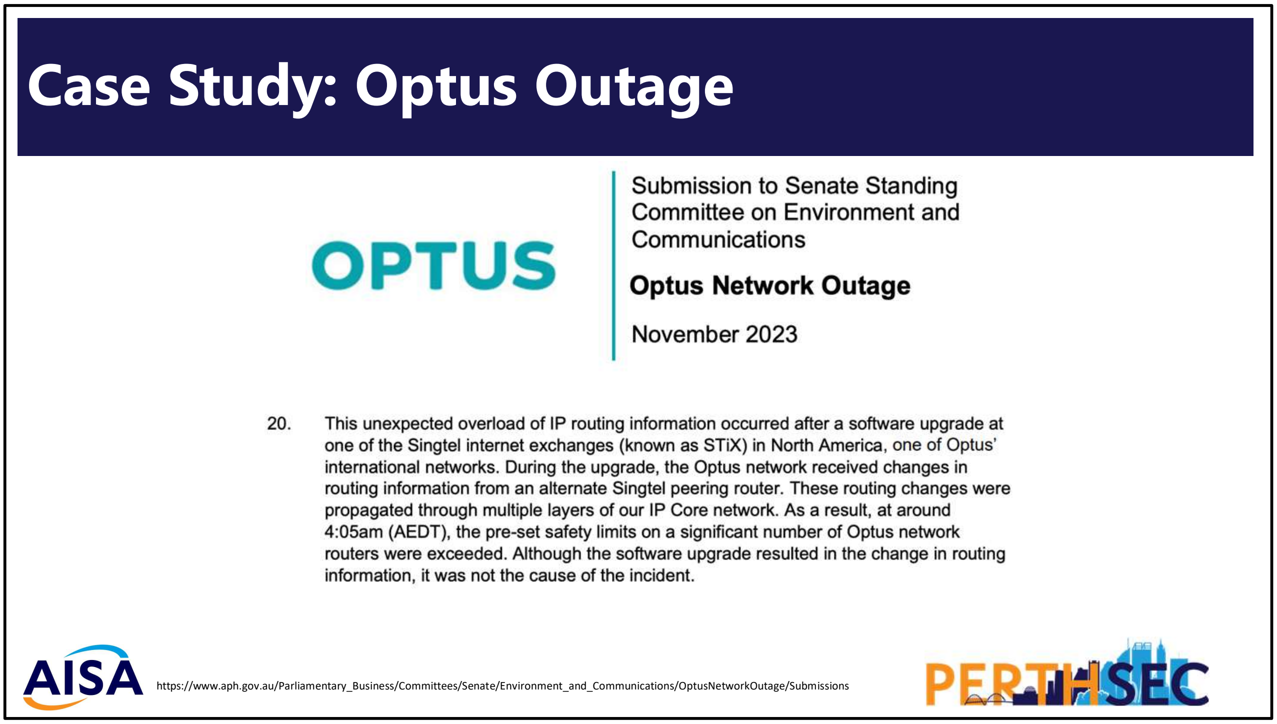


2024 Essential Eight?

Email Security	Passwordless	Identity-based Payments	Reduce Internet Exposure
Focused Patching	Block Unauthorised Software	Endpoint Security	?

So, here’s where we’re at so far, a 2024 Essential Eight might look something like this.

What’s missing?



Case Study: Optus Outage

OPTUS

Submission to Senate Standing Committee on Environment and Communications

Optus Network Outage

November 2023

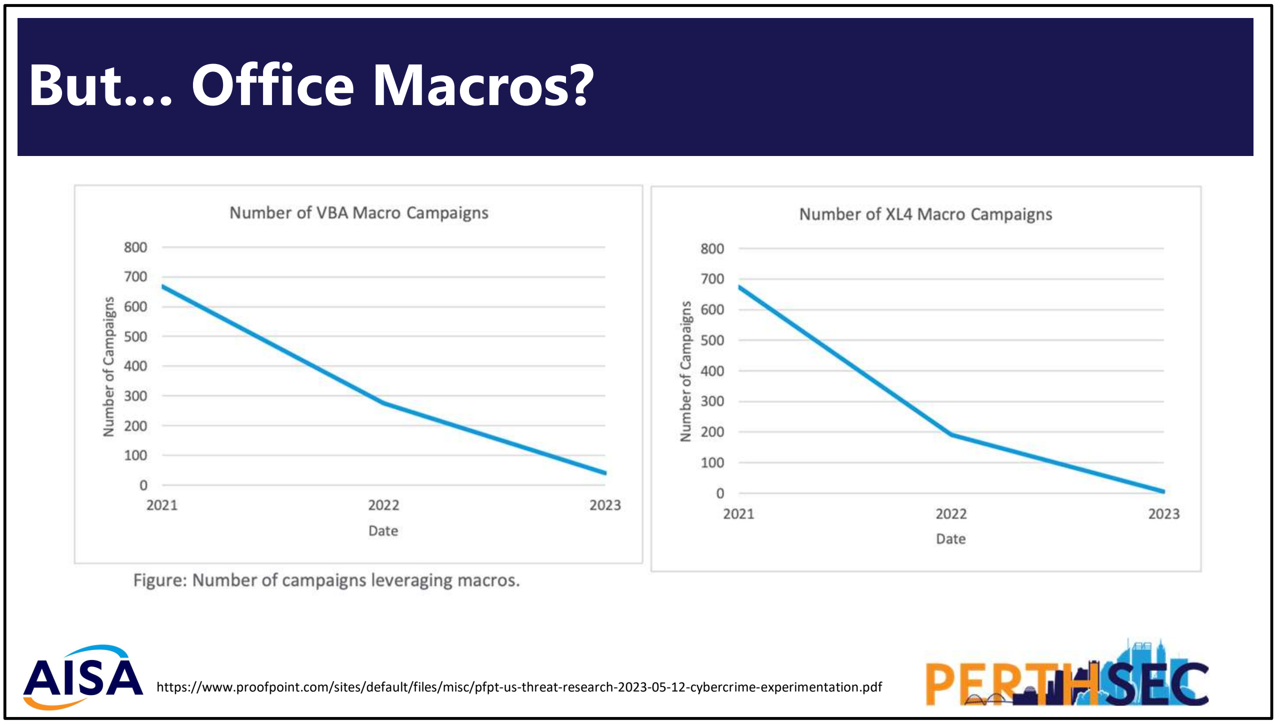
20. This unexpected overload of IP routing information occurred after a software upgrade at one of the Singtel internet exchanges (known as STiX) in North America, one of Optus' international networks. During the upgrade, the Optus network received changes in routing information from an alternate Singtel peering router. These routing changes were propagated through multiple layers of our IP Core network. As a result, at around 4:05am (AEDT), the pre-set safety limits on a significant number of Optus network routers were exceeded. Although the software upgrade resulted in the change in routing information, it was not the cause of the incident.

https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Environment_and_Communications/OptusNetworkOutage/Submissions

Finally, Business Continuity isn't just about cyber-attack.
The name of the game for commercial enterprises, is staying operational, not staying secure. So, it's worth comparing the nationwide potential $800M ransomware cost last year (self-estimated, not ACSC defined) to the $2Bn Optus outage last week (No reliable estimates of whole-of-economy costs, but Optus stock dropped by $2 billion).

And this was possibly triggered by a software upgrade in critical infrastructure.

Big business wasn't overly affected. They had business continuity plans.
Small business was. They can't afford to.
Two things: it doesn't have to be a cyber-attack to have big impact. BC plans are good for both scenarios.
Secondly, if software upgrade can do this in CI, should we really be demanding a patch, patch, patch mentality?
Reinforces, reduce your internet footprint, focused patching and have a BC plan.

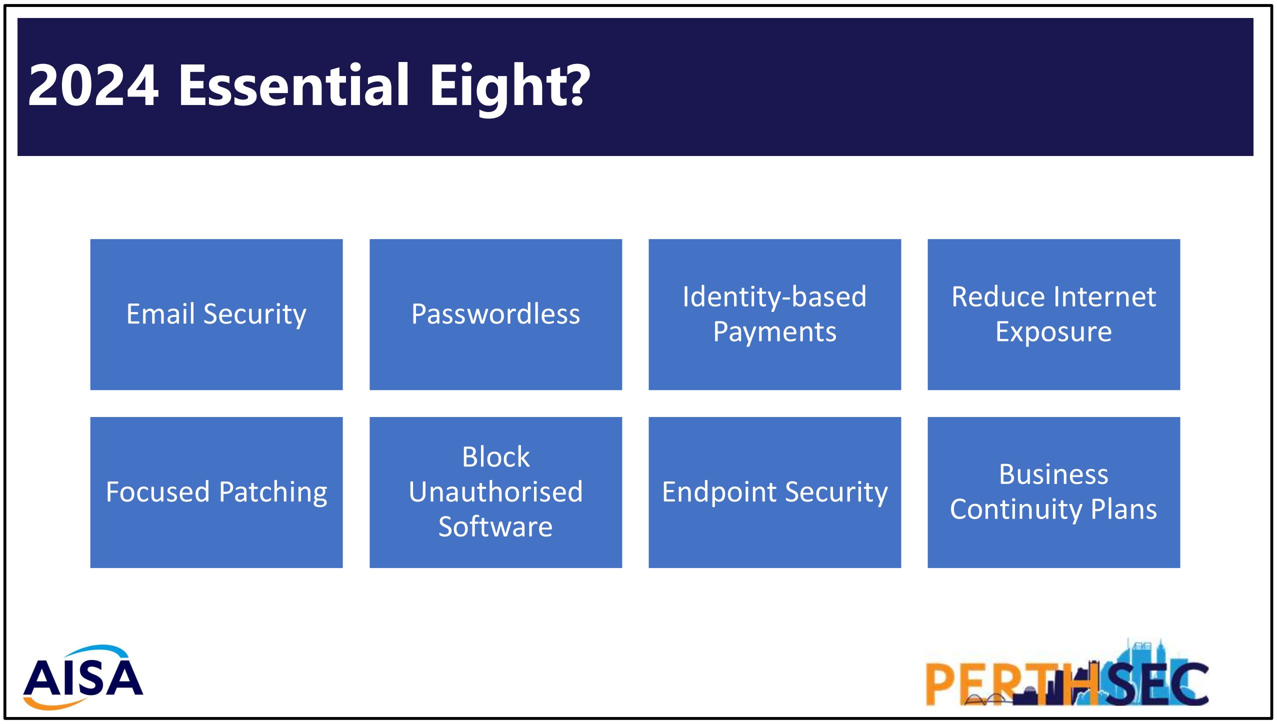


But… Office Macros?

Figure: Number of campaigns leveraging macros.

https://www.proofpoint.com/sites/default/files/misc/pfpt-us-threat-research-2023-05-12-cybercrime-experimentation.pdf

The graph says it all.



2024 Essential Eight?

Email Security

Passwordless

Identity-based Payments

Reduce Internet Exposure

Focused Patching

Block Unauthorised Software

Endpoint Security

Business Continuity Plans

AISA

PERTHSEC

So, this is what a 2024 update to the Essential Eight might look like.

We’re looking forward to seeing what the ACSC comes up with.