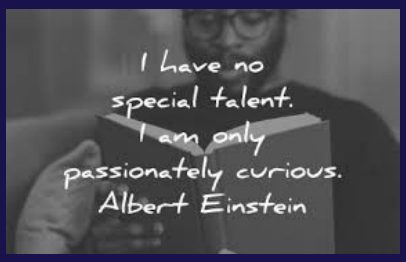
How to dissect cyber theatre and be deeply ~~technical~~ curious!



Shana Uhlmann (she/her) IT Director, CISO @ Tattarang
John Uhlmann (he/him) Security Researcher Engineer @ Elastic

AISA PERTHSEC

Another informal Uhlmann dinnertime conversation.

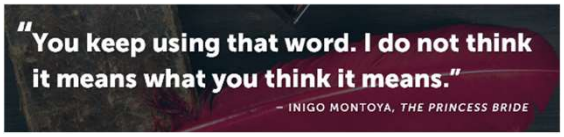
There are four themes for today
1. You cannot dissect cyber theatre by being technical.
2. You can be technically correct and wrong.
3. Curiosity is more powerful and useful.
4. Stop asking are you Technical and ask more open questions that drive innovation.

We're going to quickly review what being technical means, then what being curious means and why it's important.
We'll then run through some fun case studies to illustrate the difference.

We're going to also keep coming back to asking "Is this really the best/most critical advice right now?"

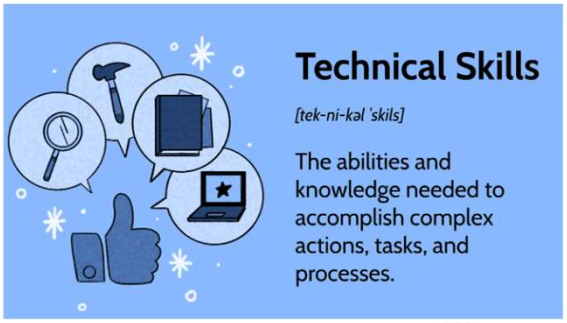
Measuring technical

adjective characterizing or showing skill in or specialized knowledge of applied arts and sciences



Gobbledygook

language that is meaningless or is made unintelligible by excessive use of abstruse technical terms; nonsense.



AISA

PERTHSEC

Technical comes from the Greek *tekhno*, which means "art or skill." Anything technical requires both art and skill. If you're an Olympic gymnast, you have technical abilities. You might go to a technical school to learn how to be a chef, a mechanic, or a massage therapist.
So that means without context it is meaningless.

The most senior software developer on a team is often not the most technical. They add value to design and code reviews by asking questions - not by reviewing technical syntax. They coach junior developers to stop focussing on the perfect syntax and elegant object-orientated design and instead to ask questions about business value, unexpected costs and worst-case scenarios.

Closed questions like 'are you technical?' are a mutual disbenefit.
They both gatekeep others access to conversations, but also your access to learn from other perspectives.

So, what are the (open) questions we should be asking instead?

Why does cyber security exist? What is our primary function?

Favourite analogies –
Cars have brakes so that they can **drive faster**.
The role of the NASA janitor was to **put people on the moon**.

First and foremost: We are there to solve problems and **enable business** to thrive. Reading LinkedIn posts, it's easy to assume that the majority of cyber security workforce think we exist to secure the business environment.

Hard news: cyber security is **not a business top priority, and it shouldn't be**. Cyber threats manifest as business risks the same way natural hazards do, and service outages do. And like the hospital emergency department, they need to be prioritised and triaged. Taking a everything is priority stance, makes nothing a priority.

Make it clear that you understand the business priorities, their top 3 business critical functions and ensure those work. Make conversations about solving their problems, rather than your own background. Business outcomes, not product features. Where does your solution or service fit into the wider business context? Most of us are technical with a different area of speciality, hence why we work as a team. But we should all be facing the same way, working on the same problem or outcome.

So, what's the alternative that we can ask folks?
What are you trying to do? What's most important? What has to happen? What does success look like?

Passion is temporary, curiosity is infinite…

> In the end, it's the people who are curious who ***change the world.***
>
> – NEIL DEGRASSE TYSON

AISA

PERTHSEC

Innovation isn't about playing it safe. It's about embracing uncertainty and thriving on the unfamiliar. **Do best what you know least.**

Curiosity is the spark that ignites innovation. It's the driving force behind some of the world's most game-changing ideas and inventions. Children are naturally curious and innovative. They question everything around them, play mind-boggling games and bombard their parents with tough questions. They experiment, try new things and never stop learning. But as we grow up, we become more risk-averse and less willing to experiment. **We become focused on the outcome** rather than the process, which limits our ability to think creatively.

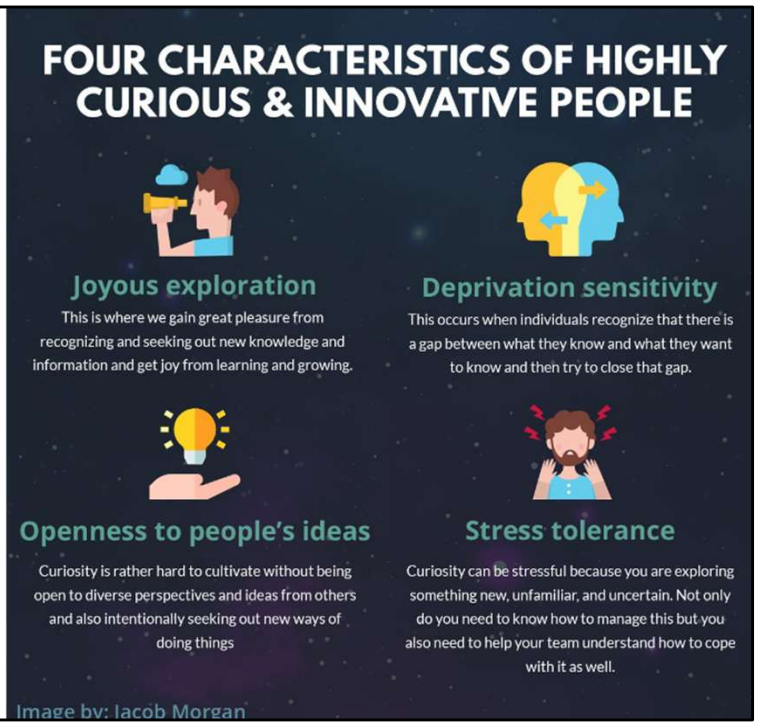
In a recent Harris Poll of US Workers, only 22% described themselves as curious at work, while 66% reported barriers to asking more questions and only 12% felt their employer is extremely encouraging of curiosity.

To innovate, we need to start questioning everything around us. Innovation isn't only about creating something from scratch; it's about improving current processes and seeing old problems with fresh eyes.

Embracing curiosity… Five steps

1. Stay curious
2. Embrace failure
3. Surround yourself with curious people
4. Stay informed
5. Take risks

AISA https://thefutureorganization.com/



So how do we create a more curious culture in cyber security?
It takes a willingness to be personally vulnerable in front of others, it takes vulnerable leadership and it takes courage to participate in uncomfortable conversations where we might learn.

Curiosity is contagious. Surround yourself with people who are also curious and innovative. This will inspire and motivate you to keep pushing the boundaries.

Innovation requires taking risks. Don't hesitate to step out of your comfort zone and try something new. This means you need to know what your personal risk appetite is. If a tour guide asks you to stand 2m back from the cliff edge, how far back do you stand? 5m, 2m or 1m?
This is directly relevant to the cyber security advice you dish out! It is biased by your personal risk zones.

Embracing curiosity is the key to developing innovation skills. It's what separates successful innovators from the rest. By questioning everything around us and exploring new ideas, we can identify problems that others have overlooked.

Cyber Theatre: Ask Questions!

A cyber program without defined threats and risks is a waste of money.

Questions to ask:

- What is your vision? Why would business care?
- If you can only do 2 things, what would you do?
- What features in my products should I not use?
- What will move the dial the most?
- Which business opportunity does this open up?
- What are my acceptable risk tolerances?
- Is this more likely than being struck by lightning?

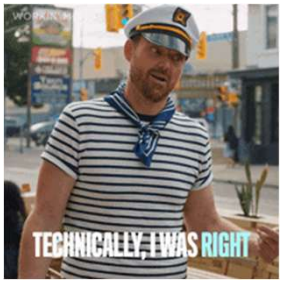
AISA

PERTHSEC

We're getting to the fun bit now! Let's start asking questions of current cyber advice out there…

If folks aren't familiar with Bob Lord and hacklore – do yourselves a favour and follow him.
As Bob says, when we tell people to worry about attacks that do not happen in the wild, we end up not protecting them from those that do!

You are technically correct



Most security advice is technically correct – and completely wrong for your organisation.

AISA

PERTHSEC

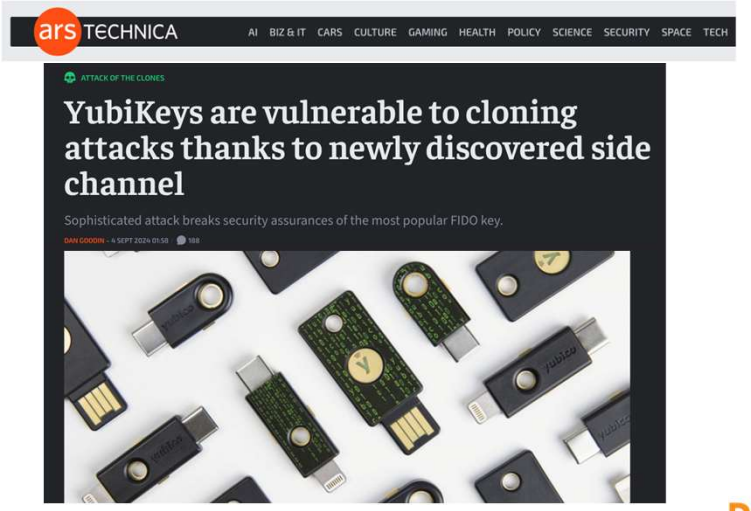
Most security advice is technically correct – and completely wrong for your organisation.

Think theoretical cyber security versus applied cyber security.
Governments (and consultants) typically product risk-adverse cybersecurity advice.
This is appropriate for government.
But most businesses are risk-exploitative.

Even worse, the advice is often coming from folks with zero practical experience with **running** *business* IT systems.
The best advice usually comes from the folks that started in the service desk and have a lived understanding of adoption costs, user friction and realised risk.

Too often the lack of specific technical knowledge is used to gatekeep cybersecurity.
But we need far less technically correct knowledge and far more curiosity asking the right questions.

You are technically correct



https://arstechnica.com/security/2024/09/yubikeys-are-vulnerable-to-cloning-attacks-thanks-to-newly-discovered-side-channel/

"Sophisticated attack breaks security assurances of the most popular FIDO key" is technically correct.

Technically interesting? Absolutely!
Relevant to your organisation's security? No.

Yubikeys are not quite as secure against cloning attacks via physical access as we previously thought.
But did those particular security assurances matter?

The standard Yubikey was never resistant to physical access. You literally just tap it to use it.
And the FIDO standard includes a monotonic counter to detect cloning.

Hacklore: Public WiFi and Juice Jacking

Bob Lord • Following
Senior Technical Advisor, CISA
1mo •

Here's some more silly, outdated #hacklore in the news. The "experts" make such bold, confident claims, without citing any evidence of the prevalence and impact of this type of alleged crime. Don't get me wrong, people have their digital lives compromised every second, just not *that* way.

Why do we not have the same amount of press for real attacks, like elder fraud, for which we can identify real victims who lost real money? Is it maybe because there isn't as clear a way to sell the snake oil?

Chris Gebhardt • 2nd
CISO. Practical. Reasonable. Creative. Concise. Experience with F...
4d •
+ Follow

Go ahead and plug in your USB cable to your phone. It's OK. Seriously, it is.

Social Media is loaded with lots of myths and this is certainly in that category. The concept was termed Juice Jacking where a malicious actor can access your phone or device when you plug the USB into a USB charging port they control. So how prevalent is this attack? Not a single case has been reported to the FBI or FCC since a proof of concept was shown at DefCon in 2011 yet both those organizations have warnings on their websites about it.

Since the #PoC was demonstrated, OS manufacturers have disabled the auto sync on USB connection. You must now give permission on the device for other connections to access it. The wild west days of data syncing are long gone. Yet, this advice still persists like this is an active threat.

#Cybersecurity decisions often come down to what is possible versus what is probable. Is this possible? Yes and no. Is it probable? Highly, highly unlikely approaching zero chance.

This is why I follow what is Practical and Reasonable. Especially around cybersecurity risk. There are only so many hours we have to help educate and prevent against real risks. Including InfoStealers, Malware, and misconfigurations (ie: MFA enabled but not enforced) all of which are highly, highly likely approaching 100% chance.

So yes, plug in your phone. Well, anywhere but BlackHat or DefCon. LOL

+ Follow

🚨 USB Alert: The Silent Data Thief 🚨
Ever plugged your phone into a public USB port for a quick charge? You might be handing over your data to cybercriminals.

AISA

https://www.linkedin.com/posts/lordbob_hacklore-activity-7233801616359874562-KQNw
https://www.linkedin.com/posts/gebhardtchris_poc-cybersecurity-activity-7252308144301772800-FJ2E

PERTHSEC

Educating users is the first aid of cybersecurity. It stems the bleeding to give us time to find and address the root cause.
Unfortunately, sometimes we forget to rip the band-aid off, and sometimes the band-aid was only applied to make the child feel better rather than for any actual necessity.

General users will always choose convenience before security. And this is right.
If you only get 20mins a year to educate a user, are you going to spend it telling them not to use public WiFi or is there a more probable threat you could help them guard against?

The public WiFi risk was unencrypted sensitive data (especially passwords) – and it was not limited to public WiFi.
The internet is literally a network of untrusted networks.
Google solved this via their HTTPS Everywhere initiative. Everything that matters is now encrypted.
Today the choice is one of user convenience – not security.

Juice jacking – never seen in the wild and mitigated by vendors.

Patch ASAP

Australian Signals Directorate + Follow
83,944 followers
4d

Delaying an update is like giving cybercriminals a free pass to access your devices.

Software developers release updates for their products to fix security concerns and improve functionality. Make sure all devices in your network have automatic updates switched on and are updated regularly.

When prompted, update devices and software to the latest version as soon as possible. This will reduce the window of opportunity that cybercriminals have to exploit any vulnerabilities. Our Essential Eight Maturity Model has recommended timeframes for patching.

If your software or device can no longer get updates, consider replacing or upgrading it.

Find resources on our website to protect yourself and your business this #CyberSecurityAwarenessMonth.

Don't delay updates!

Australian Signals Directorate + Follow
83,944 followers
1w

Microsoft has released its October security updates. This update included:
- 118 vulnerabilities patched.
- 2 vulnerabilities with evidence of exploitation.
- 3 'Critical' rated.

The ASD's ACSC encourages all users to apply the available patch updates ASAP.
For more details, visit the Microsoft Security Response Centre website
https://lnkd.in/eT7vMy2P

https://www.linkedin.com/posts/australian-signals-directorate_cybersecurityawarenessmonth-activity-7251382500441104384-voUB
https://www.linkedin.com/posts/australian-signals-directorate_microsoft-has-released-its-october-security-activity-7249567855006887936-fMS5

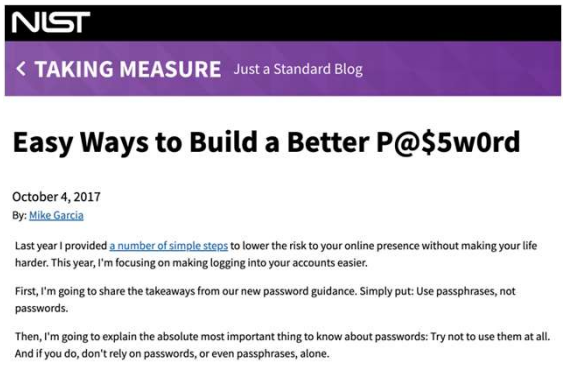
Failing to patch is the proximate cause not the root cause. It's also blaming the victims. It was useful in 2015 when we had a browser exploitation epidemic and we needed to stem the bleeding. Google solved that for us – yet we're still being told to patch even faster. The "patch everything even faster" advice had been soundly debunked as cost ineffective. Folks should just keep calm and patch at the cadence appropriate for their desired risk posture. It is pure security theatre in 2024.

The primary exploitation threat since 2020 has been network edge devices – and patching is not the best advice here.
Instead of patch asap - GET IT OFF THE INTERNET. It will save you heartache and hours of effort not having to patch future urgent updates.

Only public-facing services need to be on the discoverable internet. For employee-facing services, like VPNs, there are modern alternatives – WireGuard, ZNTA even IPv6.

The artificial urgency in this routine advice reduces the impact of alerts with true urgency, contributes to staff burnout, and pulls resources away from activities that actually reduce risk.

Passwords


NIST

< TAKING MEASURE Just a Standard Blog

Easy Ways to Build a Better P@$5w0rd

October 4, 2017
By: Mike Garcia

Last year I provided a number of simple steps to lower the risk to your online presence without making your life harder. This year, I'm focusing on making logging into your accounts easier.

First, I'm going to share the takeaways from our new password guidance. Simply put: Use passphrases, not passwords.

Then, I'm going to explain the absolute most important thing to know about passwords: Try not to use them at all. And if you do, don't rely on passwords, or even passphrases, alone.

AISA https://www.nist.gov/blogs/taking-measure/easy-ways-build-better-p5w0rd PERTHSEC

Folks are so focussed on being technically correct about the strongest passwords that they are missing that **NIST's primary advice is to not use passwords at all**!

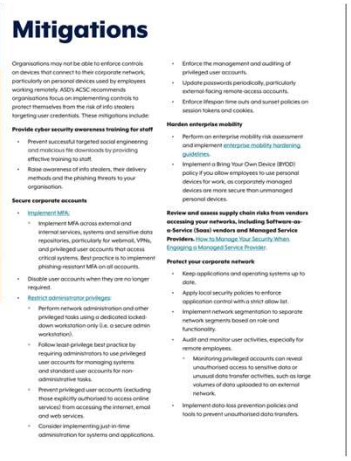
Letting users pick passwords is like letting users choose which padlock will secure your business's door - and users always correctly optimise for their convenience.

Large organisations should be passwordless and SSO where possible – and a password manager otherwise.

Small organisation and individuals should use your browser to chooses unique passwords (or passkeys) for you and sync between your devices.
And don't turn on MFA wherever possible – **just wherever it matters**. So, banking and email.

Recommending password managers instead of browsers to individuals is letting perfection get in the way of progress.
The implementation cost is **much** higher and the additional security benefits do not meaningfully change the risk.

Password stealer mitigations



Mitigations

Organisations may not be able to enforce controls on devices that connect to their corporate network, particularly on personal devices used by employees working remotely. ASD's ACSC recommends organisations focus on implementing controls to protect themselves from the risk of info stealers targeting user credentials. These mitigations include:

Provide cyber security awareness training for staff

- Prevent successful targeted social engineering and malicious file downloads by providing effective training to staff.
- Raise awareness of info stealers, their delivery methods and the phishing threats to your organisation.

Secure corporate accounts

- Implement MFA:
  - Implement MFA across external and internal services, systems and sensitive data repositories, particularly for webmail, VPNs, and privileged user accounts that access critical systems. Best practice is to implement phishing-resistant MFA on all accounts.
- Disable user accounts when they are no longer required.
- Restrict administrator privileges:
  - Perform network administration and other privileged tasks using a dedicated locked-down workstation only (i.e. a secure admin workstation).
  - Follow least-privilege best practice by requiring administrators to use privileged user accounts for managing systems and standard user accounts for non-administrative tasks.
  - Prevent privileged user accounts (excluding those explicitly authorised to access online services) from accessing the internet, email and web services.
  - Consider implementing just-in-time administration for systems and applications.
- Enforce the management and auditing of privileged user accounts.
- Update passwords periodically, particularly external-facing remote access accounts.
- Enforce lifespan time outs and sunset policies on session tokens and cookies.

Harden enterprise mobility

- Perform an enterprise mobility risk assessment and implement enterprise mobility hardening guidelines.
- Implement a Bring Your Own Device (BYOD) policy if you allow employees to use personal devices for work, as corporately managed devices are more secure than unmanaged personal devices.

Review and assess supply chain risks from vendors accessing your networks, including Software-as-a-Service (Saas) vendors and Managed Service Providers. How to Manage Your Security When Engaging a Managed Service Provider.

Protect your corporate network

- Keep applications and operating systems up to date.
- Apply local security policies to enforce application control with a strict allow-list.
- Implement network segmentation to separate network segments based on role and functionality.
- Audit and monitor user activities, especially for remote employees.
  - Monitoring privileged accounts can reveal unauthorised access to sensitive data or unusual data transfer activities, such as large volumes of data uploaded to an external network.
- Implement data-loss prevention policies and tools to prevent unauthorised data transfers.

Become an ASD Cyber Security Network Partner and join ASD's Cyber Threat Intelligence Sharing (CTIS) service

- CTIS is a two-way sharing platform that enables government and industry partners to receive and share information about malicious cyber activity.
- ASD's ACSC is tracking info stealer activity and shares details of active command and control infrastructure through the CTIS platform.
- Sign up to become a partner and protect your organisation and customer data from cybercriminal threats.

Prepare for a compromise

- Develop a cyber security incident response plan to use in the event of an info stealer compromise. Ensure that employees are aware of what to do and who to contact if they suspect they have downloaded a suspicious file.

Implement ASD's ACSC's Essential Eight

- In addition to the mitigations mentioned above, ASD's ACSC strongly recommends implementing the remainder of ASD's ACSC's Essential Eight.

Advice for your employees when working remotely

- Protect your information on your personal devices
  - Develop good cyber hygiene and do not click on suspicious links or pop-ups, or download files or software from unknown or untrusted sources.
- Use distinct passwords for work and personal accounts. Use MFA for personal accounts where possible.
- Do not store your work credentials in a personal password manager unless explicitly approved by your employer. This includes your web browser's password manager. **If in doubt, request that your employer provide a corporately supported password manager.**
- Do not log in to your work accounts from shared or communal workstations.
- Be aware of what is being stored in your web browser's autofill feature. Info stealers target the data that browsers save to autofill forms. When filling in web forms, consider manually entering sensitive data, such as credit card numbers, rather than saving it to your web browser's autofill feature.
- Log out from all online services and clear web browser cookies after finishing a browsing session in order to reduce the information available to info stealers.
- Ensure that your operating system's built in antivirus solution is enabled. If you use a third-party antivirus solution, ensure that it is kept up to date and is from a reputable vendor.

Assistance

Australian organisations that have been impacted or require assistance regarding an info stealer compromise can contact ASD's ACSC via **1300 CYBER1 (1300 292 371)** or by submitting a report at cyber.gov.au/report.

ASD's ACSC encourages entities to report suspicious network activity and indicators of compromise associated with info stealers, even if an incident is considered contained. We use the information you provide to improve our understanding of cyber threat actors' tactics, techniques and procedures, which helps us to warn other Australian organisations that have been targeted in the same way.

AISA https://www.cyber.gov.au/sites/default/files/2024-09/Information-Stealer-Malware-Advisory.pdf PERTHSEC

Let's looks at some recent password stealer advice.

Buried at the end there 2 pages of mitigation advice – 9 items. All of it is technically correct.
The ASX100 might need that depth of advice – but they also have in-house expertise.
So, who is the audience? <statistics on next slide>

Remote access is convenient, but risky. But not having remote access is also risky!
It's a business risk.
What is **your** organisation's risk tolerance for each service?
Assume breach → and that all passwords are eventually public knowledge.
So, if your user passwords are public knowledge, ask yourself what needs to be true for remote access risk to be acceptable for your business.

Scale:
Hidden Link – Password – 2FA – pMFA – MAM (←BYOD)//(Managed→) MDM – Onsite – Onsite with 10ft fence.

Australian Business Breakdown

Number of employees	Number of businesses	% of total businesses
Small business (0-19 employees)	2,589,595	97.2%
Medium business (20-199 employees)	68,214	2.6%
Large business (200+ employees)	5,189	0.2%
Total	**2,662,998**	**100.0%**

AISA **Source**: *ABS Counts of Australian Business*, Table 13a, August 2024 and ASBFEO calculations (excludes businesses that are not registered for GST).

PERTHSEC

97.2% of Australian businesses have fewer than 20 employees and 99.8% fewer than 200 employees.

So, what is the right advice for these businesses?
They are unlikely to have internal IT support, probably not even an MSP and without the skills to interpret how most Govt advisories alter their business “solvency”?

CrowdStrike Root Cause Analysis

The Guardian Aus

CrowdStrike apologizes for global IT outage in congressional testimony

Faulty update from cybersecurity company grounded hospitals, airports and payment systems in July

Screens show a blue error message at LaGuardia airport in New York, on 19 July 2024. Photograph: Yuki Iwamura/AP Photo

/ Windows Experience Blog

Security

September 12, 2024

Taking steps that drive resiliency and security for Windows customers

By David Weston, Vice President Enterprise and OS Security at Microsoft

On Tuesday, Sept. 10, we hosted the Windows Endpoint Security Ecosystem Summit. This forum brought together a diverse group of endpoint security vendors and government officials from the U.S. and Europe to discuss strategies for improving resiliency and protecting our mutual customers' critical infrastructure. Although this was not a decision-making meeting, we believe in the importance of transparency and community engagement. Therefore, we're sharing the key themes and consensus points discussed during the summit, offering insights into our initial conversations.

We want to thank every one of our summit attendees for dedicating their time to participating in these meaningful discussions. The CrowdStrike incident in July underscored the responsibility security vendors have to drive both resiliency and agile, adaptive protection. And it was inspiring to see the engagement throughout the event's agenda and activities.

https://www.theguardian.com/technology/2024/sep/24/crowdstrike-outage-microsoft-apology
https://blogs.windows.com/windowsexperience/2024/09/12/taking-steps-that-drive-resiliency-and-security-for-windows-customers/

There were two concurrent outages – OT and IT.
Companies often have contingencies for IT outages, but your OT is literally your business operations.
The primary impact per the reporting – hospitals, airports and payment systems – was the OT outage, not the IT outage.
And the root cause was (automatic) updates on OT. Staged automatic updates are still automatic updates.

How did automatic updates end up on your OT? It was running Windows and Windows always needs EDR, doesn't it?
Where do we need EDR? What is the best value for EDR deployment? Where is it least value? Can I save money and use it on something else?

If Microsoft's proposed Safe Deployment Practices for Endpoint Security policy was in place last month, would it have prevented the outage?
Probably not. CrowdStrike would have passed Microsoft's (paper based) review with flying colours.

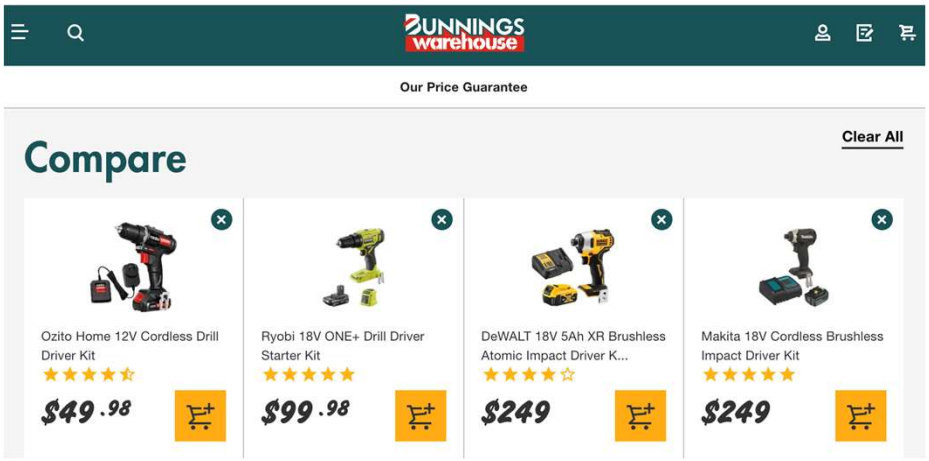
Software quality

AISA https://www.cisa.gov/resources-tools/resources/secure-demand-guide PERTHSEC

14 questions for **everyone** to demand high software quality.
Cut down from 77 questions in the Software Acquisition Guide for Government Enterprise Consumers.

But does the quality of this software matter to me?
Higher quality means higher price.
Don't I want fit-for-purpose quality?

Software quality choice?



AISA https://www.bunnings.com.au PERTHSEC

Before demanding quality start by asking some questions to determine how much quality you need.
Is it internet exposed? Is it running as root? Does it handle untrusted data? Does it handle sensitive data? Can I segment or sandbox it?

After Volt Typhoon, Microsoft was pressured into offering 6 months of security audit logs for “free”. *not actually free.
Cost driven up for folks **that will never use these logs.**
Access to audit logs should be free, but log retention should be cost recovered.

We should demand software quality **where it matters**.
We should patch **where it matters**.
We should MFA **where it matters**.

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/resources-business-and-government/essential-cyber-security/strategies-mitigate-cyber-security-incidents/strategies-mitigate-cyber-security-incidents

PERTHSEC

Our annual reminder that the Essential Eight was defined in the **most recent** update to ASD's Strategies to Mitigate Cyber Security Incidents.
This update was published in February **2017** when the primary threat was internet to the desktop.
The recent updates to the Essential Eight **Maturity Model** have tweaked the method but not the substance of the advice.

Is the Essential Eight right for my organisation?
What portion of contemporary tradecraft does it still cover?
How many incidents did ASD respond to last year involved Unpatched User Applications, Unhardened User Applications or Office Macros?
Is patching my legacy edge devices even feasible? Or do I need modern equivalents that are segmented?

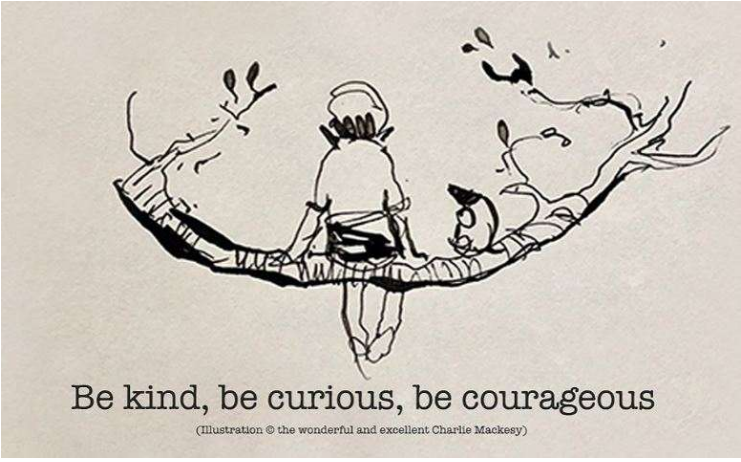
2024 Essential Eight?

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

AISA PerthSEC 2023. Essential Eight Makeover - How to marry E8 with contemporary Australian threats. PERTHSEC

Our previous suggested updates to the Essential Eight based on an analysis of the 2023 ACSC Threat Report and major contemperory incidents.

Be ~~technical~~ curious



AISA https://www.charliemackesy.com/

PERTHSEC

There were four themes for today

1. You cannot dissect cyber theatre by being technical.
2. You can be technically correct and wrong.
3. Curiosity is more powerful and useful than being technical and harder to develop
4. Stop asking are you Technical and ask more open questions that drive business innovation.

5. Understand your business priorities better than the CEO and craft your strategy to deliver these. Not to secure all the things that probably won't happen. Let your execs travel and use public wifi!

Hopefully, we've left you with some questions you can ask the next time you see an all-important critical advisory promoting immediate action.

Remember, you just need to swim faster than your neighbour ;)