

Rethink risk

Cyber Risk Discussion

presented by: Junaid Amra

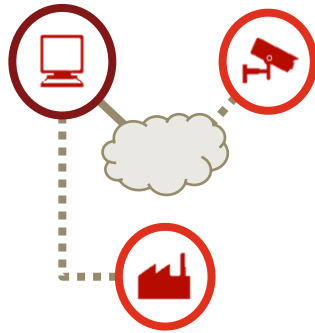


Technology convergence



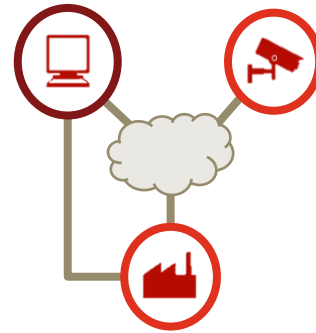
1980s

- IT, OT and CT operate in different environments and on different platforms
- OT and CT are based on proprietary platforms
- Data is not shared between technologies
- **OT and CT face little to no cyber risk since they are not connected to a network**



1990s

- OT is networked to allow centralised operation
- CT remains in a separate environment
- **OT becomes vulnerable due to the connection, but is partially protected by the obscurity of proprietary solutions**



2000s

- OT connects to IT using standardised IT channels to reduce costs and increase compatibility
- Boundaries between IT and OT start to blur
- CT connects to IT through purpose-built channels
- **OT is no longer protected by obscurity and CT is now vulnerable. Traditional IT security does not cover either**



2010+

- The technology underlying IT has become ubiquitous across OT and CT
- The combination of the three represents the integrated technology ecosystem
- **IT, OT and CT are all vulnerable to cyber threats. Businesses must adapt their security model to include the full scope of technologies**



INFORMATION TECHNOLOGY (IT)



OPERATIONAL TECHNOLOGY (OT)



CONSUMER TECHNOLOGY (CT)



INTERNET

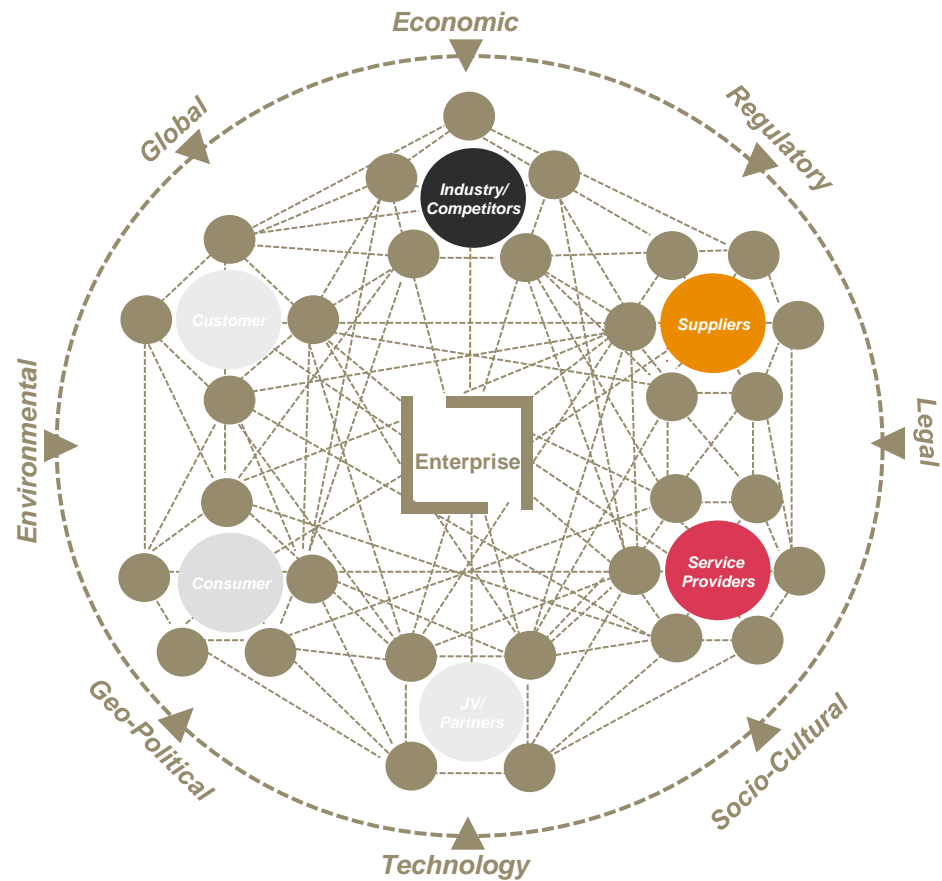


PROPRIETARY CONNECTION



IT PROTOCOL BASED CONNECTION

The new business ecosystem



Mindset

“Cyber security risk is an IT issue”

“We are rushing for the deadline, no time for us to consider security in system development”

“Our system vendors will take care cyber security risk for us”

“We have not been hacked before – do we need security?”

“We have complied to relevant regulatory guidelines, so we will not get hacked!”

“There is no regulatory pressure on cyber security risk”

“We are not a bank – too small to be a target of hackers, right?”

“We have a firewall in place – we are protected.”



Themes observed in 2023 and continuing into 2024

Adversaries



Nation State



Organized Crime and Criminals



Hacktivists



Insiders

Motives



Economic / Military Advantage / Sabotage



Financial Gain



Influence Social or Business Change



Personal or Professional Revenge / Patriotism

Targets



Independent Nation States / R&D / PEPs etc



Everyone



Ideological Supporters



Confidential Information



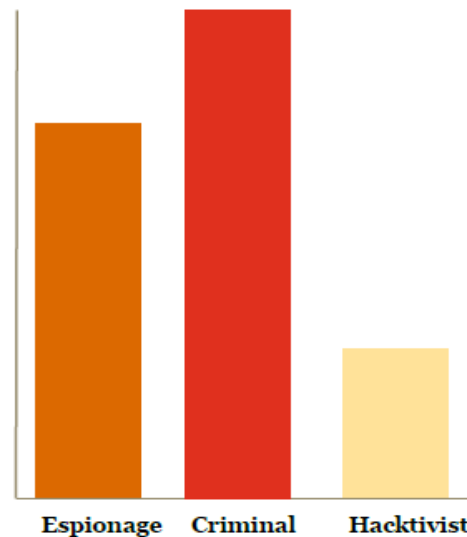
Critical

Severe

Substantial

Moderate

Low



Themes observed in 2023 and continuing into 2024



Zero days and critical vulnerabilities



Geopolitics influencing cyber threat landscape



Supply chain compromises



APT shifts and sophistication



Ransomware and cybercrime at an all-time high

Geopolitical and cyber shifts



Continuation of Russian / Ukraine conflict



October 2023 Middle East conflict



Hactivism increasing alongside conflicts



Throughout 2023 and continuing into 2024, the cyber threat landscape reflected real world events and **geopolitical tensions**, such as the Russian War in Ukraine and the Middle East conflict.

Technology has continued to play an important role in warfare, for example by enabling ground operations and tracking geolocation data.

Ransomware-as-a-Service (RaaS) and scaled operations

Automated and mass



Phish employees and deploy malware to workstations



Exploit vulnerabilities in Internet-facing services

'Human-operated' and targeted



Compromise privileged accounts by exploiting common IT/AD hygiene issues



Move laterally and establish footholds using common offensive security tools



Exfiltrate sensitive data to attacker-operated infrastructure



Deploy ransomware as widely as possible to increase impact

Initial Access



Buy valid credentials



Phishing campaigns



Exploit vulnerabilities
E.g., Log4Shell



Privilege Escalation

Valid accounts
Mimikatz
Rubeus
LSASS
Exploit vulnerabilities
Group policies



Lateral Movement

Cobalt Strike
ADFind
Bloodhound
Metasploit
PsExec
RDP
RDP Facilitator



Data Exfiltration

File compression
WinRAR

Custom tools
ExMatter
StealBit

File transfer utilities
Megasync
NGrok
FTP
WebDAV
PuTTY Secure Copy (PSCP)

Via C2

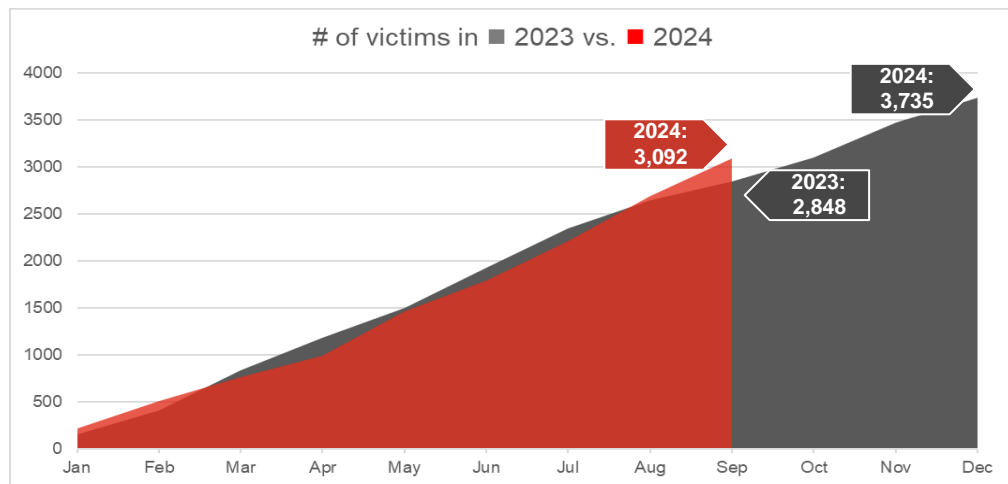


Encrypt Files

Ransomware payload

2024 ransomware leak victims, by the numbers

3092
total victims leaked in the year
(as of September 2024)



Top 10 Sectors	# Victims	% Victims
1. Manufacturing	489	16%
2. Professional Services	367	12%
3. Construction	271	9%
4. Healthcare	230	7%
5. Retail	219	7%
6. Technology	144	7%
7. Food and Agriculture	128	4%
8. Legal	123	4%
9. Education	122	4%
10. Government	117	4%

Supply chain compromises



Software

Alteration, replacement, or bundling of software with malware

Examples: 3CX, SolarWinds



Build platform

Compromise and abuse of trusted development platform or environment

Example: CircleCI



Authentication provider

Theft, forgery, or abuse of valid authentication methods and certificates

Example: Okta



Trusted third party

Abuse of third party or supplier access to downstream networks

Example: Kaseya



Multiple high profile supply chain compromises took place in 2023, with several of the most significant conducted by **North Korea-based threat actors**.

Organizations must be quick to respond to uncovered supply chain compromises to **prevent follow-on action** from threat actors.

What we expect to see in the coming year



Criminals focusing on data extortion



Geopolitical tensions unlikely to dissipate



Lowering barrier to entry

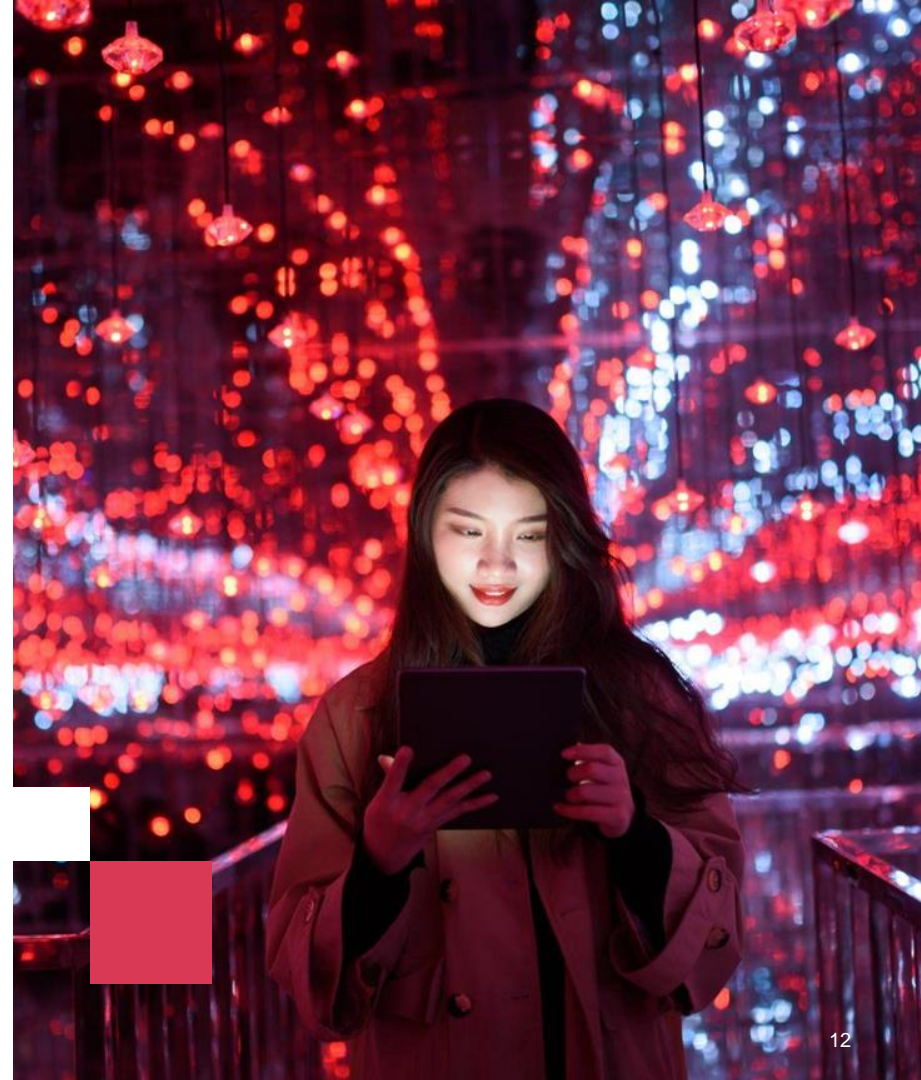


Vulnerabilities and exploits



Credentials are king

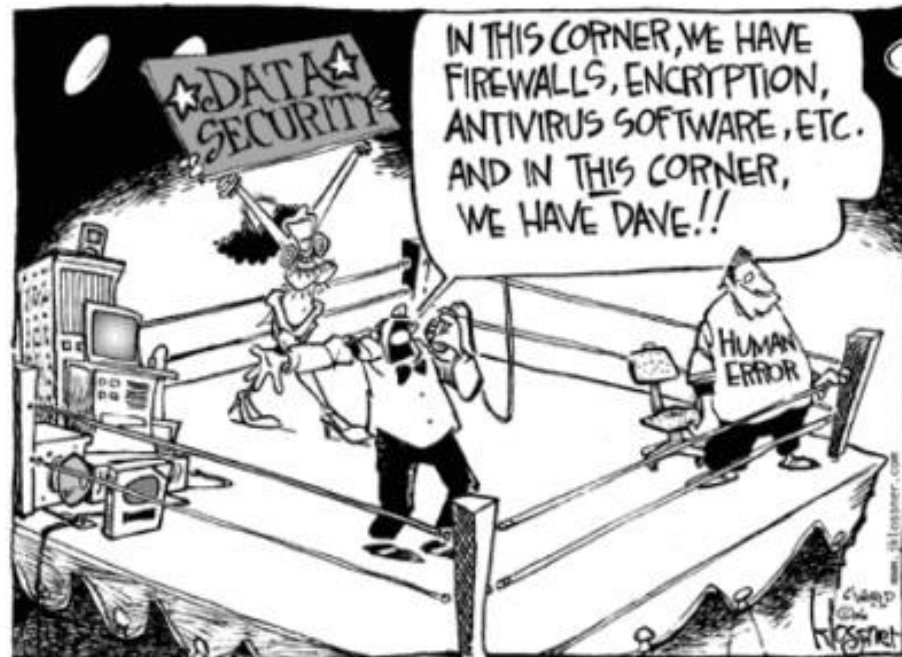
Be vigilant



Local Trends



The weakest link...



App scam



A scammer will call you and try to **lure** you into **clicking** on a **malicious link** to claim your prize or special offer.



The link will install **malware** posing as an app. The scammer may get you to read out an **OTP** that will be sent to your device.



The **malware** may open your selfie camera and take a snap of you.



During this time **money** will be transferred out of your bank account.

DStv scam warning

By Myles Illidge



The airline has urged passengers to report any suspicious offers to its customer service team. Picture: Facebook

Published Oct 9, 2024

Recommendations:

- Download apps from official platforms e.g. Play Store and AppStore
- Don't share information over a phone call
- Strong passwords and two-factor authentication
- Keep devices up to date

Social Media



Image taken by Eleni de Wet in South Africa and posted on her twitter on 4 May 2012.

Criminals can also determine:

If you're out of town

Items they may want to steal

Confidential details of family and friends

Location of loved ones

Etc.

Chinese Man Uses 'SMS Blaster' to Send 1 Million Scam Text Messages From Van

The 35-year-old allegedly drove around Bangkok earlier this month blasting out text messages to nearby phones in the hopes that recipients would click on malicious links.



By [Michael Kan](#) November 25, 2024 [f](#) [X](#) [v](#) [...](#)



US mother gets call from 'kidnapped daughter' - but it's really an AI scam

Jennifer DeStefano tells US Senate about dangers of artificial technology after receiving phone call from scammers sounding exactly like her daughter



📷 Jennifer DeStefano at a Senate hearing in Washington DC on 13 June. Photograph: Shutterstock

Conclusion



Cybersecurity Strategy (including recovery)



Incident Response



Remote working



Employee User Awareness training



Due Diligence / Procurement processes - Technology vendors & 3rd Parties



Assurance Providers



Questions?

Junaid Amra

082 953 9325

junaid.amra@pwc.com

The information is supplied on an "as is" basis and has not been compiled to meet the reader's or his/her entity's individual requirements. It is the reader's responsibility to satisfy him or her that the content meets the individual or his/ her entity's requirements. The information should not be regarded as professional or legal advice or the official opinion of PwC. No action should be taken on the strength of the information without obtaining professional advice. Although PwC take all reasonable steps to ensure the quality and accuracy of the information, accuracy is not guaranteed. PwC, shall not be liable for any damage, loss or liability of any nature incurred directly or indirectly by whomever and resulting from any cause in connection with the information contained herein."

© 2022 PwC Inc. [Registration number 1998/012055/21] ("PwC"). All rights reserved.

PwC refers to the South African member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.co.za for further details.

