



HACKED

ATTACK & DEFENSE STRATEGIES FOR BUSINESSES

DAN WEIS

PRACTICE LEAD - PENETRATION TESTING

NEXON ASIA PACIFIC

Dan Weis

- Practice Lead – Penetration Testing & Security Services
- I get paid to break into company & government networks for a living
- Major Nerd, Been in I.T since 1994.
- 15 Years in security space
- 13.5 years of doing pentests and security engagements for clients
- Trainer of upcoming ethical hackers and Nerds.
- Stack of certs (23), 1 of the first 10 people globally to become a certified ethical hacker.
- Have documented CVE's attributed for 0days identified in SCADA/Control Systems
- Public speaker on all things Infosec & Darkweb, presented at over 80 conferences and events over the last 5 years.
- Multiple TV & Radio appearances, Newspapers, magazines etc., Stack Online Stuff
- Author – Hack proof yourself! & co-author of Learn Social Engineering



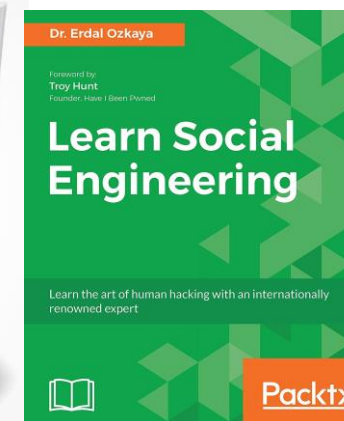
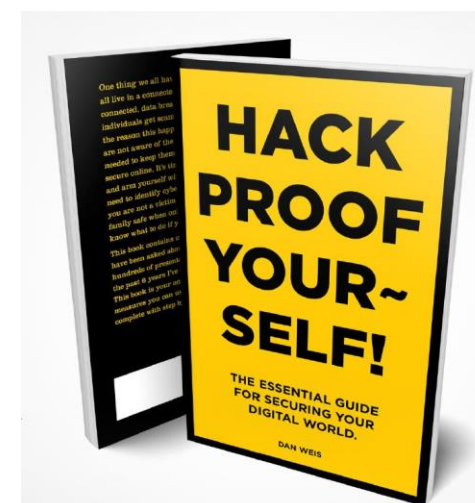
<https://au.linkedin.com/in/daweis>



Daniel.weis@corp.nexon.com.au



@Bl4ck0p



DISCLAIMER

STOP!



The content presented today contains tools, techniques and resources used for hacking & illegal activities



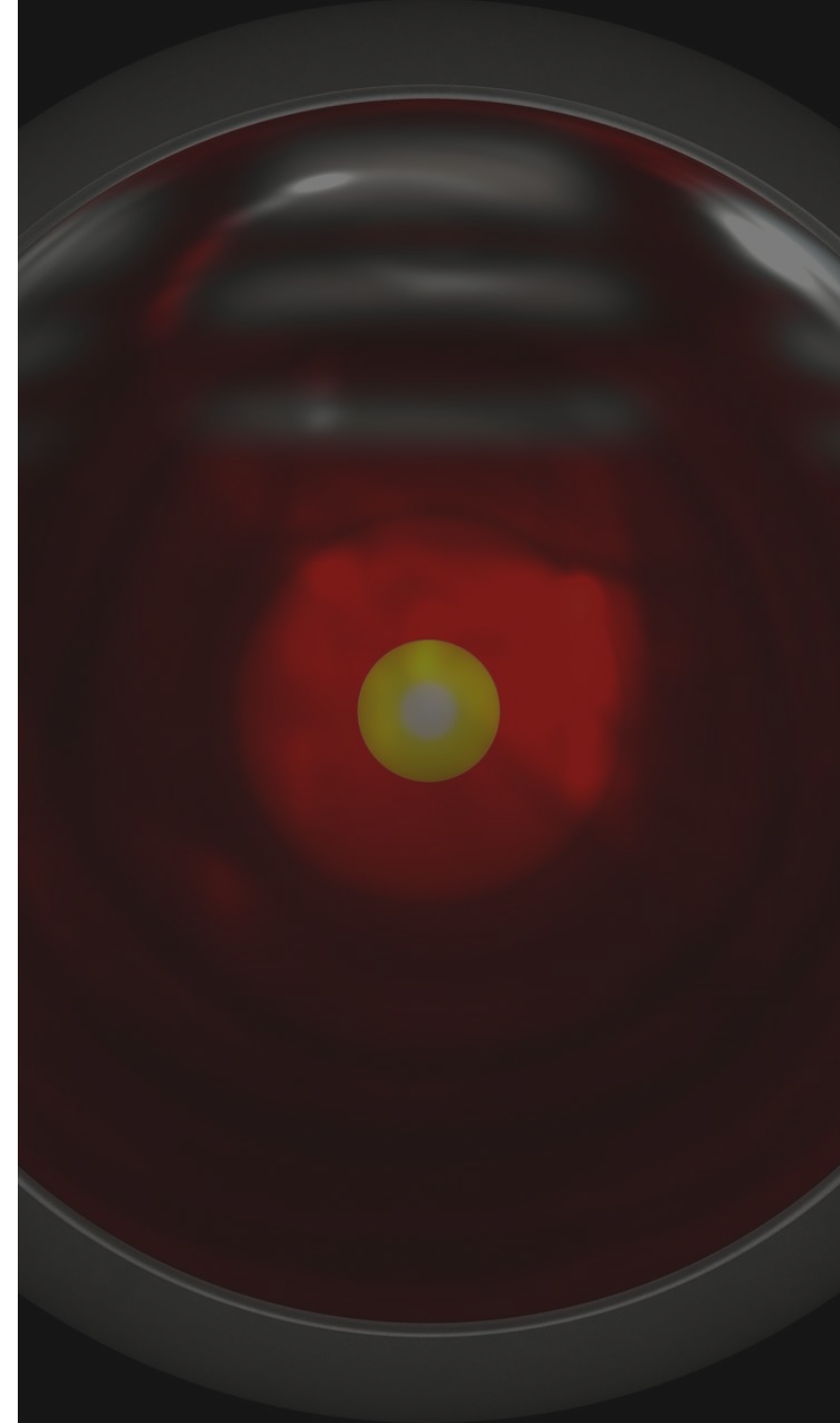
The content is for education purposes only



Hacking is illegal. You **MUST** have written permission from the associated target/party(s)



I do not condone illegal hacking or malicious activities.



Nexon engagements

- We perform Penetration Testing & Security Engagements for clients anywhere from 100-150 engagements each year:
 - Penetration Testing engagements
 - Cyber Risk Assessments
 - Security Consulting, Security Training and Phishing Simulations.
- Our clients are from all industries and sizes
- Goal is to Provide our clients a picture of their Cyber Risk Posture and to assist them with increasing their overall security posture and to not become the next headline.

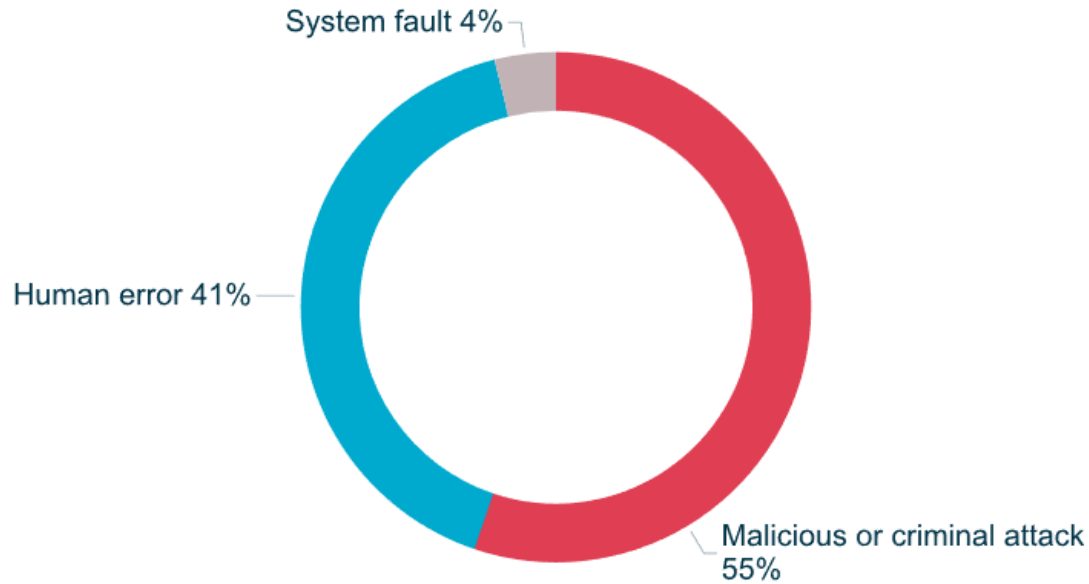
Threat Landscape

- So much scaremongering!
- We see everyday in the news, x number of hacks are happening
- X number of Data Breaches & Breach Records Each Year (Always in the Billions)
- 62% of SME's reported cyber attacks last year
- Average breaches is anywhere from 276k to 1.6M

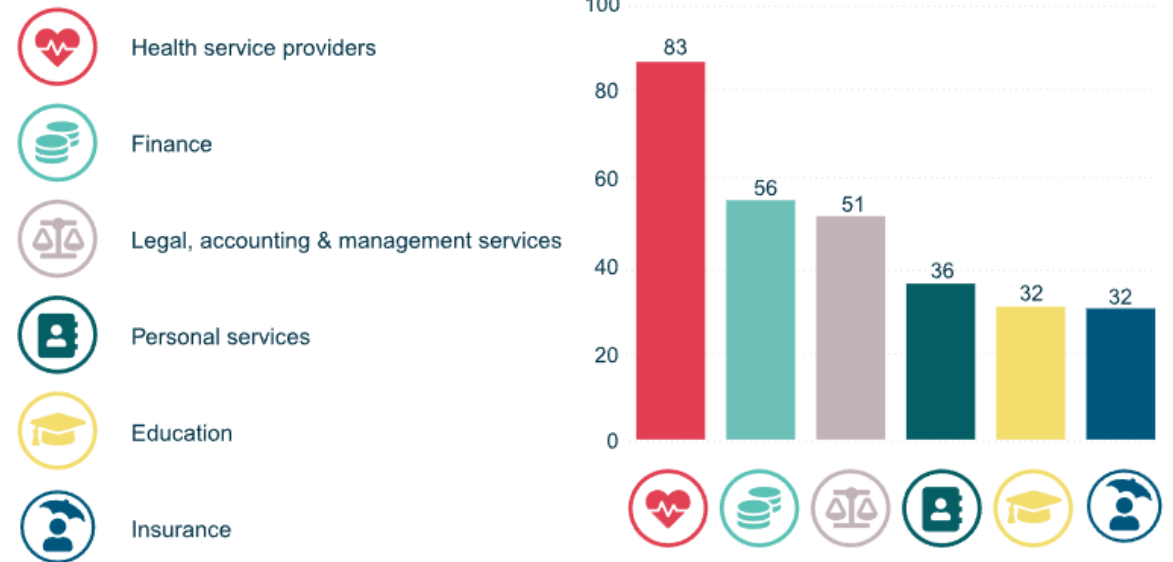
Threat Landscape

- OAIC NDB – Most accurate Source for Data Breach Stats

Chart 9 – Source of data breaches



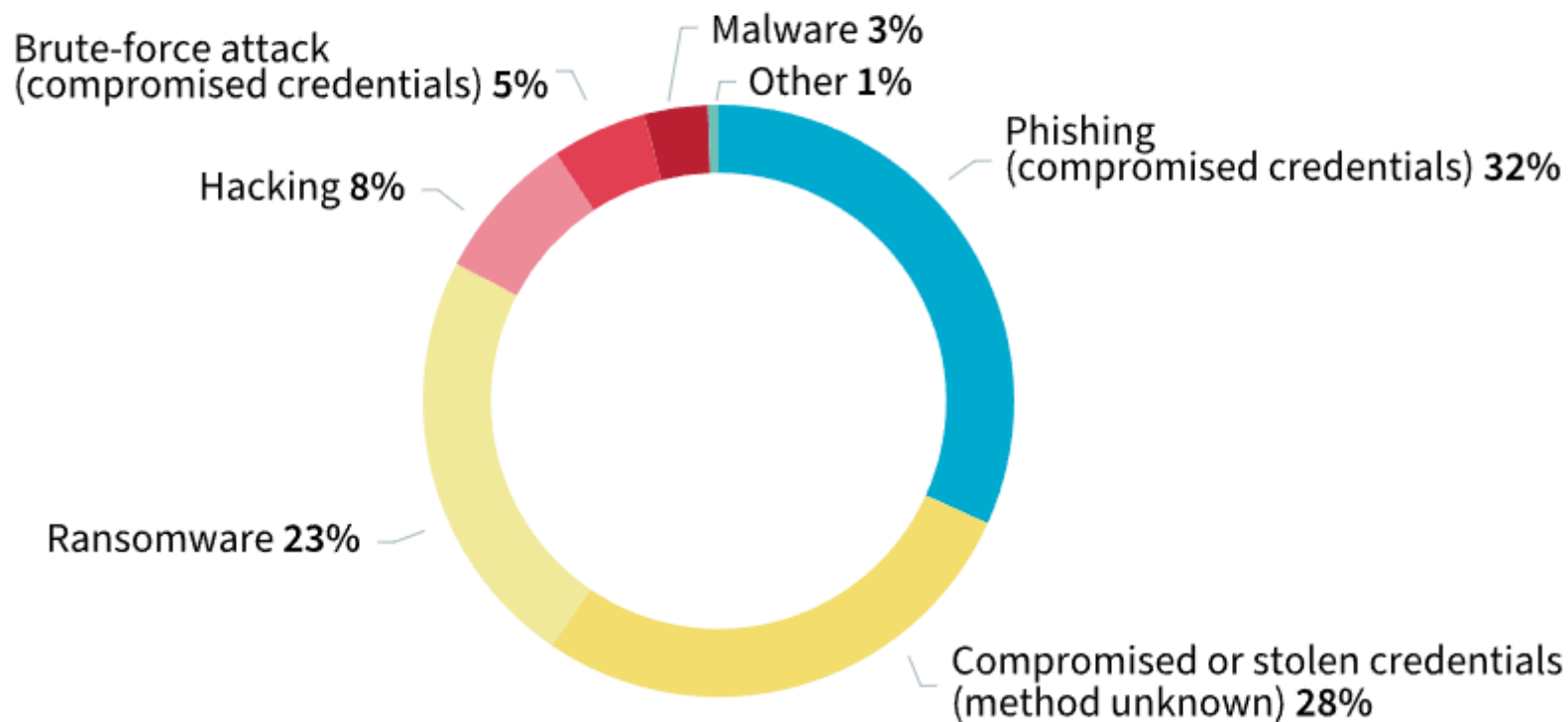
Top industry sectors to notify data breaches



Source: <https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-report-july-december-2021>

37% of all data breaches resulted from cyber security incidents (173 notifications)

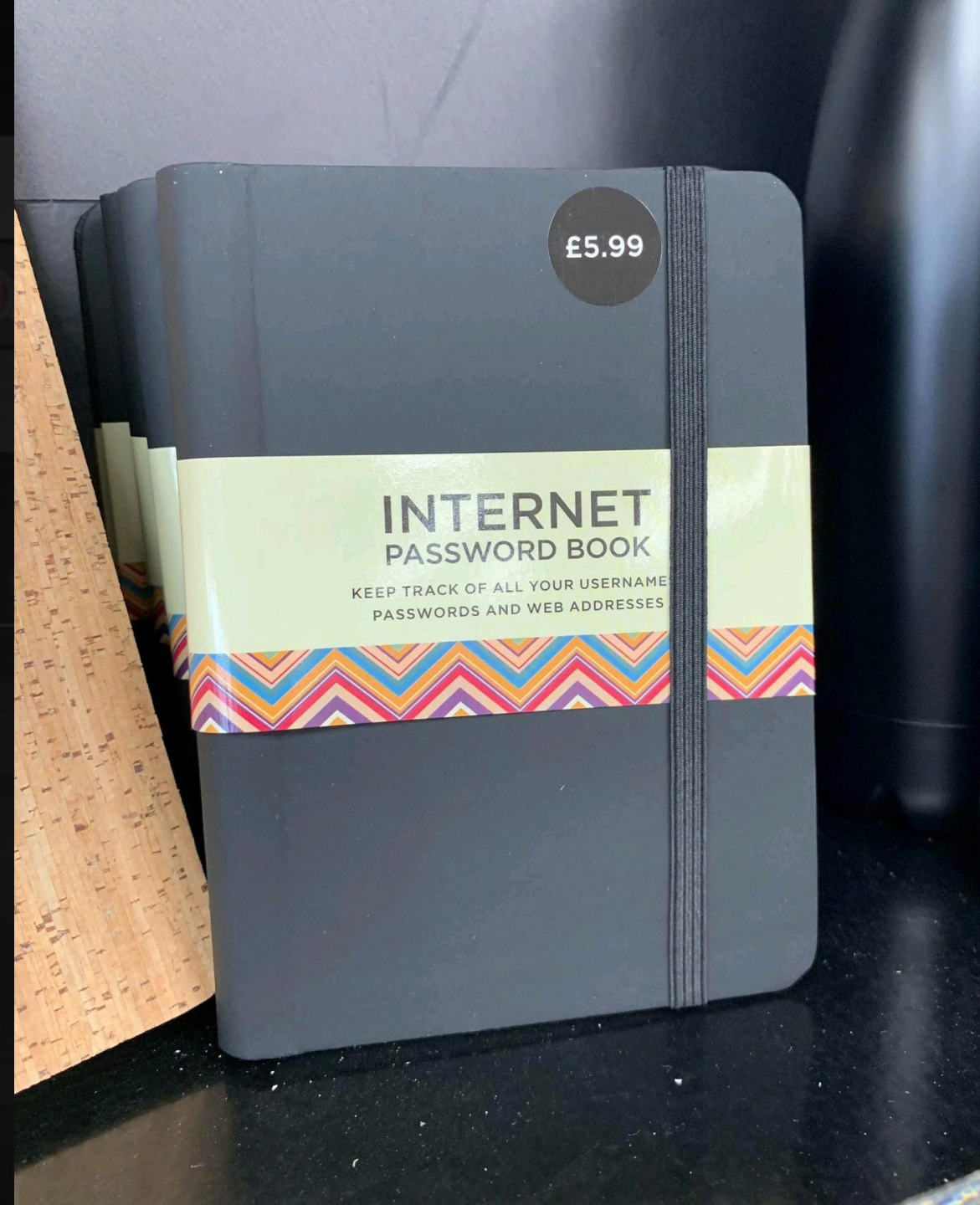
Cyber incident breakdown



CHALLENGES TO SECURITY



DUMB AS*ES BRINGING OUT
PRODUCTS LIKE THIS:



AND THAT LACK OF AWARENESS:

Password Change Sign Up sheet

If you'd like to change your password please fill out the form below and we will change your password on the system you indicate.

Full Name	System (Yardi, email, ect.)	Current password	New password
Kyle Smith	Email	Scooter 49\$	Steele4U2 (all upper case)
LIZ JONES	PHONE	89621	4281
Jack H.	Email**	Password	Password 2
Big Ed	Facebook	redstepin	mimmkay
Sqm Adams	Pike Pass	h	beer lover 1981

Come See Me
-Shawn

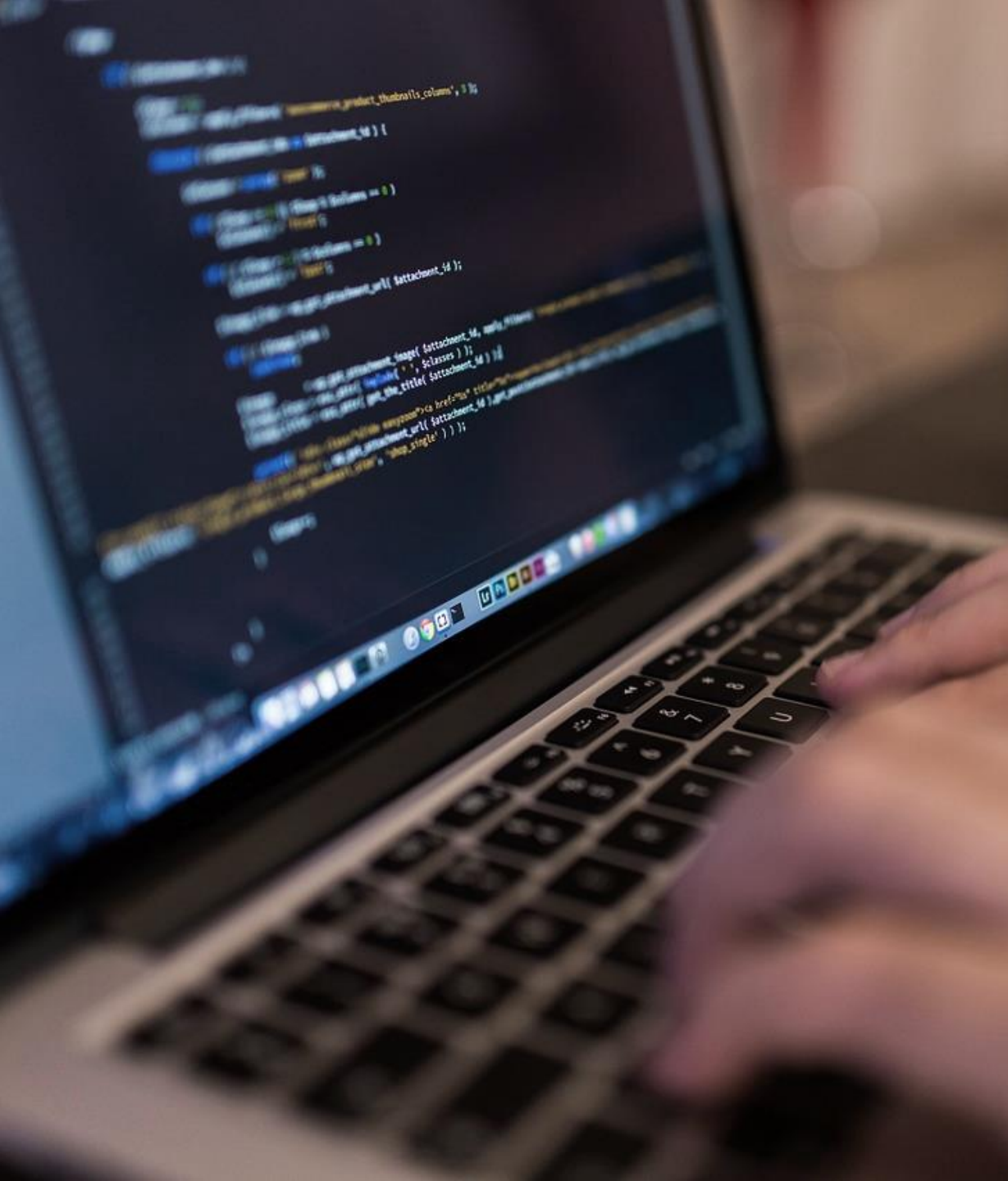
Why are they doing it?

- Cash Bro!
- Show off to their hacker buddies
- Because they can (60 minutes on youtube is enough to be dangerous)
- Because you business wronged them in some way (or so they think)
- Business Interruption (think competitive advantage)
- Nation advantage
- But they have one main goal...





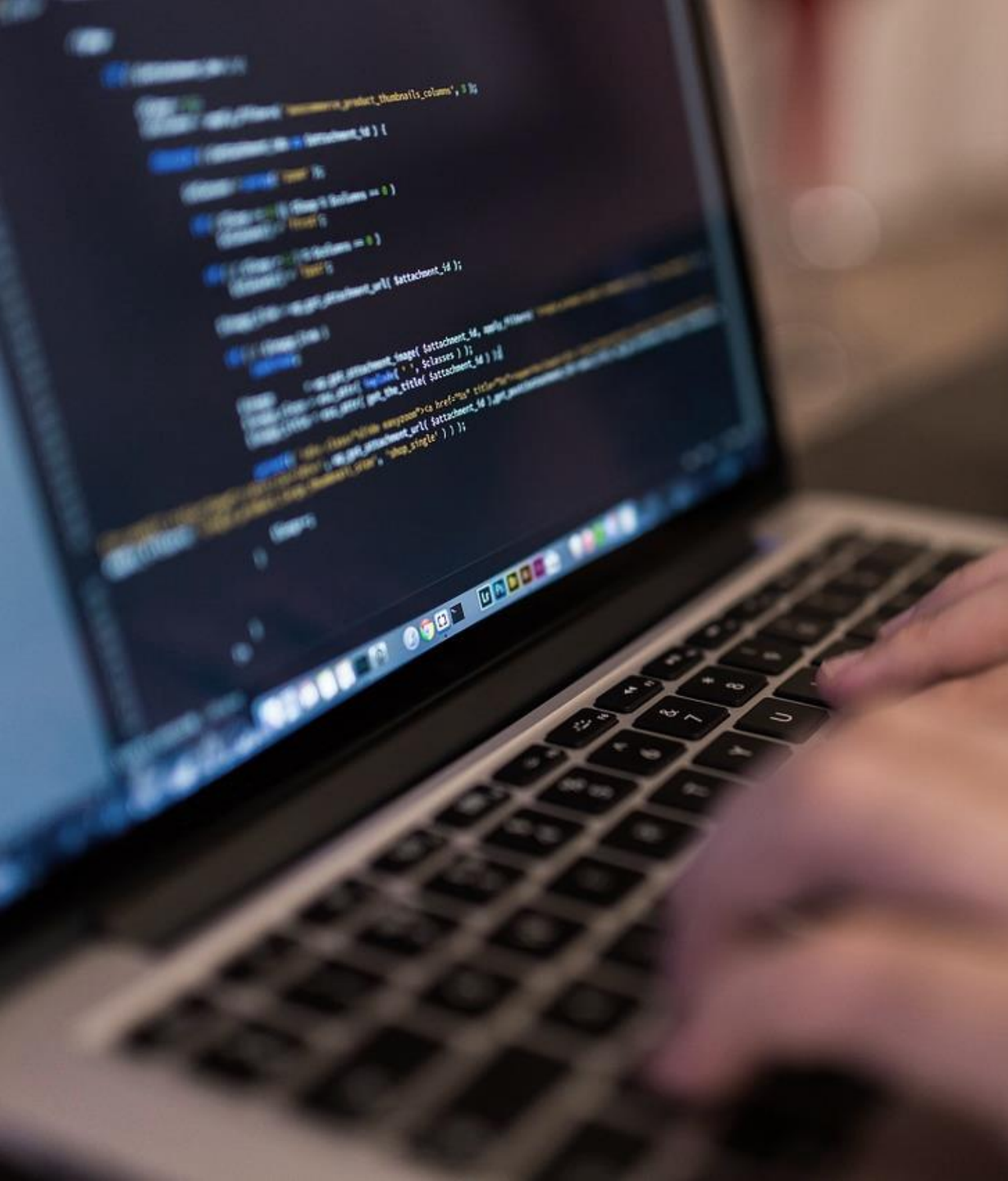
DO WHATEVER IS POSSIBLE



TECHNIQUES

How are they getting in

- Recon / Information Gathering
- Social Engineering & Phishing Staff
- Passwords (reuse of passwords), credential stuffing or password sprays
- Leverage vulnerabilities in systems like misconfiguration from I.T
- Leverage MSP's
- Relying on lack of knowledge from individuals and Business
- Every day attacks become more complex

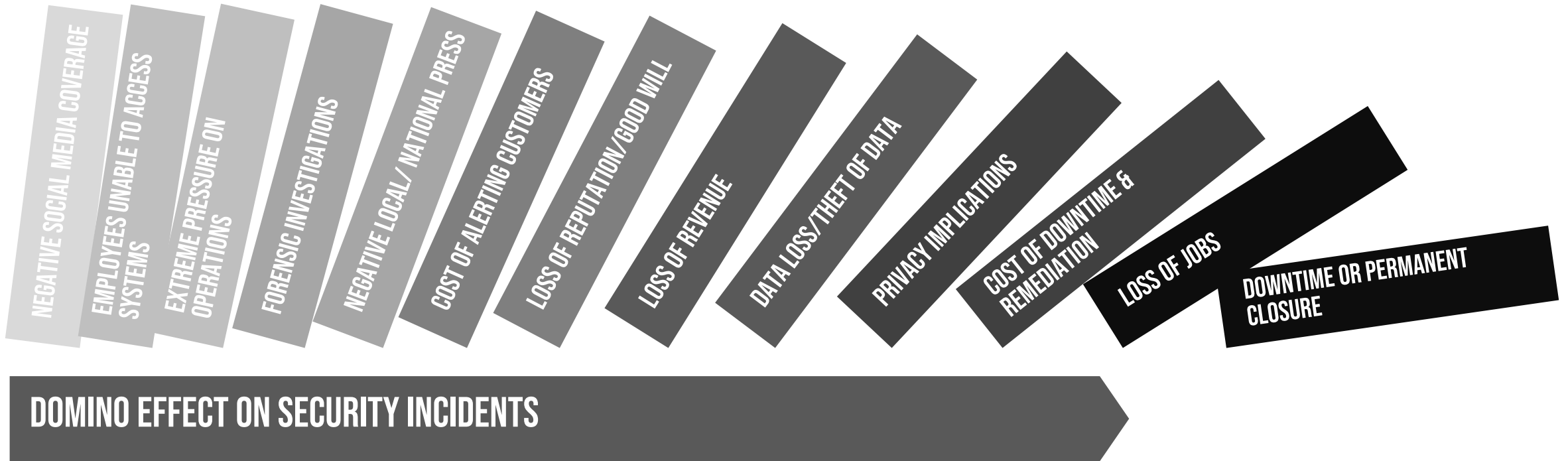


And once they are in..

- Doing whatever they can
- Mapping out your systems and processes
- Access whatever data they can get their hands on, money, files etc.
- Email/phishing customers
- Usually in the network for weeks or months before detection
- Either as a diversion or as the finale they hit you up with Ransomware to shutdown your operations and/or get paid.

EFFECTS OF BREACHES

TO I.T SECURITY



DISCLAIMER

STOP!



The demo about to be presented contains common techniques, information leakage and vulnerabilities that **EVERY** organisation has



It does not indicate that an organisation, person or entity is vulnerable or has weakness or vulnerabilities in their environment in any way.



Although a specific organisation will be targeted, the same outcomes would be achieved against ANY organisation with an internet presence



The demo's are for education purposes only.





TIME FOR A DEMO

Hacking Networks is like a jigsaw Puzzle...

We live in a digital age.

- Information is everywhere
- Everything is Online
- It's easy to get (no tech hacking)
- You just need to know how to piece it all together!

A close-up, slightly blurred photograph of a person's hand wearing a black nitrile glove, typing on a silver laptop keyboard. The hand is positioned on the right side of the keyboard, with fingers pressing down on keys. The laptop screen is visible in the upper left corner, displaying a grid of small, illegible text. The overall image has a dark, moody aesthetic with a blue and black color palette. The text "PRETTY EASY, RIGHT?" is overlaid in the center in a bold, white, sans-serif font.

PRETTY EASY, RIGHT?



“

The attacker only needs to get it right
once


You need to get it right **all the time.**



Common Findings

- IT Guys wear the security hats as well
- Non/Limited segmentation of admin accounts
- Account Hygiene
- Passwords – Weak Adoption, including length & complexity, non sentence adoption
- Lack of staff awareness & training
 - Handing over Passwords
 - Opening things they shouldn't
 - Payments without verification

Common Findings

- 
- Two men are shown in a server room. They are looking at a server rack. One man is pointing at a cable. The server room has blue lighting and many cables are visible.
- General Phishing & Credential Harvesting Success
 - 30% click rate
 - 72% hand over their passwords
 - 6% respond in under 5 minutes or less
 - Repeat offenders on every engagement
 - Lack of detection & Incident Response & Cyber Resilience
 - Have no idea an attack is underway until its too late
 - No regular testing of Incident Response plans and simulations
 - Low application whitelisting adoption
 - Unsupported Operating Systems, legacy software & Apps, Patch Management

Common Findings

- Regular Pentesting & Remediation
 - Opt for every 2 years instead of annual
 - Not remediating all issues due to under resourced

```
return null !== a.val && a.val.length >= a.arg || g.minSelected.replace("{count}", a.arg),
},
radio: function(b) {
  var c = a(this.form.querySelectorAll('input[type=radio][name="' + b.name + '"').filter(":checked").length);
  return 1 === c
},
custom: function(a, b) {
  var c = b.options.custom[a.arg],
  return c ? RegExp(c.pattern);
```



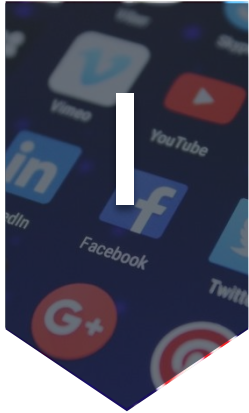
GOLDEN RULE

There is **no way to STOP** a hacker, you can only **make their**
job
HARDER!

PATH OF LEAST RESISTANCE



WHAT'S YOUR PATH OF LEAST RESISTANCE?



**USERS /
EMPLOYEES**



WEBSITE



PHISHING



WIRELESS



**MOBILE
DEVICES**



USB



**IT PROVIDER
/ LEGACY
SYSTEMS**



**PHYSICAL
ACCESS**



PASSWORDS



Your role as Auditors

- Educate your clients on cyber risk & cyber resilience.
- Ensure they have a program in place to quickly and effectively respond to a breach/incident.
- Ensure they are taking the necessary measures to prevent becoming low hanging fruit, Find those paths of least resistance!

CYBERSECURITY CHECKLIST FOR A BUSINESS

Have you had a Penetration Test (Pentest) Performed?

Do you have an incident Response policy/process in place?



Are you prepared for Mandatory Breach Reporting?

Are you cyber resilient? Can you quickly bounce back from a breach



Are your I.T Guys doing the right thing? What are they doing about:

- Backups
- Endpoint Protection (EDR)
- MFA (multifactor authentication)
- Cloud Security (Conditional Access, DLP, password Controls etc)
- Detection and Response
- Adopting ACSC E8
- Regular Vulnerability Scanning & Patch Management
- Monitoring, would they know if you were hacked?
- Locking Down the environment
- Network Security
- How are they protecting their network? (if an MSP)

CYBERSECURITY CHECKLIST FOR A BUSINESS



Cyber Insurance Coverage, is it in place and is the amount of cover suitable? (Hint your 1M ML is probably not enough)



Staff Awareness Training (Micro Learning) and Regular Phishing (Every month!)

Get Educated! keep abreast of the latest security news and vulnerabilities/exploits:


- Newsfeeds
- Websites like LinkedIn, thehackernews etc.
- Membership services, ACSC, AusCERT, Scamwatch etc.
- Discord channels etc.
- USA CISA

If you have been hacked.. Or suspect it

- IT / Incident Response provider
- Kick into play Incident Response Plan
- Contact ACSC (1300 CYBER1)
 - They will assist with you other third party involvement & reporting
- Engage Cyber Insurance Provider (Potentially)

From the Personal Side

- Reach out to IDCare

A top-down view of a person wearing a grey hoodie, sitting at a wooden desk and typing on a black keyboard. There are three computer monitors around them, all displaying lines of code. A silver laptop is also open on the left side of the desk. The person's hands are on the keyboard, and their head is bowed. The text "Every organisation has something that someone else wants" is overlaid in white in the center of the image.

Every organisation has something that someone
else wants

THANKS FOR WATCHING

See you next time



<https://au.linkedin.com/in/daweis>



<https://danielweis.wixsite.com/mysite-1>



Dan.weis@corp.nexon.com.au



[@Bl4ck0p](#)

Questions?

☎ 1300 800 000
✉ enquiries@nexon.com.au
💻 nexon.com.au
in ▶ f ▶ nexonap

