Guardians of Cyberspace

An intro to cybersecurity, and how you can help too

~$>whoami

DANIEL

@hellodanielting

daniel.ting@owasp.org

- Independent Security Architect & Consultant
- Previously,
  Senior Cloud Security Architect
  & Penetration Tester at Trustwave / Hivint
- Co-founded some startups
- Co-organise SecTalks Melbourne
- Chapter Lead,
  OWASP Melbourne Chapter
- Organiser of OWASP AppSec Day (appsecday.io)
- Leadership Team, Cyber Volunteers Australia

Why should we care?

I am nobody. Who is going to attack me?

- ✓ Setup Email
- ✓ Register business (ABR/ACN)
- ✓ Source clients
- ✓ Send/Receive contracts & invoices
- ✓ Grow
- ✓ Hire employees
- ✓ Electronic Tax Filing


Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt

What’s the impact this business
& his customers?

forbes.com/sites/leemathews/2017/08/16/notpetya-ransomware-attack-cost-shipping-giant-maersk-over-200-...

Forbes Billionaires Innovation Leadership Money Business Small Business Lifestyle Lists Advisor Featured

Aug 16, 2017, 11:47am EDT

NotPetya Ransomware Attack Cost Shipping Giant Maersk Over $200 Million

Lee Mathews Senior Contributor ⓘ
Cybersecurity
Observing, pondering, and writing about tech. Generally in that order.

The impact of NotPetya forced Maersk to reinstall 4,000 servers and over 45,000 PCs, with losses caused by serious business interruption estimated to amount to over $300m, despite the shipping firm never being the intended target of the attack.

https://www.zdnet.com/article/two-cyber-security-myths-you-need-to-forget-right-now-if-you-want-to-stop-the-hackers/

A Maersk shipping container/Wikipedia WIKIPEDIA

What is Cybersecurity?

A business enabler in cyberspace.

Physical & Digital/Internet/Cyberspace

Business Risks

- Strategic Risks
- Compliance Risks
- Operational Risks
- Reputational Risks

Business Continuity Impact

☠️ Death of the Business.


Cybersecurity
is about
Risk
Management


Cybersecurity not just a technology-people problem?

Australia wants boards held to account for infosec

Australia's new 2020 cyber security strategy is the latest national plan to propose that company directors be held accountable for meeting minimum information security baselines prescribed by the government.

Australia's Ministry of Home Affairs flagged "possible legislative changes that clarify the obligations for businesses... to protect themselves and their customers from cyber security threats" including new "duties for company directors". These new rules of the road would affect both regulated and previously unregulated entities.

Source : Risky.biz newsletter on the analysis of the new cybersecurity strategy. 11 July 2020

EAT

SLEEP

Cyberspace

operate{ IP{..},
collaborate{..},
finance{..},
CRM{..},
etc. };

REPEAT

EAT

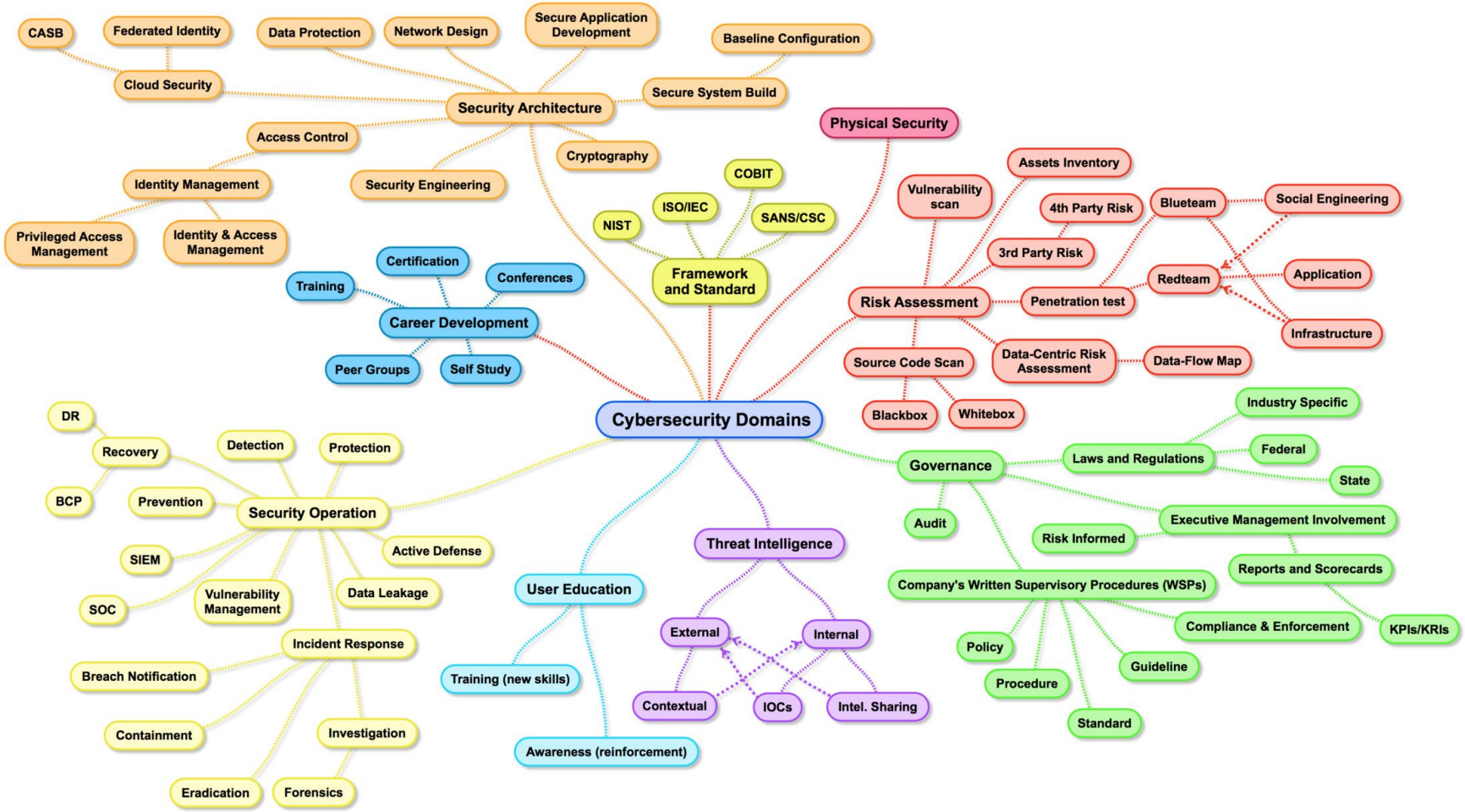
SLEEP

Cyberspace

live{ work{..},
socialise{..},
finance{..},
shopping{..},
etc. };

REPEAT


“Real life” ⇔ Cyberspace


Cybersecurity Domains
Security Architecture
CASB
Federated Identity
Cloud Security
Data Protection
Network Design
Secure Application Development
Baseline Configuration
Secure System Build
Access Control
Cryptography
Identity Management
Security Engineering
Privileged Access Management
Identity & Access Management
Physical Security
Framework and Standard
COBIT
ISO/IEC
SANS/CSC
NIST
Career Development
Certification
Training
Conferences
Peer Groups
Self Study
Risk Assessment
Vulnerability scan
Assets Inventory
4th Party Risk
3rd Party Risk
Penetration test
Blueteam
Redteam
Social Engineering
Application
Infrastructure
Source Code Scan
Data-Centric Risk Assessment
Data-Flow Map
Blackbox
Whitebox
Governance
Laws and Regulations
Industry Specific
Federal
State
Audit
Executive Management Involvement
Risk Informed
Reports and Scorecards
Company's Written Supervisory Procedures (WSPs)
Compliance & Enforcement
KPIs/KRIs
Policy
Procedure
Guideline
Standard
Threat Intelligence
External
Internal
Contextual
IOCs
Intel. Sharing
User Education
Training (new skills)
Awareness (reinforcement)
Security Operation
DR
Recovery
BCP
Detection
Protection
Prevention
SIEM
SOC
Vulnerability Management
Data Leakage
Active Defense
Incident Response
Breach Notification
Containment
Eradication
Investigation
Forensics

Okay, so how?

Something for everyone

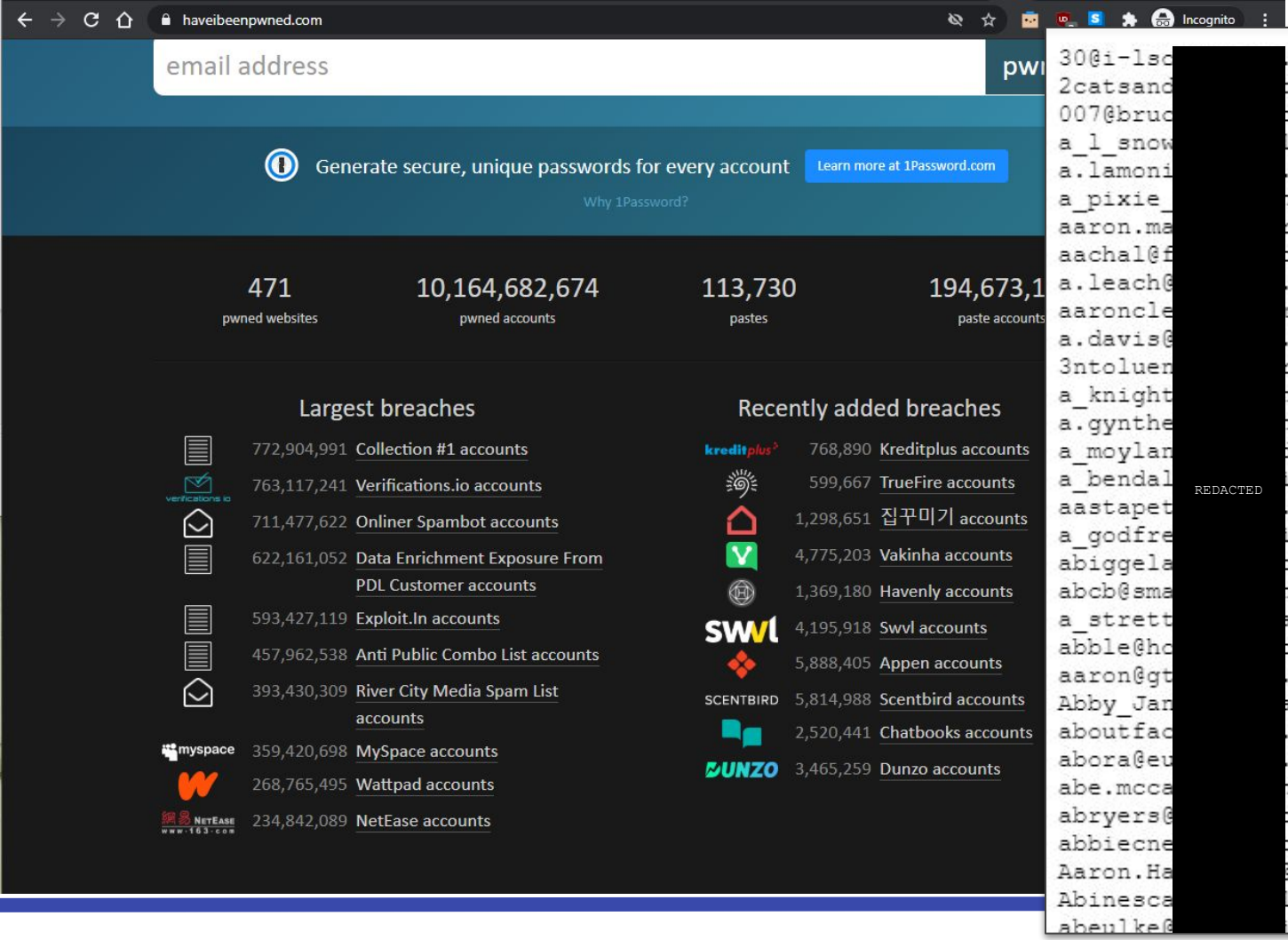
Basic safety & hygiene.

Cyber Hygiene

The 5 little things
we all can do to make us safer.

Use a Password Manager

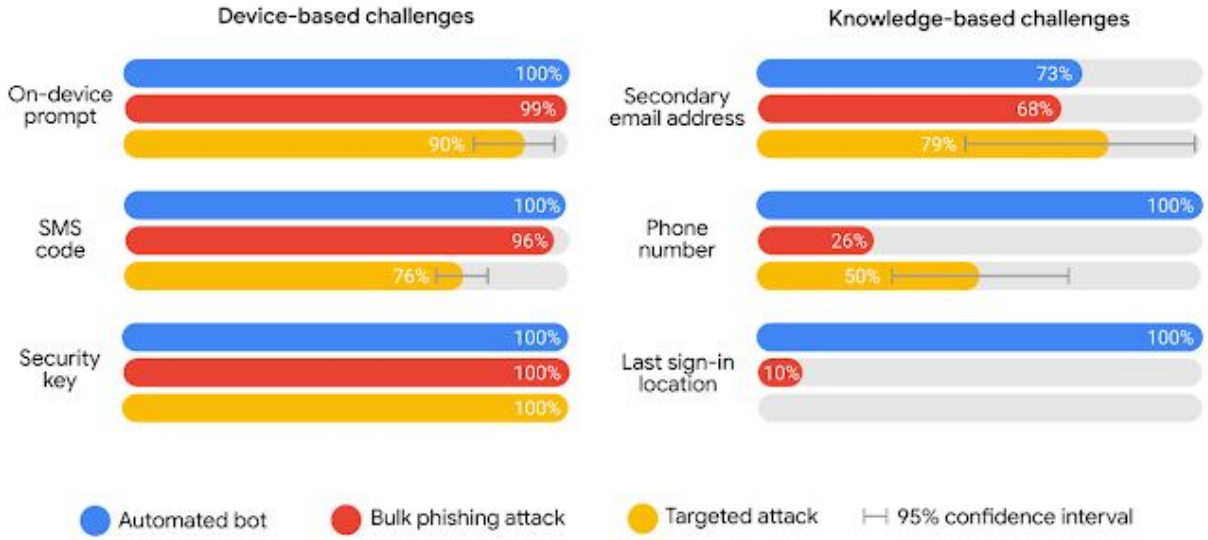
Like a toothbrush, don’t share them with other people(sites).


haveibeenpwned.com
Incognito
email address
pwn
Generate secure, unique passwords for every account
Learn more at 1Password.com
Why 1Password?
471
pwned websites
10,164,682,674
pwned accounts
113,730
pastes
194,673,1
paste accounts
Largest breaches
772,904,991 Collection #1 accounts
763,117,241 Verifications.io accounts
711,477,622 Onliner Spambot accounts
622,161,052 Data Enrichment Exposure From PDL Customer accounts
593,427,119 Exploit.In accounts
457,962,538 Anti Public Combo List accounts
393,430,309 River City Media Spam List accounts
359,420,698 MySpace accounts
268,765,495 Wattpad accounts
234,842,089 NetEase accounts
Recently added breaches
768,890 Kreditplus accounts
599,667 TrueFire accounts
1,298,651 집꾸미기 accounts
4,775,203 Vakinha accounts
1,369,180 Havenly accounts
4,195,918 Swvl accounts
5,888,405 Appen accounts
5,814,988 Scentbird accounts
2,520,441 Chatbooks accounts
3,465,259 Dunzo accounts
30@i-lsc .com:berlin3
2catsand usnet.com.au:zippy
007@bruc m:testing
a_l_snow l.com:macarthur
a.lamoni .com.au:teddyundie
a_pixie_ oo.com:shadow
aaron.ma ts.com.au:isabelle
aachal@f m.au:nehali
a.leach@ .com:buddha
aaroncle ail.com:tash1006
a.davis@ .qld.edu.au:rommel
3ntoluen rmetro.com.au:yarrabee
a_knight et.au:Snowy1
a.gynthe t.qut.edu.au:perfectwor
a_moylan d.net.au:teamoy
a_bendal l.com:celticwicc
aastapet .com.au:aasta
a_godfre l.com:kwyjibo
abiggela .com.au:camster
abcb@sma et.au:bear007
a_strett ail.com.au:calvin
abble@ho m:janerich
aaron@gt .au:nipper
Abby_Jan ail.com:marlie
aboutfac .net.au:Vis!ous2
abora@eu .net:laburdi
abe.mcca oo.com.au:*Caeyahmar
abryers@ m.au:picture
abbiecne o.com:orchid
Aaron.Ha @defence.gov.au:Aaron71
Abinesca l.com:DanC1923
abeulke@ .com:ronald
REDACTED

Use MFA

Confirming it is really you, in more than one way helps better prevent impersonation.

Account takeover prevention rates, by challenge type

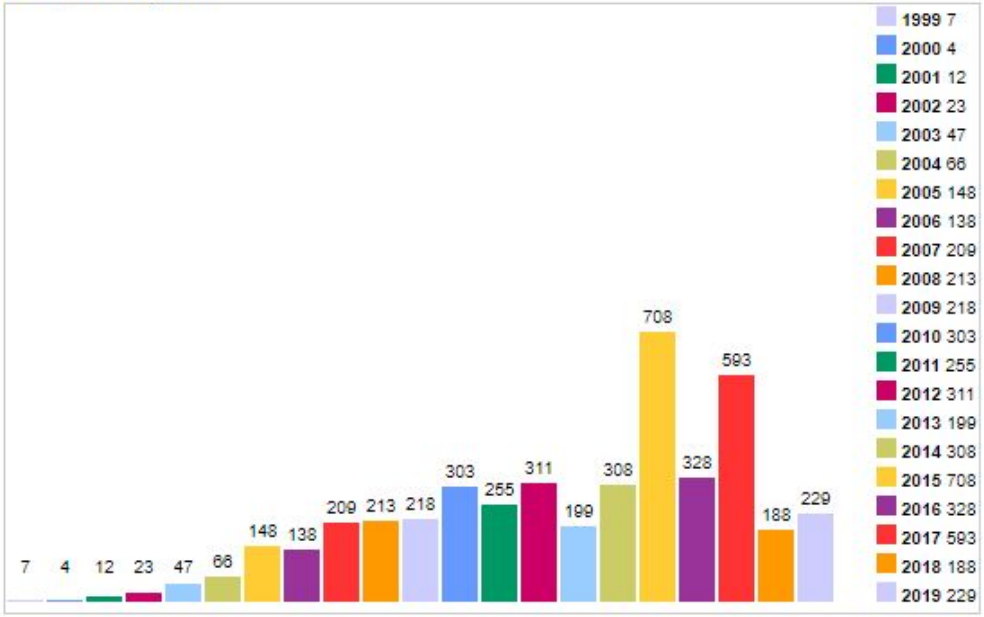


Both device- and knowledge-based challenges help thwart automated bots, while device-based challenges help thwart phishing and even targeted attacks.

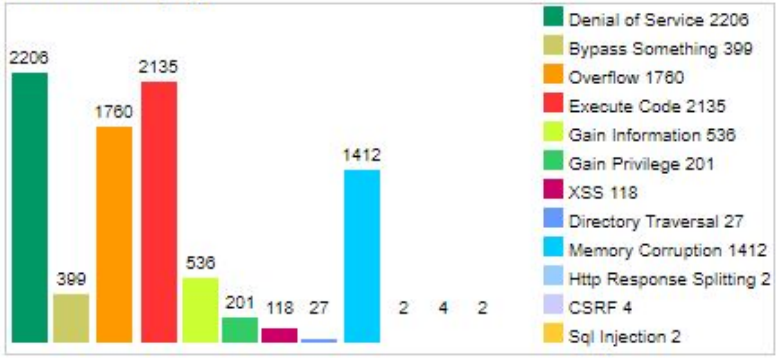
Keep software updated

Issues are often found and fixed.

Vulnerabilities By Year



Vulnerabilities By Type



Publicly Disclosed Vulnerabilities for Apple

Apple : Security Vulnerabilities Published In 2019 (Denial Of Service)

2019 : January February March April May June July August September October November December CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2019-9518	400		DoS	2019-08-13	2019-08-23	7.8	None	Remote	Low	Not required	None	None	Complete

Some HTTP/2 implementations are vulnerable to a flood of empty frames, potentially leading to a denial of service. The attacker sends a stream of frames with an empty payload and without the end-of-stream flag. These frames can be DATA, HEADERS, CONTINUATION and/or PUSH_PROMISE. The peer spends time processing each frame disproportionate to attack bandwidth. This can consume excess CPU.

2	CVE-2019-9517	400		DoS	2019-08-13	2019-08-23	7.8	None	Remote	Low	Not required	None	None	Complete

Some HTTP/2 implementations are vulnerable to unconstrained interal data buffering, potentially leading to a denial of service. The attacker opens the HTTP/2 window so the peer can send without constraint; however, they leave the TCP window closed so the peer cannot actually write (many of) the bytes on the wire. The attacker then sends a stream of requests for a large response object. Depending on how the servers queue the responses, this can consume excess memory, CPU, or both.

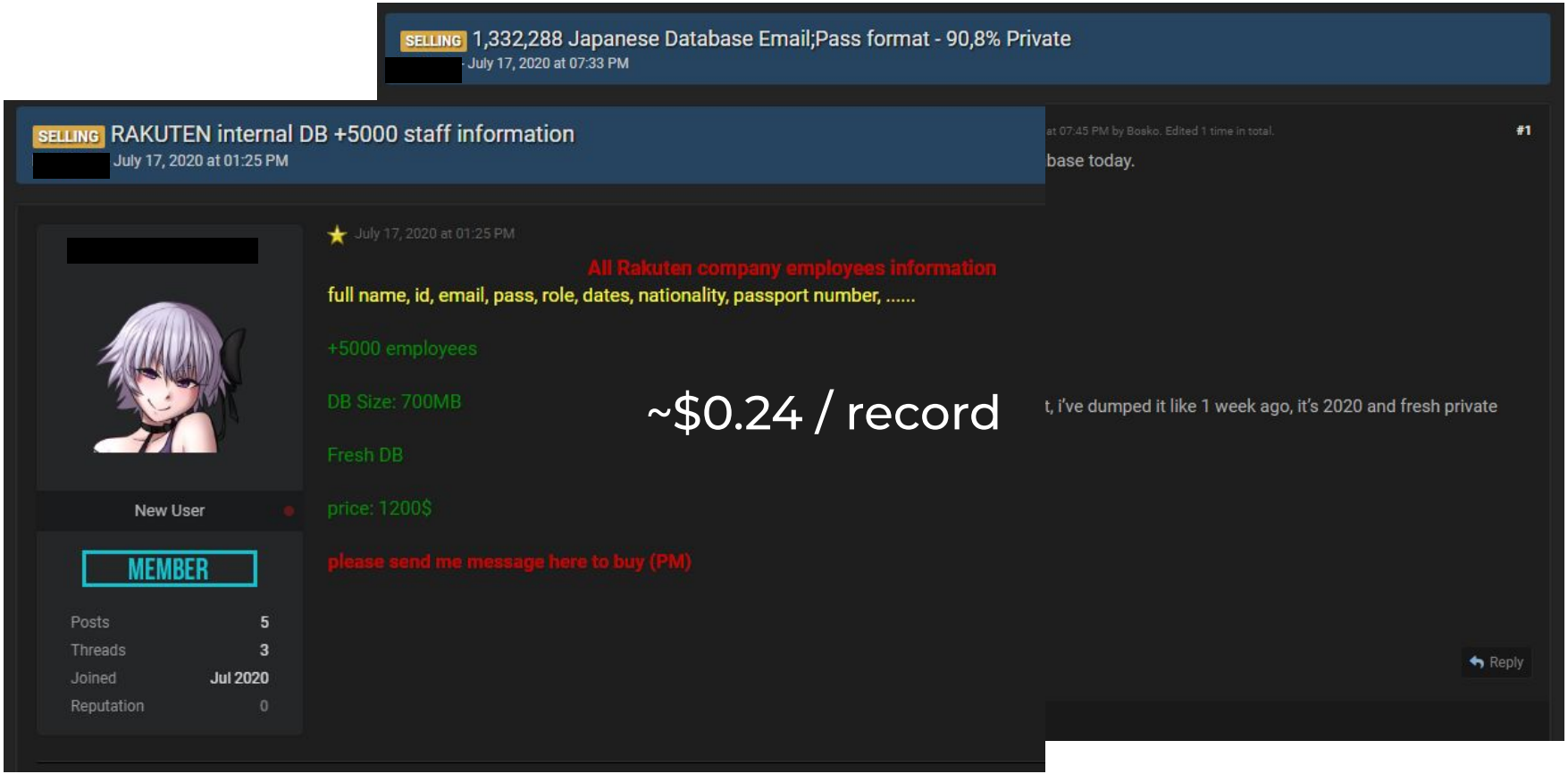
Backup Plan

Murphy’s law happens. Plan for failure, backup your data and critical tools.

Surely, they can't be that evil right?

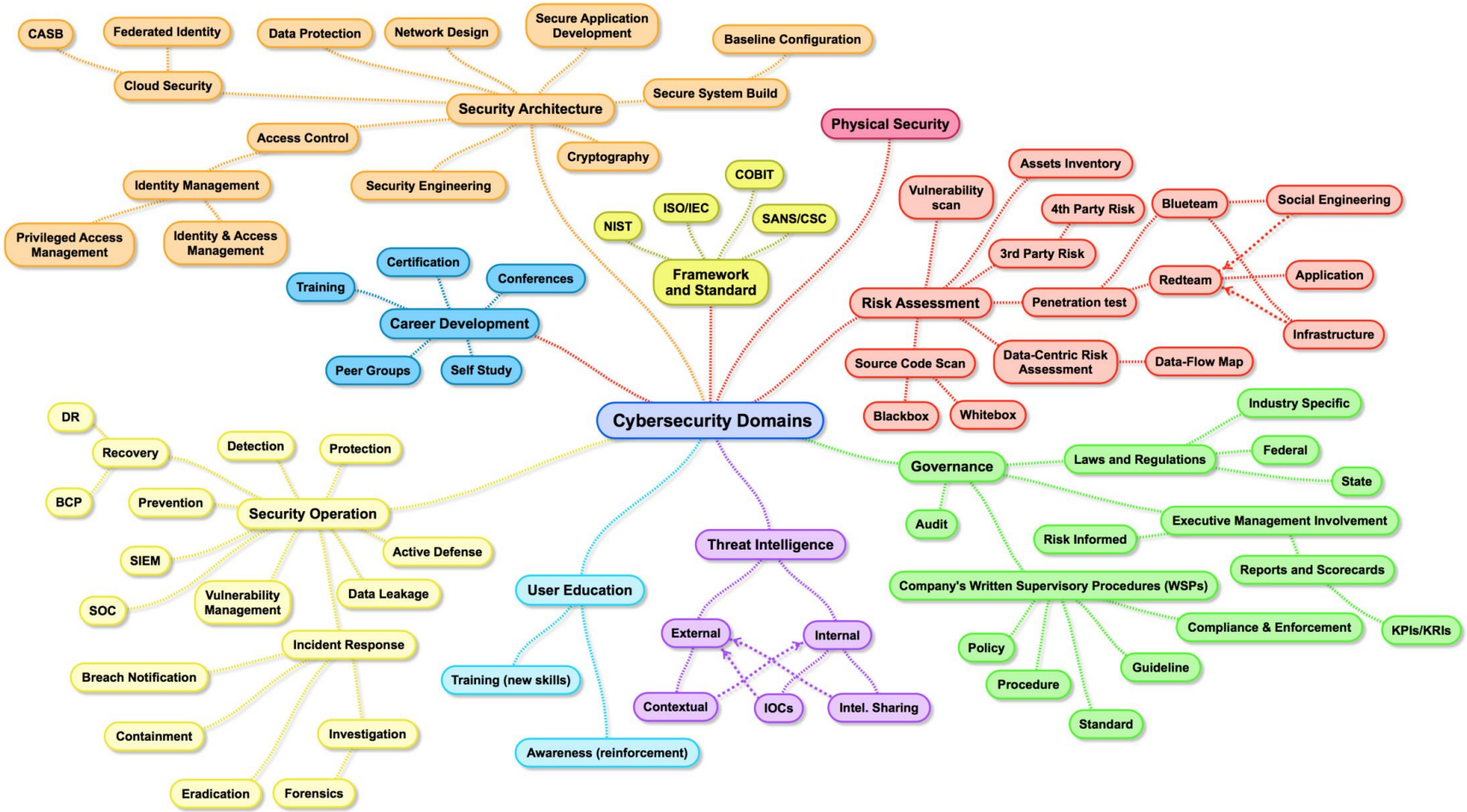
Be a Skeptic

Don’t blindly trust, independently verify.



This could happen to your service provider/employer

Something for Organisations


Cybersecurity Domains
Security Architecture
CASB
Federated Identity
Cloud Security
Data Protection
Network Design
Secure Application Development
Baseline Configuration
Secure System Build
Access Control
Identity Management
Privileged Access Management
Identity & Access Management
Security Engineering
Cryptography
Framework and Standard
COBIT
ISO/IEC
SANS/CSC
NIST
Career Development
Certification
Training
Conferences
Peer Groups
Self Study
Physical Security
Risk Assessment
Vulnerability scan
Assets Inventory
4th Party Risk
3rd Party Risk
Blueteam
Social Engineering
Redteam
Application
Infrastructure
Penetration test
Source Code Scan
Blackbox
Whitebox
Data-Centric Risk Assessment
Data-Flow Map
Governance
Laws and Regulations
Industry Specific
Federal
State
Audit
Executive Management Involvement
Risk Informed
Reports and Scorecards
Company's Written Supervisory Procedures (WSPs)
Compliance & Enforcement
KPIs/KRIs
Policy
Procedure
Guideline
Standard
Threat Intelligence
External
Internal
Contextual
IOCs
Intel. Sharing
User Education
Training (new skills)
Awareness (reinforcement)
Security Operation
DR
Recovery
BCP
Detection
Protection
Prevention
SIEM
SOC
Vulnerability Management
Active Defense
Data Leakage
Incident Response
Breach Notification
Containment
Eradication
Investigation
Forensics

Pick a framework

COBIT
ISO 27001 (ISMS)
ISM/IRAP
OWASP
SOC
PCI-DSS
SABSA
etc...

NIST
Cybersecurity
Framework

Understand the current state

Pick a maturity framework

- Reality check
- Measure progress
- Acts as a checklist

Eg:
ACSC Essential 8,
OWASP SAMM

Understand the risk & consequence

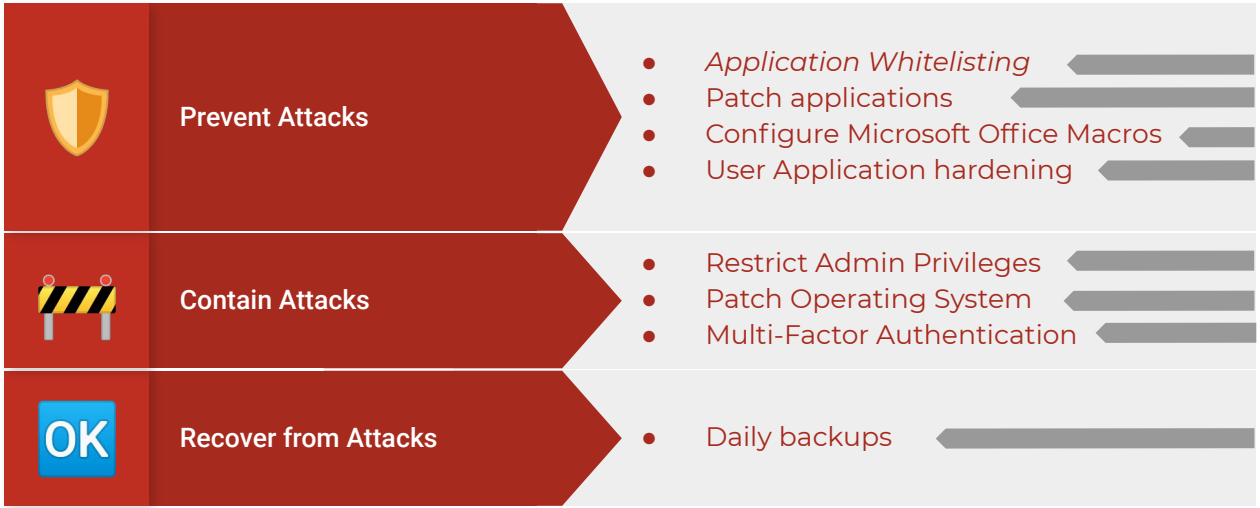
Practice

- Quality requirements, not just functional ones
- Threat modelling
- Keep a risk register
- Take a moment about the risks.

Work towards maturity

- Establish a Security program
- Build defences in depth
- Build awareness and training
- Independently verify your progress

The Basics - ACSC Essential 8



https://www.cyber.gov.au/acsc/view-all-content/essential-eight/essential-eight-maturity-model

5 Security hygiene

1. Use a password manager
2. Use Multi-factor Authentication
3. Keep software updated
4. Have a backup plan
5. Be a skeptic

Thank you.

}; EOF

Questions?

@hellodanielting

daniel.ting@owasp.org