Strategic Cyber Security Report—October 2022 Edition

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

Data breaches

Whilst not directly related to people, data breaches affect people in many ways—from PII exposure to mental health and October was a month full of news on this matter, so a recap with some backing data on the impact of Data breaches.

- ***1. Aussie's breaches many implications***

Optus' 10M users breach impact could reach upwards to 5M for privacy breach. But accountability is yet to be defined as reported by afr.com:

"The accountability for any potential failings by Optus is yet to be established and shareholders may reasonably expect to know the findings of the investigation before supporting Ms Bayer Rosmarin as a director."

Medibank followed suit, having data of more than 4M users breached. MSN.com reported:

the private health provider revealed the cyber attack on its customers' data was much wider than originally thought, and could impact about 4 million current customers along with an unknown number of former customers too.

The company said the data breach impacted its main brand, budget insurance company sub-brand ahm and data collected about international students studying in Australia who use Medibank under its OSHC service.

Late this month, Australian Defense force was also breached as reported:

Hackers have attacked an external IT provider used by military personnel and Defence department public servants.

A spokeswoman for Defence Minister Richard Marles confirmed to NCA NewsWire a breach had taken place on the ForceNet service.

She said no personal data had been compromised.

Implications include an increase on the penalties for Data breaches in Australia, announced on 22nd of October—report by IAPP:

Australia Attorney-General Mark Dreyfus introduced to the Parliament of Australia a bill to "significantly increase penalties for repeated or serious privacy breaches." The Privacy Legislation Amendment Bill 2022 proposes increases to the current fine scheme under The Privacy Act 1988, which carries a maximum fine of AU$2.22 million. Under the proposed three-factor scheme, violators face a AU$50 million fine or penalties based on data monetization and 30% of adjusted quarterly turnover. "It's not enough for a penalty for a major data breach to be seen as the cost of doing business," Dreyfus said, noting the bill is a response to recent data breaches involving Optus and MyDeal.

- ***2. This might also be worth knowing*** Microsoft Data Breach Exposed Customer Data of 65,000 Organizations, Redmond Lashes Out at Security Firm—CPO Magazine
- ***3. AirNZ faced a cyber breach reported Stuff nz:***

Multiple Air New Zealand customers have been locked out of their accounts after the airline took action against a cyber breach.

The breach was an instance of "credential stuffing", in which scammers used email and password information stolen from another online source to hack into Air NZ Airpoints accounts.

Air New Zealand chief digital officer Nikhil Ravishankar said the instance was not a hack or breach of the company's security systems, but of individual accounts.

- ***4. With all this in mind, a report found that in Q3 2022***, Data breaches soared by 70%, according to this report:

"Q3 of 2022 showed a 70% increase in breaches compared to Q2, and while this number is lower than last year, it's still an increase," Surfshark noted.

Russians continued to be the top most breached people in Q3 2022 (22.28 million) after dethroning the U.S. (which had been the most breached country for a few years) in Q1 this year, corresponding to the conflict in Ukraine. However, their contribution to the list of data breaches continued to decline (24.59 million in Q2 2022, 42.99 million in Q1 2022).

Microsoft cybersecurity program

Microsoft announces expansion of cybersecurity skilling program Cybershikshaa in India:

Aiming to build a strong pool of diverse cybersecurity talent in the country, CyberShikshaa launched by Microsoft and DSCI in 2018, has successfully trained 1,100 women and employed more than 800 women through multiple training batches. More than 5000 underserved youth have also been trained in Cybersecurity Beginners modules. CyberShikshaa for Educators with ICT Academy, the latest addition to the CyberShikshaa portfolio launched in June 2022 for providing cybersecurity training to 400 faculty members, will help build cybersecurity careers for 6,000 underserved students across 100 rural technical institutions and facilitate job opportunities for over 1,500 students.

Process

New Healthcare cybersecurity standards and Guidance from the US

The White house is aiming at releasing new Healthcare cybersecurity standards and guidance soon, according to Anne Neuberger, deputy national security advisor for cyber and emerging technology in the Biden Administration. The report is from healthitsecurity.com:

Specifically, Neuberger pointed to the healthcare, water, and communications sectors as the next three cybersecurity focus areas for the White House, furthering the administration's emphasis on critical infrastructure security.

Technology

Microsoft Ignite

This month Microsoft Ignite happened with many announcements across (virtually) all enterprise services. A full list of all announcements is available in the Ignite book of news.

Personally, these are worth knowing (all details in the book of news):

- ***Security***

Microsoft Defender Cloud: Microsoft Defender for DevOps (Preview)

Microsoft Defender Cloud: Security Posture Management (CSPM) (Preview)

M365 Defender: Automatic attack disruption (Preview)

Microsoft Defender for Endpoint: Limited-time sale of P1/P2–50% off

- ***Compliance***

Microsoft Purview Information Protection for Adobe Document Cloud

New data loss prevention capabilities (Preview)

eDiscovery (Premium) will support the ability to discover the version of the document

eDiscovery (Premium) now includes capturing reactions

- ***Identity***

Microsoft Entra Identity Governance (Preview)

Lifecycle Workflows (part of identity governance, Preview)

Conditional Access Authentication Strengths

Upcoming OpenSSL bug

An advisory released late October advises of a new flaw on OpenSSL 3.0 that will be revealed after the release of its new version (OpenSSL 3.0.7) on November 1st. According to Darkreading:

On Tuesday, Nov. 1, the project will release a new version of OpenSSL (version 3.0.7) that will patch an as-yet-undisclosed flaw in current versions of the technology. The characteristics of the vulnerability and ease with which it can be exploited will determine the speed with which organizations will need to address the issue.

The concern is for this bug to be another "Heartbleed"—from 2014. And the infrastructure affected by the deployment of the then vulnerable OpenSSL version.

If the new vulnerability turns out to be another Heartbleed bug—the last critical vulnerability to impact OpenSSL—organizations and indeed the entire industry are going to be under the gun to address the issue as quickly as possible.

Beware—there's no CVE assigned to it yet.

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