BRITISH COLUMBIA OCIO Office of the Chief Information Officer

Security News Digest
March 13, 2018

March is Fraud Awareness Month
Take our quiz and test your knowledge

This week's stories:

Most of blockchain's benefits don't come from blockchain, Bank of Canada staffer says 🇨🇦

'Black Tech' facial recognition glasses worn by Chinese police raise privacy concerns 🇨🇦

Uber to inform Canadians whose data may have been compromised in 2016 breach 🇨🇦

Top White House Aides Tricked By Email Prankster Posing As Other Top Aides

Microsoft Admits It Incorrectly Upgraded Some Windows 10 Users to v1709

Musk: 'AI is far more dangerous than nukes,' needs regulation

Checked Your Credit Since the Equifax Hack?

B.C. Archives hold rulings that shaped our history 🇨🇦

Most of blockchain's benefits don't come from blockchain, Bank of Canada staffer says 🇨🇦

http://www.cbc.ca/news/technology/blockchain-benefits-1.4572950

A new research paper by a Bank of Canada staffer says most of the proposed benefits of the technology known as blockchain don't really come from features unique to blockchain.

In recent years, blockchain has been attracting a growing amount of attention as an efficient, highly secure, distributed-ledger technology with numerous applications — from easing cross-border transfers of funds, to creating a foundation for digital currencies like Bitcoin. But a staff analytical paper from the Bank of Canada is peeling back the layers of blockchain's proposed advantages and suggests most of its assets actually come from more-conventional technologies such as encryption and smart contracts.

Author Hanna Halaburda also suggests the enthusiasm and uncertainty surrounding blockchain has an impact on the economy, for example, through optimistic valuations of blockchain-referencing startups. The central bank says positions presented in its staff papers solely represent the views of the author and may differ from those of the bank.

Governments in Canada and businesses, including big banks, have dedicated growing pools of resources to studying the possible applications of blockchain — and even the Bank of Canada itself has been collaborating as part of a research initiative that has tested whether the technology could help underpin an inter-bank wholesale payment system.

'Black Tech' facial recognition glasses worn by Chinese police raise privacy concerns 🇨🇦

https://globalnews.ca/news/4079525/black-tech-facial-recognition-glasses-worn-by-chinese-police-raise-privacy-concerns/

At a highway check point on the outskirts of Beijing, local police are this week testing out a new security tool: smart glasses that can pick up facial features and car registration plates, and match them in real-time with a database of suspects. The AI-powered glasses, made by LLVision, scan the faces of vehicle occupants and the plates and light-up warnings for the wearers if the glasses match the information with a centralized "blacklist." The test, which coincides with the annual meeting of China's parliament in central Beijing, underscores a major push by China's leaders to leverage technology to boost security in the country.

That drive has led to growing concerns that China is developing a sophisticated surveillance state that will lead to intensifying crackdowns on dissent. **"(China's) leadership once felt a degree of trepidation over the advancement of the internet and communication technologies," said David Bandurski, co-director of the China Media Project, a media studies research project at the University of Hong Kong. "It now sees them as absolutely indispensable tools of social and political control."** Wu Fei, chief executive of LLVision, said people should not be worried about privacy concerns because China's authorities were using the equipment for "noble causes," such as catching watched suspects and fugitives. "We trust the government," he told Reuters at the company's headquarters in Beijing. Reuters was able to verify that the glasses were being used in tests by the police to help identify suspect individuals and vehicles in the Beijing area in recent days.

China, under President Xi Jinping, is making a major push to use artificial intelligence, facial recognition and big data technology to track and control behaviour that goes against the interests of the ruling Communist Party online and in the wider world. Xi is expected to cement his power base this weekend as a reform to remove term limits is pushed through. That would, in effect, allow him to stay in his post indefinitely.

Delegates and visitors entering the Great Hall of the People, the venue for the parliament, the National People's Congress, have to go through facial scanners. The same happened to those attending the related advisory body, the Chinese People's Political Consultative Conference. "This year, security at the two sessions has some freshly-baked 'black tech' coming online," wrote the state-run Science and Technology Daily newspaper, using a comic-book term in China for futuristic surveillance gadgets. The paper said cameras at the event had been upgraded to capture, analyze and compare suspicious faces in around two seconds, powered by a system called "Skynet" — which has a national database of blacklisted individuals. "The plot of sci-fi film 'Minority Report' is now basically becoming a part of daily life," the newspaper added, referring to the Tom Cruise movie set in a futuristic society where crimes are solved and punished before they even happen.
[The story continues online]

Uber to inform Canadians whose data may have been compromised in 2016 breach 🇨🇦

https://www.theglobeandmail.com/report-on-business/uber-to-inform-canadians-whose-data-may-have-been-compromised-in-2016-breach/article38264637/

Uber will inform all Canadians whose personal data may have been compromised in a 2016 breach after Alberta's privacy commissioner ruled it must notify impacted drivers and riders in the province. **In a decision dated Feb. 28, the commissioner ruled that there is a real risk of significant harm to the affected individuals as a result of an Oct. 2016 breach that saw the theft of information – including names, email addresses and mobile numbers – from some 57 million accounts globally. The personal information of drivers, such as their driver's license numbers, could be used for identity theft or fraud, wrote Jill Clayton, information and privacy commissioner. "These are significant harms," she wrote.** The organization must notify affected drivers and riders whose information was collected in Alberta, she ruled, and notify the commissioner in writing that it has done so within 10 days of the decision. It has already informed all drivers globally, including the 23 that appeared to have Canadian connections, according to the ruling. But affected riders had not yet been notified.

While Uber disagrees with the ruling, it will comply, said spokesman Jean-Christophe de le Rue. **Uber will email affected riders and drivers in not just Alberta, but across the country over the next few days. It previously disclosed that 815,000 Canadian riders and drivers may have been affected. The stolen information included names, email addresses and mobile numbers. An internal investigation failed to identify that any location history, credit card numbers, bank account numbers or birth dates were downloaded, the company said.**

When Uber discovered the breach, De Le Rue said, it conducted a thorough investigation and notified Canadian privacy commissioners, fully co-operating with their investigations. **The company has seen no evidence of fraud or misuse tied to the incident and continues to monitor the affected accounts, he said**. Uber plans to ask for a judicial review of the ruling because, in its view, the breach did not create a real risk of significant harm. The privacy commissioner's office did not immediately respond to a request for comment.

In 2010, the province of Alberta became the first Canadian jurisdiction to require private-sector organizations, like Uber, to notify consumers of such breaches when "a real risk of significant harm" exists.

Top White House Aides Tricked By Email Prankster Posing As Other Top Aides

http://www.huffingtonpost.ca/entry/white-house-aides-tricked-email-prankster_us_59800071e4b00bb8ff391b7e

Senior officials at the White House, including ousted communications director Anthony Scaramucci, were duped by an email prankster after being sent a series of messages that appeared to come from other top aides in the Trump administration, CNN first reported Monday night. The anonymous prankster, who lives in Britain and tweets using the handle @SINON_REBORN, reportedly **posed as White House Chief of Staff Reince Priebus** in one of the email chains to Scaramucci shortly after Priebus announced his resignation last week. “At no stage have you acted in a way that’s even remotely classy, yet you believe that’s the standard by which everyone should behave towards you?” a mock Priebus emailed. “General Kelly will do a fine job. I’ll even admit he will do a better job than me. But the way in which that transition has come about has been diabolical. And hurtful. I don’t expect a reply. ”Scaramucci replied: “You know what you did. We all do. Even today. But rest assured we were prepared. A Man would apologize.” He later went on to tell the prankster (thinking it was still Priebus) to “Read Shakespeare. Particularly Othello.” Scaramucci was also sucked into an exchange with a fake Jon Huntsman, the former Utah governor who was chosen last month to be the U.S. ambassador to Russia. The real Huntsman was also tricked by a fake Eric Trump, and the real Eric Trump was emailed by a fake Donald Trump Jr., although the younger son of the president later said he forwarded the messages to authorities.

The prankster was able to successfully pose as President Donald Trump’s son-in-law, Jared Kushner, in an email sent to homeland security adviser Tom Bossert. The message from a fake Kushner included an invitation to “a bit of a soirée” alongside promises of “food of at least comparible [sic] quality to that which we ate in Iraq.” “Should be a great evening,” the note ends. “Thanks, Jared. With a promise like that, I can’t refuse,” Bossert wrote back, according to the email obtained by CNN. He also included his personal email address, which CNN redacted. CNN obtained the emails from the prankster and confirmed their authenticity with the White House. Press Secretary Sarah Huckabee Sanders responded that the White House was investigating the cyber-spoofing.
[Follow the link above for more on the full text message exchanges]

Microsoft Admits It Incorrectly Upgraded Some Windows 10 Users to v1709

https://www.bleepingcomputer.com/news/microsoft/microsoft-admits-it-incorrectly-upgraded-some-windows-10-users-to-v1709/

Microsoft admitted last week that it incorrectly updated some Windows 10 users to the latest version of the Windows 10 operating system —version 1709— despite users having specifically paused update operations in their OS settings. The admission came in a knowledge base article updated last week. Not all users of older Windows versions were forcibly updated, but only those of Windows 10 v1703 (Creators Update). This is the version where Microsoft added special controls to the Windows Update setting section that allow users to pause OS updates in case they have driver or other hardware issues with the latest OS version. But according to reports, a Microsoft snafu ignored these settings and forcibly updated some users to Windows 10 v1709 (Fall Creators Update). "This happened to me last night, "said a user sharing his experience on the AskWoody tech support website. "About 30 minutes later, a box pops on my screen and informs me that there are security updates available and that it needs to update to latest version of Windows 10 to be able to install them and then starts the update. "I have Dell XPS8900 with version 1703 and when the update finished, I had version 1709, but no sound, no color (everything black and white), reinstall software notifications and errors saying certain shortcut keys are not available," the user added. "I had pause[d updates] on for 35 days enabled and 365 days set on feature updates. After restoring an image and disabling WU service, the forced update began to update all over again !!!"

Microsoft admitted its blunder. The OS maker says it shipped last week a Windows feature update — KB4023814 — that would show an update notification for users of older Windows versions. The update was meant primarily for Windows 10 v1507 and v1511, two Windows 10 versions released in 2015 that are now officially end-of-life. Microsoft was just trying to notify users that they should update to the latest Windows 10 version to receive security updates. The update was also displayed for Windows 10 v1607 and v1703, even if those OS versions are still supported, but as an optional update alert.

But it appears that KB4023814 misfired for v1703 users with custom update settings and forcibly installed the latest version, v1709. "Microsoft is aware that this notification was incorrectly delivered to some Windows 10 Version 1703 devices that had a user-defined feature update deferral period configured. Microsoft mitigated this issue on March 8, 2018," the company said.

Users who were affected by this issue and who upgraded to Windows 10 Version 1709 can revert to an earlier version within 10 days of the upgrade. To do this, open **Settings** > **Update & Security** > **Recovery**, and then select **Get started** under **Go back to the previous version of windows 10**.

This incident marks the third time in the past year when Microsoft has mistakenly updated v1703 users to v1709. It happened before in November 2017 and January 2018 when Patch Tuesday security updates accidentally upgraded some users.

Musk: 'AI is far more dangerous than nukes,' needs regulation

https://www.techrepublic.com/article/musk-ai-is-far-more-dangerous-than-nukes-needs-regulation/?ftag=TREe01923b&bhid=19662319145962710268575546540229

Just how dangerous is artificial intelligence (AI)? Well, according to Tesla CEO Elon Musk, "AI is far more dangerous than nukes." That statement was made at the 2018 SXSW conference in Austin. Speaking to panel moderator Jonathan Nolan, co-creator of HBO's Westworld, Musk said AI "scares the hell out of me," and even though he typically isn't big on regulation, he believes that AI is something where stronger regulation is called for.

Musk has been known to sound the alarm on AI in the past, but recent growth of technologies like Google's AlphaGo have perpetuated those fears in him, he said speaking to Nolan. As noted by Asha McLean, of our sister site ZDNet, the AI competitor went from losing games of Go to relatively average players to absolutely crushing the game's world champion in a few short months. That rate of growth is what scares Musk, he said.

The big issue in the space is hubris, Musk said. In the talk, Musk said that some experts in the field of AI "think they know more than they do and they think they're smarter than they are." That's a problem, because these experts don't believe a machine could ever be smarter than they are. In addition to the rate of improvement seen in AlphaGo, the rate of improvement in self-driving cars is also something that needs to be addressed. "The rate of improvement is really dramatic, but we have to figure out some way to ensure that the advent of digital super intelligence is one which is symbiotic with humanity," Musk said. "I think that's the single biggest existential crisis that we face, and the most pressing one."

According to Musk, AI represents a serious danger to the public, and needs regulatory oversight from a public body. In touching on the nuclear weapon analogy, he said: "The danger of AI is much greater than the danger of nuclear warheads, by a lot and nobody would suggest that we allow anyone to just build nuclear warheads if they want—that would be insane." The potential danger of AI is one of the most stressful things in Musk's life, he said, next to the production of the Tesla Model 3. One option to keep humans safe from the machines would be to create a physical input on the human body, so AI would be an extension one's self, Musk said.

In keeping with the dystopian theme, Musk also said that he believed we might be heading toward a Dark Age brought about by World War III. To protect humanity, he said we need to build self-sustaining bases on the moon and on Mars to survive the war.

Checked Your Credit Since the Equifax Hack?

https://krebsonsecurity.com/2018/03/checked-your-credit-since-the-equifax-hack/#more-42689

[Blog post by Brian Krebs]

A recent consumer survey suggests that half of all Americans still haven't checked their credit report since the Equifax breach last year exposed the Social Security numbers, dates of birth, addresses and other personal information on nearly 150 million people. If you're in that fifty percent, please make an effort to remedy that soon. Credit reports from the three major bureaus — **Equifax**, **Experian** and **TransUnion** — can be obtained online for free at annualcreditreport.com — the only Website mandated by Congress to serve each American a free credit report every year.

Annualcreditreport.com is run by a Florida-based company, but its data is supplied by the major credit bureaus, which struggled mightily to meet consumer demand for free credit reports in the immediate aftermath of the Equifax breach. Personally, I was unable to order a credit report for either me or my wife even two weeks after the Equifax breach went public: The site just kept returning errors and telling us to request the reports in writing via the U.S. Mail. Based on thousands of comments left here in the days following the Equifax breach disclosure, I suspect many readers experienced the same but forgot to come back and try again. If this describes you, please take a moment this week to order your report(s) (and perhaps your spouse's) and see if anything looks amiss. If you spot an error or something suspicious, contact the bureau that produced the report to correct the record immediately.

Of course, keeping on top of your credit report requires discipline, and if you're not taking advantage of all three free reports each year you need to get a plan. My strategy is to put a reminder on our calendar to order a new report every four months or so, each time from a different credit bureau.

Whenever stories about credit reports come up, so do the questions from readers about the efficacy and value of credit monitoring services. KrebsOnSecurity has not been particularly kind to the credit monitoring industry; many stories here have highlighted the reality that they are ineffective at preventing identity theft or existing account fraud, and that the most you can hope for from them is that they alert you when an ID thief tries to get new lines of credit in your name. But there is one area where I think credit monitoring services can be useful: Helping you sort things out with the credit bureaus in the event that there are discrepancies or fraudulent entries on your credit report. I've personally worked with three different credit monitoring services, two of which were quite helpful in resolving fraudulent accounts opened in our names.

At $10-$15 a month, are credit monitoring services worth the cost? Probably not on an annual basis, but perhaps during periods when you actively need help. However, if you're not already signed up for one of these monitoring services, don't be too quick to whip out that credit card: There's a good chance you have at least a year's worth available to you at no cost. If you're willing to spend the time, check out a few of the state Websites which publish lists of companies that have had a recent data breach. In most cases, those publications come with a sample consumer alert letter providing information about how to sign up for free credit monitoring. California publishes probably the most comprehensive such lists at this link. Washington state published their list here; and here's Maryland's list. There are more.

It's important for everyone to remember that as bad as the Equifax breach was (and it was a dumpster fire all around), most of the consumer data exposed in the breach has been for sale in the cybercrime underground for many years on a majority of Americans. If anything, the Equifax breach may have simply refreshed some of those criminal data stores.
[Follow the link above for more on this blog post]

And Now this:

B.C. Archives hold rulings that shaped our history

http://www.timescolonist.com/life/islander/b-c-archives-hold-rulings-that-shaped-our-history-1.23197626

Based on the British legal system, but adapted to local conditions, our court system has developed over the more than 160 years it has been in existence and has become increasingly complex. Our holdings reflect that evolution and complexity. The courts for which we have records include the Colony of Vancouver Island's Inferior Court of Civil Justice and Supreme Court of Civil Justice, the Supreme Court of B.C., the Full Court and the Court of Appeal, Assize courts, county courts, mining courts, magistrate's courts, juvenile courts and family courts. The records include the proceedings and decisions of the courts in civil and criminal actions, documents filed with the court, minute books, cause books, plaint and procedure books, bench books, and registers, indexes, and other tools to manage the records.

In addition to their legal and evidentiary value, these records are a rich source of historical information about the administration of justice since colonial times, but also about other aspects of B.C.'s history in as much as the courts deal with a wide range of issues, including social, political, economic, Indigenous, environmental, cultural, business, labour and human rights.

Requests for and about records for specific court actions and cases come from genealogists for family history and biography; historians and scholars researching a topic; individuals for evidentiary purposes; file and search companies; lawyers, usually for litigation purposes; government agencies; and others. Probate files and divorce orders are probably the most commonly requested and sought court records at the B.C. Archives. An example of the former is the probated will of **Emily Carr**, which appointed her executors and gave instructions for the disposition of her estate, including her art works and her papers. An example of the latter is **Francis Rattenbury's divorce**. His wife took him to court and divorced him, not in Victoria where they lived, but in Vancouver, probably to avoid publicity at the time. The page from the cause book shows the proceedings and is the tool that is used to locate the order shown here.

As well, many researchers make use of court records that touch upon a particular topic or field of study; for example, the Landscapes of Injustice project, of which the Royal B.C. Museum is a partner institution. Two examples pertinent to Landscapes of Injustice research are Tomey Homma, arguing for his right to vote in the early 1900s, and the trial of four men for the murder of a Japanese-Canadian man during a convenience-store robbery shortly after the bombing of Pearl Harbor. Both cases reflect not only the sentiments at the time, but also the legal arguments and how the legal system dealt with the cases. In the first, the judgment of the B.C. Supreme Court sitting as the Full Court was in Homma's favour, but was subsequently overturned by the Privy Council in England. In the second, the verdict of murder was overturned by the Supreme Court of Canada and a new trial ordered, which returned a verdict of manslaughter.

Litigation involving Indigenous issues and/or parties date back to colonial times. From colonial cases dealing with whether evidence by Indigenous witnesses was admissible, to more recent aboriginal rights and title cases (e.g. R.V. White and Bob), B.C.'s court records are a rich source for both legal and research purposes. However, this body of records presents many challenges in terms of access and use, not the least of which are its extent and complexity and the case-name search limitations. As the official legal records of a judicial system, court records are created to suit its needs, purposes and requirements. The language used, often incorporating terms and expressions in Latin, their format and organization (by individual court registries) as well as how they are managed, recorded and searched (i.e. by case name) do not lend themselves to ease of research access. For example, an ordinary person looking for a divorce order or a probate file is not interested in how, where and by what court the records were created and managed. For the archivist who must make sense of them and provide the descriptive tools to assist researchers and others in locating specific records, or records by subject or type, it is necessary to be familiar with the history and structure of the courts and the system that created them, as well as their jurisdictional basis and extent. In the archival world, this is called an administrative history and is a critical component in making sense of the records and developing appropriate search tools, as well as determining legislative and other access restrictions. As more and more court records are transferred to the B.C. Archives and as requests for and research into court records increase, it is needed more than ever. It also helps in locating requested records that are not at the B.C. Archives.

The history of the courts and the administration of justice in B.C. is also a fascinating history in its own right, starting with the unauthorized creation of B.C.'s first Supreme Court by James Douglas and his appointment of his brother-in-law — who had no legal training — as first chief justice. One of the cases over which he presided was the case of Charles Mitchell, a young African-American who fled his owner in Washington Territory and claimed his freedom once he reached British soil, the Colony of Vancouver Island. When the captain of the ship where he stowed away insisted that he be returned, Chief Justice Cameron ruled in Mitchell's favour.

Click Unsubscribe to stop receiving the Digest.

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

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.

****