Security News Digest
Information Security Branch
BRITISH COLUMBIA OCIO Office of the Chief Information Officer

November 15, 2022

Challenge yourself with our Online Shopping Security Quiz

This past week’s stories:

🍁 Auditor general calls for stronger federal action on cloud cybersecurity

🍁 Sobeys data breach serves as wake up call for industry: expert

🍁 Taking down a ransomware hacker

🍁 UK, Canada and Singapore join forces to secure IoT devices

Cybersecurity: These are the new things to worry about in 2023

New security measure for Queensland driver licence following Optus hack

Why businesses shouldn't cut cybersecurity costs—especially during a crisis

'We warned you': Medibank hackers leak sensitive data related to customers' mental health and alcohol-related issues

Huge cyber security skills shortage amid six-figure salaries on offer

How Google and Mandiant are forging synergies in cyber security

Twitter chaos after wave of blue tick impersonations

“We know who are” says AFP to Medibank hackers

After hack, Thales defense and security project data yet to appear on dark web

Darktrace says business demand is high for AI-based proactive cybersecurity

Exclusive: Russian software disguised as American finds its way into U.S. Army, CDC apps

---

Auditor general calls for stronger federal action on cloud cybersecurity

The federal auditor general says government departments have not always effectively implemented measures to ensure secure storage of information in the digital cloud.

In a report tabled in Parliament today, Karen Hogan says requirements were not always clear for putting information in the cloud -- computer servers located in data centres.

https://www.ctvnews.ca/politics/auditor-general-calls-for-stronger-federal-action-on-cloud-cybersecurity-1.6153624

Click above link to read more.

Back to top

Sobeys data breach serves as wake up call for industry: expert

Sylvain Charlebois, a food researcher and professor at Dalhousie University in Halifax, said the industry has been particularly vulnerable to cyberattacks in recent weeks.

He said this most recent incident, which Sobeys has said is now resolved, is going to serve as a bit of a wake-up call for the country’s agri-food sector because of the high-value, low-margin nature of the industry.

https://globalnews.ca/news/9271365/privacy-sobeys-data-breach-perscriptions/

Click above link to read more.

Back to top

Taking down a ransomware hacker

In the early morning hours of Jan. 27, 2021, two police forces descended on a snowy cul-de-sac in Gatineau, Que., each tasked with an important role in one of the largest-ever ransomware takedowns in Canada.

Members of the RCMP, led by the cybercrime unit, were executing a search warrant at a white brick house on the street, while the Gatineau police service was on hand to make an arrest on behalf of the FBI. The codename for the operation was Project Olunar.

https://www.cbc.ca/newsinteractives/features/takedown-homegrown-ransomware-hacker

Click above link to read more.

Back to top

UK, Canada and Singapore join forces to secure IoT devices

The UK, Canada, and Singapore are joining forces to improve the security of IoT devices.

In a joint statement, the governments of the respective countries noted the economic and social benefits of IoT devices. However, they also warned of the risks of insecure IoT devices not just to consumers' own security, privacy, and safety, but also to the broader economy through large-scale cyberattacks.

https://www.iottechnews.com/news/2022/nov/10/uk-canada-and-singapore-join-forces-secure-iot-devices/

Click above link to read more.

Back to top

Cybersecurity: These are the new things to worry about in 2023

A year is a long time in cybersecurity.

Certainly, there are some constants. Ransomware has been a major cybersecurity issue for years, but shows no signs of going away as cyber criminals continue to evolve their attacks. And significant numbers of enterprise networks remain vulnerable, often as a result of security flaws for which updates have long been available.

https://www.zdnet.com/article/cybersecurity-these-are-the-new-things-to-worry-about-in-2023/

Click above link to read more.

Back to top

New security measure for Queensland driver licence following Optus hack

Queensland has changed the way a resident's identity can be verified when using a driver's licence in light of major data breaches like Optus and Medibank.

The new layer of protection means organisations like banks and telecommunication companies will use two-factor verification to confirm a person's identity from Monday, November 7.

This verification will be done through the Australian government's document verification service.

https://www.9news.com.au/national/queensland-security-verification-change-drivers-licence-optus-hack/274cdd6f-c7ad-4d97-9cd0-bc8c4d4d8651

Click above link to read more.

[Back to top](#)

Why businesses shouldn't cut cybersecurity costs—especially during a crisis

The global economy has been shaken enough times in the past two years for some experts to say the world will likely enter another recession soon. While it's essential to work on a renewed crisis management plan, it's always a question of what to prioritize and which costs to minimize while preserving the quality of your product. This rethinking can have a major impact on the processes of small- and medium-sized companies.

In evaluating risks, it might seem reasonable at first to eliminate the costs that don't directly affect production. If your business has never been exposed to a real cyber threat before, expenses for security systems might seem too pricey—a common misconception.

https://www.forbes.com/sites/forbestechcouncil/2022/11/10/why-businesses-shouldnt-cut-cybersecurity-costs-especially-during-a-crisis/?sh=66ed2fa13189

Click above link to read more.

[Back to top](#)

'We warned you': Medibank hackers leak sensitive data related to customers' mental health and alcohol-related issues

The hackers behind the Medibank data breach have released more personal information linked to mental health status and alcohol abuse of customers.

Around 241 private medical details were posted on an online ransomware forum on Friday, marking the third release from the hackers in three days.

https://www.skynews.com.au/australia-news/we-warned-you-medibank-hackers-leak-sensitive-data-related-to-customers-mental-health-and-alcohol-issues/news-story/e25c25ce5cebf5864247b1b645ed37b9

Click above link to read more.

[Back to top](#)

Huge cyber security skills shortage amid six-figure salaries on offer

Australia’s cyber security sector could soon experience a shortage of thousands of workers just as the nation is under increased attack from online criminals.

Australia’s Cyber Security Sector Competitiveness Plan from AustCyber has been released this week, outlining the risk to the community as the threat from hackers grows.

The report found the industry will face a shortage of 3000 cyber security workers by 2026.

https://www.news.com.au/technology/online/security/huge-cyber-security-skills-shortage-amid-sixfigure-salaries-on-offer/news-story/c15a07eb13dda563a532e5d710c8153c

Click above link to read more.

Back to top

How Google and Mandiant are forging synergies in cyber security

Just over a month after Google completed its purchase of Mandiant, the cloud provider has demonstrated its synergies with its latest acquisition, baking threat intelligence capabilities into its Chronicle security operations platform.

Called Mandiant Breach Analytics for Chronicle, the offering combines Mandiant’s threat intelligence with Chronicle’s threat detection capabilities.

https://www.computerweekly.com/news/252527228/How-Google-and-Mandiant-are-forging-synergies-in-cyber-security

Click above link to read more.

Back to top

Twitter chaos after wave of blue tick impersonations

A wave of new paid blue tick accounts impersonating influential individuals and brands has led to chaos and confusion on Twitter.

Fake "verified" accounts in the names of politicians, celebrities, major organisations and businesses started appearing on the platform on Thursday.

https://www.bbc.com/news/technology-63599553

Click above link to read more.

Back to top

“We know who are” says AFP to Medibank hackers

The hackers responsible for a cyber attack against Australian health insurer Medibank have been identified by the Australian Federal Police (AFP) as being associated with Russia.

The breach, which was initially identified on October 13, saw 200GB of data stolen, 9.7 million people affected and the private medical details for a significant number of people distributed on the dark web.

https://www.cshub.com/attacks/news/we-know-who-are-says-afp-to-medibank-hackers

Click above link to read more.

Back to top

After hack, Thales defense and security project data yet to appear on dark web

French defense and aerospace firm Thales was attacked by hackers last week, with company data having been published on the dark net. However, sources close to the matter tell Breaking Defense that the published data is not linked to any of the company’s major defense or national security programs.

The sources, speaking under condition of anonymity, expressed confidence that military and security projects were not affected by the breach, but admitted that it’s possible information was stolen that has yet to be discovered or made public. Even with that caveat, that sensitive defense information has yet to become public is a good sign for the firm.

https://breakingdefense.com/2022/11/after-hack-thales-defense-and-security-project-data-yet-to-appear-on-dark-web/

Click above link to read more.

Back to top

Darktrace says business demand is high for AI-based proactive cybersecurity

In the midst of data breaches impacting Australia, cybersecurity provider Darktrace says it is receiving strong demand from the market for its new Darktrace Prevent product family as organisations seek to proactively prevent cyber attacks, rather than waiting for breaches to happen.

Darktrace further says since Prevent became generally available in August 2022 it has seen the longest list of customer opt-ins than for any other Darktrace product launch ever.

https://itwire.com/business-it-news/security/darktrace-says-business-demand-is-high-for-ai-based-proactive-cybersecurity.html

Click above link to read more.

Back to top

Exclusive: Russian software disguised as American finds its way into U.S. Army, CDC apps

Thousands of smartphone applications in Apple (AAPL.O) and Google's (GOOGL.O) online stores contain computer code developed by a technology company, Pushwoosh, that presents itself as based in the United States, but is actually Russian, Reuters has found.

The Centers for Disease Control and Prevention (CDC), the United States' main agency for fighting major health threats, said it had been deceived into believing Pushwoosh was based in the U.S. capital. After learning about its Russian roots from Reuters, it removed Pushwoosh software from seven public-facing apps, citing security concerns.

https://www.reuters.com/technology/exclusive-russian-software-disguised-american-finds-its-way-into-us-army-cdc-2022-11-14/?mkt_tok=MTM4LUVaTS0wNDIAAAGIG26A4XwhSVf7Rn9tsy2xn2hgDJCNurm-K1VGf736TMG5BhUe33zhvPEQD2st3_ofocbJytu9cM3Sy6Mst-b_B1jPQt3juSUWzKyVV8gwm-BP

Click above link to read more.

Back to top

Click unsubscribe to stop receiving the Digest.

****

The Security News Digest (SND) is a collection of articles published by others that have been compiled by the Information Security Branch (ISB) from various sources. The intention of the SND is simply to make its recipients aware of recent articles pertaining to information security in order to increase their knowledge of information security issues. The views and opinions displayed in these articles are strictly those of the articles' writers and editors and are not intended to reflect the views or opinions of the ISB. Readers are expected to conduct their own assessment on the validity and objectivity of each article and to apply their own judgment when using or referring to this information. The ISB is not responsible for the manner in which the information presented is used or interpreted by its recipients.

For previous issues of Security News Digest, visit the current month archive page at:

http://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/security-news-digest

To learn more about information security issues and best practices, visit us at:

https://www.gov.bc.ca/informationsecurity

OCIOSecurity@gov.bc.ca

The information presented or referred to in SND is owned by third parties and protected by copyright law, as well as any terms of use associated with the sites on which the information is provided. The recipient is responsible for making itself aware of and abiding by all applicable laws, policies and agreements associated with this information.

We attempt to provide accurate Internet links to the information sources referenced. We are not responsible for broken or inaccurate Internet links to sites owned or operated by third parties, nor for the content, accuracy, performance or availability of any such third-party sites or any information contained on them.

Security News Digest
Information Security Branch

BRITISH COLUMBIA OCIO Office of the Chief Information Officer