

Strategic Cyber Security Report — November 2022 Edition



Andre Camillo, CISSP

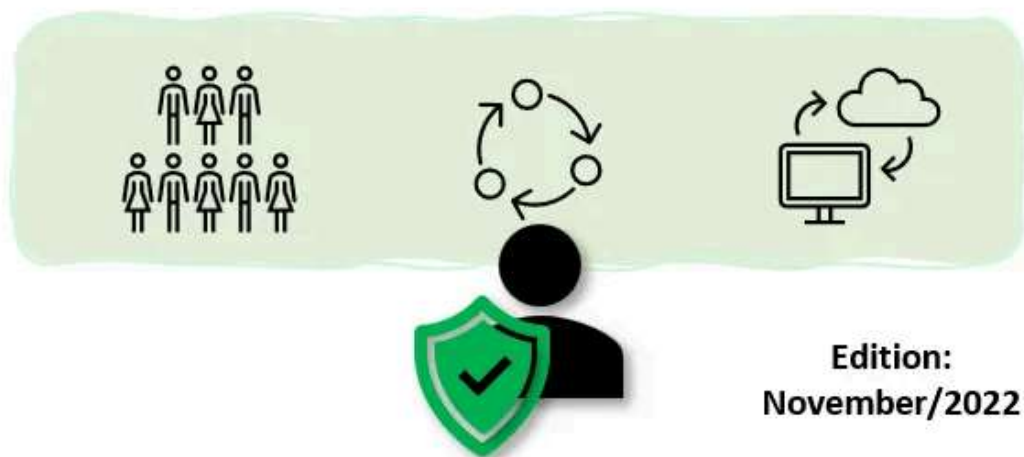
Published in Geek Culture · 5 min read · Dec 1, 2022



22



A Monthly summary of Strategic Information for Cyber Security Leaders



This is a series spun from a need I identified when talking to CISOs — as explained on the kick-off article, this series follows the format of:

What's Top of mind in 3 domains: People, Processes, Technology for CISOs.

People

Essential eight and a people-centric approach

This is an interesting article on how the Australian Essential Eight Framework needs to be complemented by a people-centric approach.

As the article explains, the essential eight is a critical framework for entities in Australia:

The Essential Eight is an Australian cybersecurity framework developed by the Australian Signals Directorate (ASD). Considering the rapid digitalisation leading to expanded attack surfaces, the Australian government aims to significantly improve the cyber resilience of Australian organisations. The government mandates the use of the framework for federal government entities. The government also hopes that the private sector will widely adopt it.

Why the framework needs to be complemented?

Essentially, it's focused on prevention and checklist as the author of the article highlights:

“Organisations that want a simple checklist approach to cybersecurity and have skills to implement recommended controls, can use the ‘Essential Eight’ to identify major gaps in their cybersecurity posture and make changes aligned with their risk

tolerance. But merely following a checklist is not necessarily the key to building a well-protected organisation.”

Using frameworks such as NIST's and/or MITRE ATT&CK that assume breach help put the focus on more relevant, environment specific, imminent risk.

Remaining Medibank breached data dumped by hackers

The Australian Medibank data breach has had its final ramification (from a Data privacy perspective, at least).

Medibank refused to pay the ransom for the data, so the Hackers have dumped all the remaining data in their own blog. This last piece of data was 5GB -big zip file.

The report from ia.acs.org.au, mentions:

In a statement on Thursday morning, Medibank said it was still sifting through the files but that it “appears to be” the stolen data.

“While our investigation continues there are currently no signs that financial or banking data has been taken,” the health insurer said.

“And the personal data, in itself, is not sufficient to enable identity and financial fraud. The raw data we have analysed today so far is incomplete and hard to understand.”

Process

Microsoft Digital Defense Report 2022

Microsoft security teams have released in November the annual Digital Defence Report, 2022 edition — Also known as “MDDR”.

The findings come from Security incident response engagements, signals across its security platform mesh, internal research teams and more.

This year’s edition includes a number of findings related to Nation State actors, with a lot of activity in the Ukraine war. The effect and impact on public services has been felt.

Some impressive numbers I found are:

- how many security incidents could have been prevented by implementing modern security approaches.
- The impact of 5 key activities in order to achieve 98% protection against attacks

I’m not going to summarize the answers to these here, feel free to access the report (link below) or I should write something about it in the coming weeks.

The report [can be accessed publicly here](#).

2022 Interpol Global Crime Trend Summary Report

Interpol [released the first edition of its Global Crime Trend Report](#).

Why is the report relevant? According to Interpol’s Secretary General:

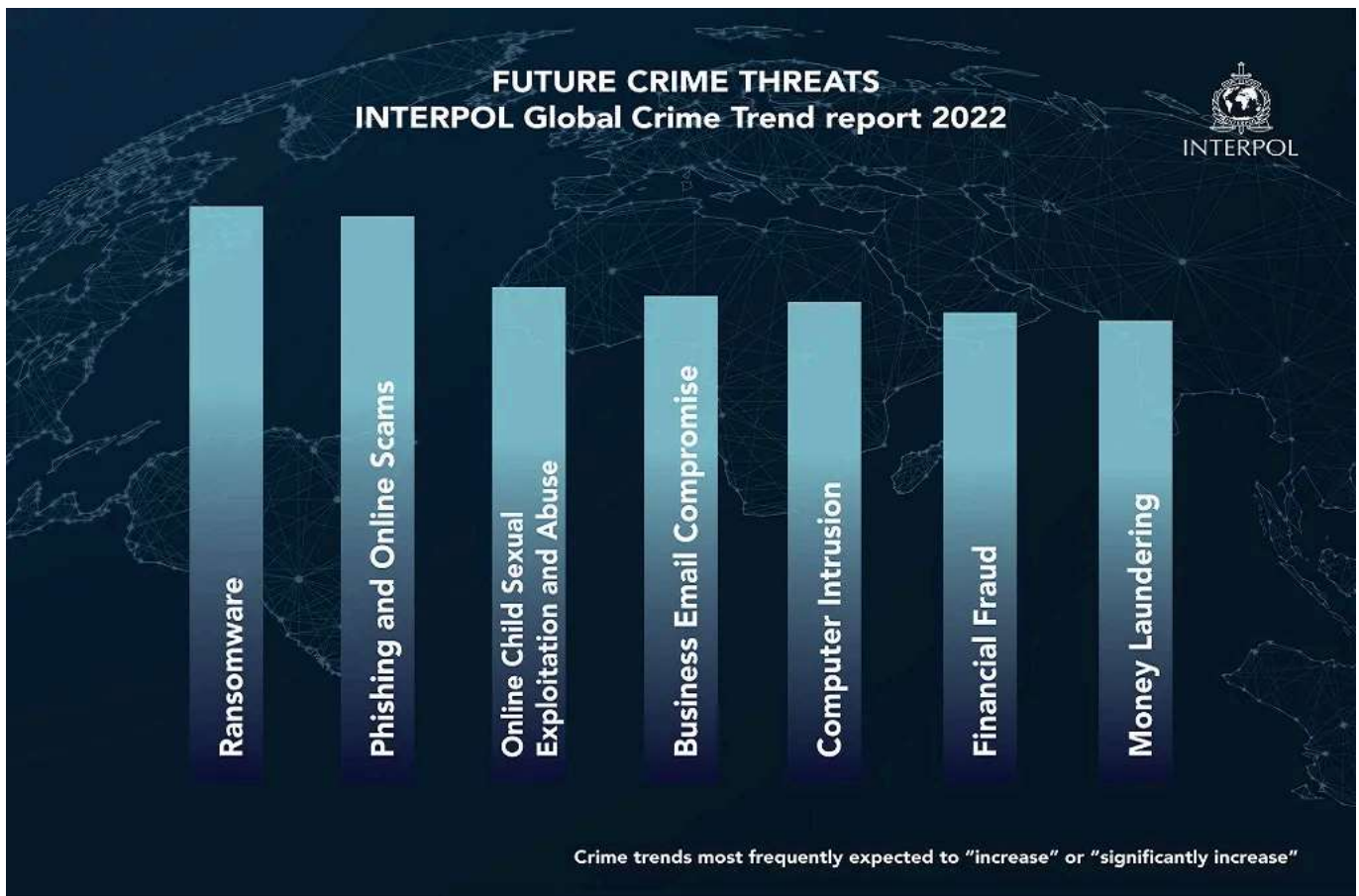
“Understanding and pre-empting crime trends is an absolute bedrock of policing, and INTERPOL’s Global Crime Trend report offers an unparalleled picture of the global crime landscape as seen by police officers around the world.” *Jürgen Stock, INTERPOL Secretary General*

Who’s responded?

It’s restricted to law enforcement, brings together data received from INTERPOL’s 195 member countries alongside information and detailed analysis from the organization’s data holdings and other sources.

Findings include:

- more than 60 per cent of respondents rank crimes such as money laundering, ransomware, phishing and online scams as high or very high threats.
- more than 70 per cent of respondents expect crimes such as ransomware and phishing attacks to increase or significantly increase in the next three to five years.
- While drug trafficking has traditionally dominated crime threat lists, cyber-enabled financial crime has increased precipitously in recent years, notably throughout the global COVID-19 pandemic. During and following lockdowns, rates of digitalization accelerated, with professional and personal activities performed almost exclusively from home and online.
- Future Crime Threats:



source: [Financial and cybercrimes top global police concerns, says new INTERPOL report](#)

NIST's Architecture project for Secure Water and Wastewater utilities

Early in December, National Cybersecurity Center of Excellence (NCCoE) is presenting about the proposed project, Securing Water and Wastewater Utilities: Cybersecurity for the Water and Wastewater Systems.

All details in the official [event page](#).

"The NCCoE is in the initial phase of a project that will result in a reference architecture designed specifically for the Water and Wastewater Systems sector. The project team is currently seeking the public's input on a draft project description, available here: <https://www.nccoe.nist.gov/sites/default/files/2022-11/securing-water-and-wastewater-utilities-project-description-draft.pdf>. We are seeking feedback from all stakeholders in the water and wastewater utilities sector."

Technology

Use Memory Safe Languages

Here's something great to be aware of — according to NSA:

“Microsoft and Google have each stated that software memory safety issues are behind around 70 percent of their vulnerabilities. Poor memory management can lead to technical issues as well, such as incorrect program results, degradation of the program’s performance over time, and program crashes.”

So, NSA issued guidance to use memory safe languages — examples of memory safe language include C#, Go, Java®, Ruby™, Rust®, and Swift®.

Official, full guidance available here: [NSA Releases Guidance on How to Protect Against Software Memory Safety Issues > National Security Agency/Central Security Service > Article](#)

Learn more about my Cloud and Security Projects: <https://linktr.ee/acamillo>

[Consider subscribing to Medium \(here\)](#) to access more content that will empower you!

Thank you for reading and leave your thoughts/comments!

./references

Scattered throughout the document

- Cybersecurity
- Strategy
- Report
- Cloud



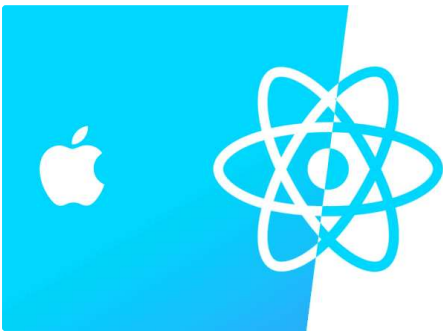
Written by Andre Camillo, CISSP


Edit profile

1K Followers · Writer for Geek Culture

Cloud and Security technologies, Career, Growth Mindset. Follow: <https://linktr.ee/acamillo>.
Technical Specialist @Microsoft. Opinions are my own.

More from Andre Camillo, CISSP and Geek Culture



 Andre Camillo, CISSP in CloudnSec

 Anshul Borawake in Geek Culture

Cybersecurity Careers and Jobs for 2024

I've recently had the chance to talk about Diversity & Inclusion & the cyber security fiel...

★ Feb 21 🖱 52 💬 2



 Masud Afsar in Geek Culture

How to install Node.js by NVM?

Install and manage multiple versions of Node.js with nvm

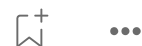
Sep 14, 2021 🖱 201 💬 2




React Native Generate APK— Debug and Release APK

Generate Debug and Release APK in React Native; Windows, iOS and Linux

Apr 4, 2021 🖱 1.8K 💬 11



 Andre Camillo, CISSP in CloudnSec

Microsoft Defender for Endpoint on Linux—Manual Scan Tips

Deploying and managing Defender for Endpoint on linux at Scale is something you'l...

Feb 14 🖱 154



See all from Andre Camillo, CISSP

See all from Geek Culture

Recommended from Medium