Security Digest
Information Security Branch
British Columbia
OCIO
Office of the Chief Information Officer

February 26th, 2019

February is Cyberbullying Month

This week's stories:

- BlackBerry completes acquisition of Cylance 🇨🇦
- B.C. privacy commissioner launches awareness campaign for firms 🇨🇦
- Stolen unencrypted NWT laptop held sensitive health information: News report 🇨🇦
- Why some countries are building 'walls' in the worldwide web
- Cost of cyber breach recovery hits all-time high of $5.8M: Scalar Security Study
- Some airplane seats have built-in cameras – but companies say they've never been used
- 2019 data security predictions
- Data Breach Notification: California Targets 'Loopholes'
- UConn Health Among the Latest Phishing Victims

BlackBerry completes acquisition of Cylance 🇨🇦

https://www.itworldcanada.com/article/blackberry-completes-acquisition-of-cylance/415246

BlackBerry Ltd. has completed its largest acquisition ever, the Waterloo, Ont.-based company announced today.

First announced November 2018, the $1.4 billion acquisition of Cylance is a major move for BlackBerry, which has had its eyes on Cylance's security solutions – most of which include embedded AI and machine learning capabilities – for some time. BlackBerry has made it clear that the endgame is to integrate those capabilities into its own end-to-end secure communications portfolio, and accelerate the development of BlackBerry Spark, the secure communications platform for the Internet of Things.

Click link above to read more

B.C. privacy commissioner launches awareness campaign for firms 🇨🇦

https://www.itworldcanada.com/article/b-c-privacy-commissioner-launches-awareness-campaign-for-firms/415265

Why are Canadian businesses often caught violating customers' privacy rights, not protecting personal data they hold and victimized by data breaches?

One answer is they don't know they have to follow provincial and federal privacy laws. It may be even worse.

"Frankly, judging by some of the phone calls we get, some don't even know there is privacy legislation," says Michael McEvoy, British Columbia information and privacy commissioner.

Click link above to read more

Stolen unencrypted NWT laptop held sensitive health information: News report 🇨🇦

https://www.itworldcanada.com/article/stolen-unencrypted-nwt-laptop-held-sensitive-health-information-news-report/415414

Encrypting data isn’t cheap, nor is it necessarily easy. However, as the case of a laptop stolen in Ottawa last year shows, the damage to people can be high.

The laptop belonged to an employee of the Northwest Territories’ department of health and social services, in the national capital last May on a business trip. It was in a backpack in a minivan without a trunk that was broken into. The laptop was used to do statistical analysis on thousands of health records –almost everyone in the N.W.T — had a strong login password.

Click link above to read more

Why some countries are building ‘walls’ in the worldwide web

https://globalnews.ca/news/4987866/internet-censorship-china-india-russia/

Former U.S. President Bill Clinton once laughed at China for trying to censor the internet.

“Good luck,” he said, during a speech at Johns Hopkins University in 2000. “That’s sort of like trying to nail Jell-O to the wall.”

After 19 years, China has become so good at “nailing Jell-O to the wall” that other nations are asking how they can do it too. China’s so-called “Great Firewall” filters everything that Chinese internet users see, blocking controversial content – including political speech – and funneling a vast amount of personal data back to government authorities watching for dissent.

Click link above to read more

Cost of cyber breach recovery hits all-time high of $5.8M: Scalar Security Study

https://www.canadiansecuritymag.com/news/data-security/cost-of-cyber-breach-recovery-hits-all-time-high-of-$58m

Cyber security incidents have become the new normal for Canadian companies, with 100 per cent of organizations experiencing attacks, according to the findings of a new study from Scalar Decisions Inc. of more than 400 Canadian IT and security workers.

The 2019 Scalar Security Study (commissioned by Scalar and conducted independently by IDC Canada) found that the average cost per organization of responding to, and recovering from, cyber security incidents increased to between $4.8 million to $5.8 million, up from $3.7 million last year.

Despite facing fewer cyber-attacks overall (440 on average, down from 445 last year), organizations suffered more breaches (12.5 on average, up from 9.3) as bad actors became more efficient and effective.

Click link above to read more

Some airplane seats have built-in cameras – but companies say they’ve never been used

https://globalnews.ca/news/4988225/airplane-seat-cameras/

A viral photo shows something you might not expect: a camera lens looking back at you in your airplane seat.

The photo posted online partially shows the entertainment system on a Singapore Airlines flight — along with a small lens below the familiar screen.

Click link above to read more

2019 data security predictions

https://www.canadiansecuritymag.com/news/data-security/2019-data-security-predictions

What to expect this year as new data privacy regulations take hold and IT skillsets take on a premium role in the enterprise

Privacy-first becomes a priority

As government agencies increasingly cite enterprises for non-compliance with the European Union's GDPR and other strict data privacy regulations, and other governments implement new data privacy regulations, enterprises will increasingly adopt a "Privacy First" approach to data management. We've seen this discussion quite a bit in the Waterfront Toronto / Sidewalk Labs (smart cities) project where the push for "privacy by design" has come to the forefront. Canada recently expanded its own data privacy act (PIPEDA) to include much more stringent requirements around record keeping for data breaches and notifications of those incidents to the public. However, the challenges enterprises will face as they seek to integrate data privacy best practices into their existing applications, as well as new mobile, IoT and other applications, will be significant. Enterprises will need AI-powered, automated, outcome-driven data management solutions to address these challenges if they hope to implement strong data privacy policies without sacrificing productivity or agility.

Click link above to read more

Data Breach Notification: California Targets 'Loopholes'

https://www.databreachtoday.com/data-breach-notification-california-targets-loopholes-a-12047

A proposed California law would expand the state's pioneering data breach notification requirements to include breaches of biometric data and passport numbers.

California Attorney General Xavier Becerra on Thursday announced the proposed law, AB 1130, saying it would close a loophole in the state's current breach notification law.

The state's current data breach law doesn't require organizations to notify individuals if their passport number has been exposed.

Click link above to read more

UConn Health Among the Latest Phishing Victims

https://www.databreachtoday.com/uconn-health-among-latest-phishing-victims-a-12048

Phishing and other hacking incidents have led to several recently reported large health data breaches, including one that UConn Health reports affected 326,000 individuals.

In describing a phishing attack, UConn Health says that on Dec. 24, 2018, it determined that an unauthorized third party illegally accessed a limited number of employee email accounts containing patient information, including some individuals' names, dates of birth, addresses and limited medical information, such as billing and appointment information. The accounts also contained the Social Security numbers of some individuals.

Click link above to read more

****

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:

Information Security Awareness Team - Information Security Branch

Office of the Chief Information Officer,

Ministry of Citizens' Services

4000 Seymour Place, Victoria, BC   V8X 4S8

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.

Information Security Branch
www.gov.bc.ca/informationsecurity

British Columbia

OCIO
Office of the Chief Information Officer