BRITISH COLUMBIA OCIO Office of the Chief Information Officer

Security News Digest

June 5th, 2018

June is IoT (Internet of Things) Month

Take our monthly quiz and test your knowledge

This week's stories:

- Torontonians should take control of their data 🇨🇦
- Privacy Commissioner issues new guidance to help address consent challenges in the digital age 🇨🇦
- How do data companies get our data?
- Large amount of desktop software in Canada is unlicenced and a major threat: Industry study 🇨🇦
- Sooke School District warns parents of privacy breach 🇨🇦
- Only 40 per cent of Canadian firms surveyed have data breach response procedures 🇨🇦
- With possible summit approaching, North Korean espionage hacks continue
- Ticketfly hacked: What to know about the online ticketing service's data breach
- Continental Bans WhatsApp and Snapchat From Work Phones
- In Australia, Email Compromise Scams Hit Real Estate
- Regulator: Don't Neglect Physical Security of 'Workstations'
- Another Fitness App Exposes Users' Data 🇨🇦

Torontonians should take control of their data 🇨🇦

https://nowtoronto.com/news/owns-data-toronto-smart-city/?_lrsc=48125879-74e3-47b0-94f1-be7d9ed9d5ff

A smart city is knocking at Toronto's door. Sidewalk Toronto, a joint venture between Sidewalk Labs, which is owned by Google parent company Alphabet Inc., and Waterfront Toronto, is proposing a high-tech neighborhood called Quayside for the city's eastern waterfront. A Master Innovation and Development Plan is in the works and set to be submitted at the end of 2018 for government approval.

The 12-acre smart city, which will be located between East Bayfront and the Port Lands, promises to tackle the social and policy challenges affecting Toronto: affordable housing, traffic congestion and the impacts of climate change. Imagine self-driving vehicles shuttling you around a 24/7 neighborhood featuring low-cost, modular buildings that easily switch uses based on market demand. Picture buildings heated or cooled by a thermal grid that doesn't rely on fossil fuels, or garbage collection by industrial robots. Underpinning all of this is a network of sensors and other connected technology that will monitor and track environmental and human behavioral data.

Click link above to read more

Privacy Commissioner issues new guidance to help address consent challenges in the digital age 🇨🇦

https://www.priv.gc.ca/en/opc-news/news-and-announcements/2018/nr-c_180524/

The Office of the Privacy Commissioner of Canada has published two important new guidance documents – on obtaining meaningful consent and on inappropriate data practices – to help organizations ensure they comply with their privacy obligations in the digital age.

The guidance will also help Canadians to understand their privacy rights under the law – and what they can expect from businesses that handle their personal information.

The two guidance documents are:

- Guidelines for obtaining meaningful consent
- Guidance on inappropriate data practices: Interpretation and application of subsection 5(3)

Click link above to read more

How do data companies get our data?

https://privacyinternational.org/feature/2048/how-do-data-companies-get-our-data

Open a Russian Matryoshka doll and you will find a smaller doll inside. Ask a large data company such as Acxiom and Oracle where they get their data from, and the answer will be from smaller data companies.

While it appears that the most common way for companies to obtain their data is to buy lists from other companies, the original question still stands: where does the data originally come from?

This article lists 9 primary ways

1. Electoral register, open registry, census:
2. Cookies and web beacons:
3. E-Mail Tracking
4. Apps and third party trackers
5. When your favorite shops give away your data
6. Platform registration: registering for more than you intend
7. Personality tests, quizzes, surveys and prizes: the data baits
8. Financial companies
9. Offline data and cross-device identification

Click link above to read more

Large amount of desktop software in Canada is unlicensed and a major threat: Industry study

https://www.itworldcanada.com/article/large-amount-of-desktop-software-in-canada-is-unlicenced-and-a-major-threat-industry-study/405941

The amount of unlicensed and unsupported software in the desktop computers of Canadians continues to slowly drop but still poses a great risk to users, says an industry survey released Tuesday.

The survey by BSA The Software Alliance –which includes giants like Adobe, Microsoft, IBM, Oracle and Symantec — 22 per cent of software installed on PCs in this country in 2017, worth an estimated $819 million, was not licensed. That continues a steady drop from the first global survey in 2011, when 27 per cent of Canadian computers were estimated to have unlicensed software.

By comparison, 15 per cent of PCs in the U.S. had unlicensed software last year. Globally the number was 37 per cent, which .the report called “alarming.”

The software industry loses a lot of money from unlicensed applications, but the hammer it uses is that this unsupported software is a security risk by allowing malware to exploit unpatched vulnerabilities. So the report urges CIOs to thoroughly inventory the software on their machines “so they can reduce the risk of harmful cyber attacks and boost the bottom line.”

Click link above to read more

Sooke School District warns parents of privacy breach

https://www.bclocalnews.com/news/sooke-school-district-warns-parents-of-privacy-breach/

“It has been discovered that the email account of a staff member was compromised by someone outside of the district and used to email out a spam informational link to other staff. Approximately 15 other staff members clicked on the link, thereby exposing their email accounts and email contents to the hacker(s),” said school superintendent Jim Cambridge.

Cambridge said the technology department deactivated all emails addresses that were affected, but the contents of the emails could have been compromised, meaning some emails from students in the district could be visible to someone outside the school district.

The school district has also notified the Office of the Information and Privacy Commissioner of the privacy breach.

Click link above to read more

Only 40 per cent of Canadian firms surveyed have data breach response procedures 🇨🇦

https://www.itworldcanada.com/article/only-40-per-cent-of-canadian-firms-surveyed-have-data-breach-response-procedures/405833

The survey of 1,014 Canadian senior decision-makers with responsibility and knowledge of their company’s privacy and security practices was conducted last fall. Asked to rate their level of concern about a possible data breach, nearly one-quarter (23 per cent) of respondents said they are extremely concerned, whereas 36 per cent said they were not concerned at all. Overall, nearly half (48 per cent) were moderately concerned (scores of three or higher on the seven-point scale) and half (50 per cent) expressed low or no concern at all.

Click link above to read more

With possible summit approaching, North Korean espionage hacks continue

https://arstechnica.com/information-technology/2018/06/with-possible-summit-approaching-north-korean-espionage-hacks-continue/

As North Korea’s government prepares for a possible summit with US President Donald Trump later this month, hackers working on behalf of the isolated country have continued a volley of network intrusions that target media, aerospace, financial, and critical-infrastructure companies in the US, South Korea, and other nations, researchers in private industry and the federal government said this week.

On Tuesday, the US Department of Homeland Security and the FBI identified two pieces of malware North Korea is actively using against multiple organizations throughout the world, including in the US.

The first piece of malware is a fully functional remote-access trojan called Joanap. It typically infects computers as a payload that is delivered by another piece of Hidden Cobra malware, and targets unknowingly download it when they visit a compromised website.

The second piece of malware is a worm that spreads across SMB networks by guessing weak passwords. Known as Brambul, the self-replicating malware is usually delivered through a dropper.

effects of infection include:

- temporary or permanent loss of sensitive or proprietary information,
- disruption to regular operations,
- financial losses incurred to restore systems and files, and
- potential harm to an organization’s reputation.

Click link above to read more

Ticketfly hacked: What to know about the online ticketing service’s data breach

https://globalnews.ca/news/4250616/ticketfly-breach-hacked-online-conert/

On May 31, Ticketfly was defaced by an attacker and was subsequently taken offline, Vice’s Motherboard reported. The attacker allegedly requested a ransom to share details of the vulnerability with Ticketfly but did not receive a reply and subsequently posted the breached data online to a publicly accessible location, Motherboard reported.

Customers’ names, addresses, email addresses and phone numbers had been exposed. Passwords and credit-card numbers were apparently not affected.

According to Motherboard, the hacker has several spreadsheet files that appear to contain personal information about thousands of Ticketfly customers and employees of venues that use the service.

Click link above to read more

Continental Bans WhatsApp and Snapchat From Work Phones

https://www.bleepingcomputer.com/news/technology/continental-bans-whatsapp-and-snapchat-from-work-phones/

Car parts manufacturer Continental, one of Germany's biggest companies, has banned the use of the WhatsApp and Snapchat apps on employees' work phones.

The company cited the two apps' intrusive permissions as the reason for the ban, and especially their ability to access a worker's contacts list.

"In the company’s opinion, these services have deficiencies when it comes to data protection, as they access a users’ personal and potentially confidential data such as contacts, and thus the information of third parties who are not involved. In the case of these apps, access to the contact list cannot be restricted," a spokesperson said in a statement announcing the ban, published yesterday.

Click link above to read more

In Australia, Email Compromise Scams Hit Real Estate

https://www.databreachtoday.com/in-australia-email-compromise-scams-hit-real-estate-a-11049

Late last year in Australia, cybercriminals began targeting a fertile yet relatively poorly protected business sector for so-called business email compromise scams: the real estate industry.

The bounties are home deposits, bonds and settlements, says Alex Tilley, senior security researcher with Dell's SecureWorks Counter Threat Unit. Tilley gave a rundown of the complex criminal networks behind the scams at the AusCERT security conference in Gold Coast on Thursday.

"That's literally how you steal someone's life savings," Tilley says. "It's brutal."

According to a report released in May by the Australian Competition and Consumer Commission, or ACCC, losses from email compromise scams reached $22.1 million (US$16.5) million in 2017. The FBI estimates that since it first started tracking email compromises five years ago, worldwide losses are in the billions.

The scams, often initiated in Nigeria, use a network of money handlers and local bogus bank accounts to siphon and launder money in ways that can be difficult to track and recover.

Click link above to read more

Regulator: Don't Neglect Physical Security of 'Workstations'

https://www.databreachtoday.com/regulator-dont-neglect-physical-security-workstations-a-11047

A May 30 cybersecurity alert issued by the Department of Health and Human Services' Office for Civil Rights urges HIPAA covered entities and BAs to pay closer attention to providing good physical security for "workstations," which include a wide variety of devices.

As of May 31, OCR's HIPAA Breach Report Tool website - commonly known as the "wall of shame" - lists 632 major health data breaches involving theft of electronic computing devices that have impacted more than 20.3 million individuals since 2009.

That represents about 27 percent of the 2,322 breaches on the tally, and about 8 percent of the nearly 253 million individuals impacted by those incidents.

"Physical security covers a lot of topics. Obviously, things like locking doors is always important in general," he says. "A lot of the other issues depend on the business activities. As workplaces evolve, some of these issues become even more important. Shared office spaces require special protections for sensitive information. Working from home creates a variety of new risks. The mobility of information - on mobile devices, laptops, thumb drives and the like - requires significant attention."

Click link above to read more

Another Fitness App Exposes Users' Data

https://www.databreachtoday.com/another-fitness-app-exposes-users-data-a-11055

For at least the third time in recent months, a mobile fitness app maker apparently has exposed consumers' sensitive personal information.

In the latest incident, independent researcher Oliver Hough discovered that Ontario, Canada-based fitness company PumpUp was exposing sensitive consumer health data and private messages between users via an unsecured backend server hosted on Amazon's cloud infrastructure.

The researcher reportedly contacted news site ZDNet to investigate the situation, according to a May 31 story posted on the media company's website.

Hough confirmed to Information Security Media Group that on May 23, he discovered that PumpUp consumer data, including user email addresses, location and workout records, as well as self-reported health information - such as height and weight - and some unencrypted credit card information, including card numbers, was accessible on the unsecured Amazon server.

"The MQTT server did not have any authentication enabled; anyone with the knowledge to connect to an MQTT could connect and view all messages in transit," Hough says.

ZDNet reports that it tried for over a week to inform PumpUp of the breach, but the vendor did not respond. PumpUp also did not immediately respond to an ISMG request for comment on the breach.

Click link above to read more

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:
Information Security Awareness Team - Information Security Branch
Office of the Chief Information Officer,

Ministry of Citizens’ Services
4000 Seymour Place, Victoria, BC   V8X 4S8
http://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.

****