





February 25th, 2020

Try our February Quiz – [Love Information Security](#)

This week's stories:

- [UN disarmament chief warns of 'dark side' of AI, as Liberals tout benefits](#) 
- [Regina police arrest alleged Peeping Tom after camera found in Tim Horton's restroom](#) 
- [Ransomware attack forces 2-day shutdown of natural gas pipeline](#)
- [One of Albany's largest accounting firms was hit with a ransomware attack — what happened next](#)
- [MGM Hotel breach highlights need for sophisticated cloud security](#)
- [Summer Olympics is ripe for cyberattacks](#)
- [The good, the bad, and the scary from Experian's data breach report](#)
- [Airbnb Is Recommending Surveillance Devices To Make Sure Guests Behave](#)
- [A 'stalkerware' app leaked phone data from thousands of victims](#)
- [Met police chief: facial recognition technology critics are ill-informed](#)
- [New DNA test that reveals a child's true age has promise, but ethical pitfalls](#)

UN disarmament chief warns of 'dark side' of AI, as Liberals tout benefits

<https://www.timescolonist.com/un-disarmament-chief-warns-of-dark-side-of-ai-as-liberals-tout-benefits-1.24082995>

OTTAWA — The United Nations' top disarmament official says governments need to pay more attention to the "dark side" of artificial intelligence, including the implications of so-called killer robots that could take military decisions out of human hands.

The benefits of AI will be groundbreaking but governments need to take stronger measures to prevent bad military applications, including potentially catastrophic hacks of nuclear arsenals, said Izumi Nakamitsu, the UN's undersecretary-general for disarmament affairs.

[Click link above to read more](#)

Regina police arrest alleged Peeping Tom after camera found in Tim Horton's restroom



<https://www.cbc.ca/news/canada/saskatchewan/peeping-tom-at-tims-1.5474073>

A 42-year-old man is facing two counts of voyeurism after Regina police discovered and seized a camera from a Tim Horton's bathroom on Jan. 20.

Police say they were called to the 5800 block of Rochedale Boulevard that day after an electronic device had been discovered in the women's washroom. An employee of the Tim Horton's on that block confirmed that was where the incidents happened.

[*Click link above to read more*](#)

Ransomware attack forces 2-day shutdown of natural gas pipeline

<https://nakedsecurity.sophos.com/2020/02/20/ransomware-attack-forces-2-day-shutdown-of-natural-gas-pipeline/>

The US Department of Homeland Security (DHS) on Tuesday [said](#) that an infection by an unidentified ransomware strain forced the shutdown of a natural-gas pipeline for two days.

Fortunately, nothing blew up. The attacker never got control of the facility's operations, the human-machine interfaces (HMI) that read and control the facility's operations were successfully yanked offline, and a geographically separate central control was able to keep an eye on operations, though it wasn't instrumental in controlling them.

Where this all went down is a mystery

[*Click link above to read more*](#)

One of Albany's largest accounting firms was hit with a ransomware attack — what happened next

<https://www.bizjournals.com/albany/news/2020/02/20/bst-co-ransomware-attack-community-care.html>

BST & Co. was hit with a ransomware attack in December that exposed the data of some of its accounting and tax service clients, including the medical group Community Care Physicians.

The company revealed the attack in an advisory sent to media this week, along with letters sent to Community Care customers affected by the attack. Community Care is the region's third-largest physician group.

Here's how the attack played out: On Dec. 7, BST learned that part of its network was infected with a virus that prohibited access to its files. BST restored its systems and hired a forensic investigation firm to determine the nature and scope of the incident. It found out the virus was active from Dec. 4 to Dec. 7.

[*Click link above to read more*](#)

MGM Hotel breach highlights need for sophisticated cloud security

<https://www.techrepublic.com/article/mgm-hotel-breach-highlights-need-for-sophisticated-cloud-security/?ftag=TRa988f1c&bhid=42420269>

On Wednesday, cybercriminals posted the information of more than 10 million MGM Hotel customers on a hacker forum, exposing their personal data to thousands of criminals nearly a year after the initial breach.

In a statement to ZDNet, an MGM spokesperson said: "Last summer, we discovered unauthorized access to a cloud server that contained a limited amount of information for certain previous guests of MGM Resorts. We are confident that no financial, payment card or password data was involved in this matter."

[*Click link above to read more*](#)

Summer Olympics is ripe for cyberattacks

<https://www.techrepublic.com/article/summer-olympics-is-ripe-for-cyberattacks/?ftag=TRa988f1c&bhid=42420269>

Millions of people are eagerly anticipating this summer's Olympic Games in Tokyo—and so are cyberattackers. "Events like the Olympics serve as an amplifier for cybercrime," said Emily Wilson, vice president of research at Terbium Labs. Cyberattackers will be exploiting the "increased distraction around the Olympics, allowing them to be more successful."

When people are traveling and out of their element, they may be more suspicious of the emails they receive, but when it comes to an event like the Olympic games their defenses may be down.

So if they get an email saying their hotel reservation has been canceled or a last-minute notification that a ticket to an event requires another level of validation, for example, "there is a higher sense of urgency," Wilson explained.

[Click link above to read more](#)

The good, the bad, and the scary from Experian's data breach report

<https://www.techrepublic.com/article/the-good-the-bad-and-the-scary-from-experians-data-breach-report/?ftag=TR Ea988f1c&bhid=42420269>

Spear phishing and global attacks went up in 2019 but so did investment security technology spending. Security teams are also more confident about their data breach response plans, even though the number is only 57%. Experian and the Ponemon Institute shared the state of data breaches and defenses against these attacks in the seventh annual "Is Your Company Ready for a Big Data Breach?" report.

Experian has firsthand experience with a massive data breach. In 2015, Experian disclosed a data breach which led to the compromise of information -- including Social Security numbers -- belonging to 15 million consumers. The data belonged to T-Mobile customers; Experian processes credit checks for the wireless carrier.

[Click link above to read more](#)

Airbnb Is Recommending Surveillance Devices To Make Sure Guests Behave

<https://www.forbes.com/sites/zakdoffman/2020/02/23/airbnb-just-launched-these-intrusive-new-surveillance-bugs-to-ensure-you-all-behave/#100b63364719>

Airbnb, the world's leading short-term rental platform has put aside the stories of hosts secretly spying on guests to promote a range of guest surveillance devices. "We want to help you protect your space, maintain the privacy of your guests, and preserve your relationship with neighbors," the company says on its website. "This means helping you detect issues in real time." Creepy, necessary or just a sign of the times—you decide.

There have been issues with the misuse of Airbnb properties—stories hitting the headlines of parties out of control, properties trashed, even the use of rentals to record adult movies. Well, now there's a solution.

[Click link above to read more](#)

A 'stalkerware' app leaked phone data from thousands of victims

<https://techcrunch.com/2020/02/20/kidsguard-spyware-app-phones/>

spyware app designed to "monitor everything" on a victim's phone has been secretly installed on thousands of phones.

The app, KidsGuard, claims it can "access all the information" on a target device, including its real-time location, text messages, browser history, access to its photos, videos and app activities, and recordings of phone calls.

But a misconfigured server meant the app was also spilling out the secretly uploaded contents of victims' devices to the internet.

[Click link above to read more](#)

Met police chief: facial recognition technology critics are ill-informed

https://www.theguardian.com/technology/2020/feb/24/met-police-chief-cressida-dick-facial-recognition-technology-critics-ill-informed?CMP=fb_a-technology_b-gdnitech

The Metropolitan police commissioner, Cressida Dick, has attacked critics of facial recognition technology for using arguments she has claimed are highly inaccurate and ill-informed.

The Met began operational use of the technology earlier this month despite concerns raised about its accuracy and privacy implications by civil liberties groups, including Amnesty International UK, Liberty and Big Brother Watch (BBW).

[Click link above to read more](#)

New DNA test that reveals a child's true age has promise, but ethical pitfalls

<https://theconversation.com/new-dna-test-that-reveals-a-childs-true-age-has-promise-but-ethical-pitfalls-126676>

Epigenetic clocks are a new type of biological test currently capturing the attention of the scientific community, private companies and governmental agencies because of their potential to reveal an individual's "true" age.

Over the past two years, companies such as Chronomics and MyDNage have started to sell epigenetic age tests to the public online, and the life insurance company YouSurance has announced that it would be testing the epigenetic age of their policy holders to assign them to risk groups. Forensic scientists are also contemplating how epigenetic clocks could help determine the age of suspected criminals.

[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

<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



OCIO

Office of the
Chief Information Officer