BRITISH COLUMBIA OCIO Office of the Chief Information Officer

Security News Digest
August 01, 2017

August is here and it will be a hot one!
Check out a new fun game with the Dog Days of Summer quiz

Promote Information Security Day on the First Thursday of August [the 3rd].

http://informationsecurityday.com/

Protection of information assets and the technology resources that support the business enterprise is very critical to the functioning of any business organization. Information System assets are always at risk from potential threats such as malicious or criminal actions, employee error, system failure, natural disaster, and lack of proper security infrastructure. Such events and situations could result in the damage to or loss of information resources, corruption or loss of data integrity, interruption in business continuity, or compromise to confidentiality or privacy of end users of the information systems.

Information Security Day was started to spread the awareness of information security issues. Information Security, also known as Information Systems Security (INFOSEC) deals with the different aspects of information and its protection. Information Security Day aims at reducing the risk associated with the information systems by increasing the awareness of the user community.

INFOSec Day aims at increasing the awareness in the following areas: (1) Understanding the various information system components, (2) Security Management Principles, (3) Risk Assessment, Sensitivity and Criticality, (4) Disaster Recover and Emergency Procedures, (5) Logical Security, (6) Physical Security, and (7) Managerial Security Measures.

The annual event is held around the world on the first Thursday of August every year. If a local holiday coincides with the Information Security Day, you can always re-arrange the date for your convenience. Let's make a difference

NAFTA Talks: U.S. Proposal for Cross-Border Data Storage at Odds with B.C., N.S. Law 🇨🇦

http://www.cbc.ca/news/politics/nafta-data-storage-privacy-1.4220272

One of the American targets in the upcoming renegotiation of the North American Free Trade Agreement appears on a collision course with ***privacy laws*** *in British Columbia and Nova Scotia.* In negotiating objectives published last week, the Office of the United States Trade Representative said it wanted to "establish rules to ensure that NAFTA countries do not impose measures that restrict cross-border data flows and do not require the use or installation of local computing facilities." *But provincial legislation in two Canadian provinces does exactly that, with rules requiring personal information collected by governments, such as health records, to be stored on domestic servers to prevent it being accessed for reasons other than those for which it was collected.*

For example, under the U.S. Patriot Act brought in to fight terrorism in the days after Sept. 11, if a Canadian government had contracted a U.S. facility to store electronic records, American security or intelligence officers could access them. *"This is something that we have decided democratically that we want to do to protect our privacy rights," said Vincent Gogolek, the executive director of B.C.'s Freedom of Information and Privacy Association*. Following an outcry over the move by a previous Liberal government in B.C. to outsource the administration of government health-care information, "this is something that has acquired political consensus in B.C.," he said. "We want the feds to protect our privacy rights."

'Swapping rights for tariffs'. Canadian restrictions on data storage have been a burr under the USTR's saddle for years, even before the most recent push to modernize NAFTA for e-commerce. "The American position is that we would prefer to have our server farms in Arizona or California or wherever ... and you send your data down here," Gogolek said. The U.S. viewpoint is: "this gets in the way of us making money, and we resent it, so we want you to change it." "They haven't had any opportunity to go after it, and this is their opportunity," he said. But Canada "shouldn't be swapping rights off in exchange for lower tariffs on widgets. It should be pretty straightforward for the federal government to just stand up and say 'No, we're not doing it.'"

Previous negotiations among the three NAFTA partners, who were all part of the 12-country Trans-Pacific Partnership, proposed grandfathering existing privacy legislation. Would that happen this time? It's unclear. The federal government hasn't been afraid of invoking national security to ensure government email is stored in Canada, Gogolek said. If it's willing to do that, "why shouldn't we be protecting Canadians' information generally, that they have to provide to government?" *Both provinces adopted their laws over a decade ago, out of concern about foreign intelligence gathering without notice to individuals, which isn't consistent with Canadian privacy standards*. …

Protectionism or security? *The Information Technology Association of Canada* - which represents 330 technology companies, two-thirds of which are Canadian-owned small and medium-sized businesses - said in its recent submission to Canada's NAFTA consultation process that it wants to see more open contracting for all public institutions. "Data residency rules don't make a whole lot of sense. It really creates a false sense of security," said David Messer, ITAC's vice-president of policy. "Most internet traffic, whether it's emails or data … goes around the world," he said, including major exchange points in Seattle or New York. "The way to address security in the cloud and over the internet isn't through data localization," he said, but other safeguards like contractual obligations for service providers and encryption. …

'Standing up for our values'. *John Horgan said during B.C.'s provincial election campaign that he supports maintaining the privacy legislation and would resist any move by the Trump administration to undermine these rights*.

Deal to Share Passenger Info Between EU and Canada Struck Down on Privacy Concerns 🇨🇦

http://www.cbc.ca/news/business/airline-travel-deal-1.4222074

A deal between the European Union and Canada to share airline passenger data must be revised as parts of it violate privacy and data protection laws beyond what could be justified for fighting terrorism, the EU's top court said. The European Court of Justice (ECJ) said that while transfer, retention and use of passenger data was allowed in general, the envisaged rules for handling sensitive personal data "are not limited to what is strictly necessary". The EU's 28 states and Canada negotiated the deal in 2014 but the European Parliament - where the collection of data including names, travel dates, itineraries and contact details, has been debated fiercely - asked for the ECJ's position.

"The PNR (passenger name records) agreement may not be concluded in its current form because several of its provisions are incompatible with the fundamental rights recognised by the EU," the court said on Wednesday. The ruling will come as a blow to governments in Europe who have stepped up their arguments in favour of data retention after a spate of militant attacks over the past years. The bloc's security commissioner, Britain's Julian King, told a news conference in Brussels he would speak to his Canadian counterparts later in the day about "what we're going to do to take account of the points" raised by the ECJ. "Exchanges of information such as PNR are critical for the security of our citizens, and the European Commission will do what is necessary to ensure they can continue in accordance with the Court's opinion and in full respect of fundamental rights." ..The ECJ said PNR data can reveal travel and dietary habits of people, their existing relationships, health conditions and financial situation.

The agreement allows Canada to keep this data for up to five years and possibly share it with other non-EU states, which the ECJ said constituted an "interference with the fundamental right to respect private life" and to personal data protection. Privacy advocates says the schemes are ineffective in battling terrorism while infringing people's privacy.

WestJet Rewards Member Profiles Posted Online After Privacy Breach 🇨🇦

http://globalnews.ca/news/3633823/westjet-rewards-member-profiles-posted-online-after-privacy-breach/

WestJet said it is working with members of the Calgary Police Service and the RCMP after data of some WestJet Rewards member profiles were posted online by an “unauthorized third party.” None of the data contained credit card or banking information, WestJet said in a media release Friday night. The airline said it received an email on Thursday afternoon that appeared to be spam and became aware of the privacy breach on July 28. Immediate steps were taken to secure the affected systems, WestJet said.

“The privacy and protection of our guests’ information is a matter we take very seriously and we have worked swiftly and aggressively to resolve this incident,” said Craig Maccubbin, WestJet’s executive vice-president and chief information officer. WestJet is in the process of contacting affected guests and we deeply regret any inconvenience this may cause.” WestJet said it is still investigating to determine how many member profiles were affected by the breach. The Office of the Information and Privacy Commissioner of Alberta and the federal Privacy Commissioner have also been informed. *WestJet recommends all WestJet Rewards members update their passwords on a regular basis*.

U.S. Man Arrested for Attempted Extortion, DDoS Attacks on Canadian Media, Others 🇨🇦

http://globalnews.ca/news/3636608/ddos-attacks-on-canadian-media/

U.S. authorities announced Friday the arrest of a man in connection with cyberattacks and attempted extortion on a U.S. law website, and several Canadian and Australian news sites that refused to scrub his name from the internet. U.S. Attorney John Parker says 32-year-old Kamyar Jahanrakhshan was arrested Friday and charged with extortion by threats to cause damage to the Dallas-based hosting company for Leagle.com, which provides copies of court decisions, the CBC, The Metro News, Canada.com and the Sydney Morning Herald. According to the attorney general’s office, Jahanrakhshan, from Seattle, threatened Leagle.com with a cyberattack if the firm didn’t remove a court opinion from its website detailing a case he was involved with in Canada.

Leagle.com reported its website was attacked January 2015 and the attack didn’t stop until it removed the opinion from its site. The website was “contacted by an individual by the name of Andrew Rakhshan by e-mail requesting that a URL linking to a court decision involving Rakhshan be deleted,” according to an affidavit filed with the complaint. “Claiming that he was the plaintiff in the case, Rakhshan stated that he did not want the opinion available on the internet as it was tarnishing his reputation and violating his privacy. Rakhshan offered to pay a fee to have the post removed.” According to the attorney general’s office, Jahanrakhshan went by several names including “Andy or Andrew Rakhshan.”

According to court documents, Jahanrakhshan sent an email to the legal website claiming he met a “group of hackers online whom are willing to launch a massive cyberattack.” The man threatened that the group would launch a “distributed denial of service” (DDoS) attack on the site. In January 2015, Jahanrakhshan sent an email to Metronews.ca, allegedly threatening the news site with a DDoS attack if it didn’t delete articles about him from the site, court documents show. “Since I have been deported from Canada and have been banned from entering it for LIFE, I want it out of my life. I cannot afford to be haunted and followed by this ordeal wherever I go in the world,” Jahanrakhshan said in an email, according to an affidavit. “If you do not comply with my demand, Metronews.ca will be hit with a massive cyberattack (DDOS).” Jahanrakhshan was deported from Canada in 2014 after spending 18 months in prison on fraud and obstruction charges. Jahanrakhshan also threatened “death/bomb threats to Metro Offices across Canada and to their employees,” according to the court documents. “I will continue this trend for as long as necessary until you succumb and press ‘delete,’ Jahanrakhshan wrote, according to court documents.

Jahanrakhshan sent similar emails and carried out cyberattacks on the CBC, Canada.com and Fairfax Media properties in Australia and New Zealand, according to the attorney general’s office. *In the emails Jahanrakhshan would often offer to pay for the removal of the links and news stories before threatening the DDoS attacks, according to court documents*. Jahanrakhshan faces up to five years in prison if convicted. [cyber rage?]

Phishers’ Techniques and Behaviours, and What To Do If You’ve Been Phished

https://www.helpnetsecurity.com/2017/07/28/phishers-tactics-and-behaviours/

Once a user has been phished, how long does it takes for the phishers to misuse the stolen credentials? To discover the answer to that question and many others, *Imperva researchers went undercover by creating 90 personal online accounts, including email and file sharing accounts with Google and Dropbox. Once the so-called honey pot accounts were active, the researchers deployed techniques to lure in the criminals and tracked them over the span of nine months*. The research report reveals details of hacker techniques and behaviors, including how long it takes from takeover to exploitation, what the attacker looks for in the hacked account, which decoys attract their attention, and what security practices they use to cover their tracks.

Among the most interesting findings are: (1) **Business data is highly sought.** 25 percent of the phishers looked at email subject lines related to business such as those that included the words financial data, customer database or supplier details. (2) **Attackers aren't quick to act.** More than 50 percent of the accounts were accessed 24-hours or more after the credential takeover. *The result is a brief window where if the attack is suspected, a quick password change results in a 56 percent chance of preventing an account takeover*. (3) **Attackers access content manually not through automated tools.** 74 percent of the first alerts were triggered within three minutes of account penetration. This timing indicates that the attacker accessed bait documents while exploring the inbox. (4) **Less than half of the leaked credentials were exploited by attackers.** *One explanation for this could be that attackers have access to so much data they don't have enough time to explore it all*. (5) **Beside attempts to obtain sensitive information (mostly passwords and credit card numbers) from the hacked accounts**, the attackers also used them for a variety of other things:

Attacker behavior. *The report revealed common behaviors of cybercriminals by delving into how attackers cover their tracks*. *For example, to remain anonymous, attackers should destroy evidence of their presence in accounts by erasing contaminated logins and messages. Yet it was surprising that 83 percent of the attackers did little to cover their tracks*. Of those who did cover their tracks, 15 percent erased new sign-in alerts from the email inbox, but usually forgot to delete them from the email trash container.

The research also demonstrated *phishers are no more careful than their victims*. The researchers planted various traps within the accounts and *most attackers did not hesitate to click the links and open documents - blithely doing so without taking precautionary measures such as using a sandbox or anonymity service*. This also means that with a bit of detective work the cybercriminals can be tracked. "As we began this research, our prediction had been that most accesses would be anonymized through Tor or anonymous proxy services," the researchers also noted. But, as it turned out, *only 39% of the phishers accessed the hacked accounts through Tor, anonymous proxies, or hosting services*. According to the IP addresses from which the other 61% accessed the accounts, more than half of the attackers are located in Nigeria and 22% are in the United States.

"By studying cyberattackers, we've learned many things including that *most attackers don't bother to cover their tracks, which means they leave evidence behind*," said Itsik Mantin, head of data research at Imperva. "Furthermore, if we can quickly detect an attack, we then know that swift remediation including a simple password change significantly reduces the odds of a successful attack."

How to spot if you're account has been compromised?

Firstly and most importantly, if you have been phished and you realized it pretty quickly, you can minimize the damage by accessing your account (if still possible) and making sure to boot the attacker out of it.

Change the password and check to see if the attacker has changed some of your settings in order to keep having access to the account (e.g. a new secondary email address to help with account recovery, email forwarding, etc.) *If you're not sure whether an attacker did ultimately access your account, you can check for three signs he or she did: (1)* "New sign-in alert" emails in the "Trash" folder. "Only 2% of the attackers deleted a new sign-in alert permanently," the researchers noted. (2) If your email provider offers an activity log, check it to see if there have been repeated actions to make messages as "Unread". (3) Check out the "Sent" folder for unusual sent messages, and the "Trash" folder for delivery failure notification messages. During this research, only 13% of the attackers bothered to permanently delete this type of messages.

Hackers Leak Data From Mandiant Security Researcher in Operation #LeakTheAnalyst

https://www.bleepingcomputer.com/news/security/hackers-leak-data-from-mandiant-security-researcher-in-operation-leaktheanalyst/

Earlier today, **a hacker group named 31337 Hackers** has leaked personal details and files belonging to a security researcher working for Mandiant, FireEye's breach investigation unit. The leak came to light today after hackers posted a message on PasteBin. Two download links for the stolen data were included. *The password-protected archives contained information taken from the security researcher's personal computer. Bleeping Computer will not be naming the researcher, even if his name was included in the breach*.

Hackers appear to have hacked the researcher, not FireEye. The leaked data included more screenshots than documents. Images showed that the hackers might have gained access to the researcher's Microsoft (Hotmail, OneDrive) and LinkedIn accounts. Earlier in the day, when Bleeping

Computer was alerted of the leak, the researcher's LinkedIn account had been defaced. The leaked data also included work files related to the researcher's activity at Mandiant, but these files could have very easily been taken from the researcher's OneDrive account and not FireEye servers.
In their brash statement, the hackers claimed they had access to FireEye's internal network, but no file in the leak suggests this might have happened. No other evidence or proof of access to FireEye's internal network was included….
Leak part of operation #LeakTheAnalyst. *31337 Hackers said the leak was part of a larger operation named #LeakTheAnalyst during which they plan to hack and leak data from security researchers, the people who hunt hackers alongside law enforcement officials*.
Message from 31337: "For a long time we - the 31337 hackers - tried to avoid these fancy [EXPLETIVE] "Analysts" whom trying to trace our attack footprints back to us and prove they are better than us. In the #LeakTheAnalyst operation we say [EXPLETIVE] the consequence let's track them on Facebook, Linked-in, Tweeter, etc. let's go after everything they've got, let's go after their countries, let's trash their reputation in the field. If during your stealth operation you pwned an analyst, target him and leak his personal and professional data, as a side job of course ;)."

Embedded Chip on Your Shoulder? Some Privacy and Security Considerations

https://iapp.org/news/a/embedded-chip-on-your-shoulder-some-privacy-and-security-considerations/
On August 1, Wisconsin-based Three Square Market will hold a "Chip Party," where it will embed radio frequency identification chips in its own employees. While RFID technologies are not new - the Center for Democracy & Technology issued a set of best practices for RFID chips in 2006 - the shift to embedding RFID and other technologies into human beings suggests the time for establishing smart policies and clearly communicating them to individuals. *"Cyborgification" raises a host of ethical questions, but employer-driven "chipping" poses at least three immediate challenges*.
The potential for mission creep. We must be cognizant of how these sorts of technologies can be repurposed. The initial plan put forward by 32M focuses on convenience for employees, allowing them to use an installed RFID chip to seamlessly make purchases in the company break room, open doors, access copy machines and log in to their computers. There are a lot of potential conveniences and technological innovation in this space, but companies and society at large should be mindful of the potential for mission creep. Social Security numbers are a prime example of how identifiers might be misused or abused. SSNs were established to serve as a unique identifier or username but became a de facto password and authentication tool. An embedded RFID chip could similarly have far more potential applications than initially planned, and an important question to consider is how 32M might use this technology tomorrow.
32M has emphasized that this program involves no GPS tracking, but RFID and GPS are separate technologies. The surveillance and location-tracking potential of RFID systems, however, is no less significant, depending on where sensors are deployed and who may be monitoring. Companies already use RFID systems to track employee behavior and productivity, as well as to understand team cohesiveness, but there is a qualitative difference when this data is derived from an ID badge one can leave at their desk or in their car and a chip embedded under their skin. The larger vision, according to 32M's CEO, moves closer to Elon Musk's cyberhuman, *using the RFID as a ticket for public transit or a passport for global travel, even as a portal to access and store health information. Such applications might be valuable to employees or consumers, but they should know that the information they are generating is also providing value to a host of marketers, data brokers and law enforcement entities*.
CDT's RFID best practices emphasize the role of appropriate notice. Companies proposing to chip their employees should provide clear disclosures about the specific purposes for which they collect data from embedded technologies and place limitations on how they use information, including what information is being linked together via RFID functionality….
Voluntariness and employee consent
32M insists that its chipping program is entirely optional, but the line between voluntary and obligatory is blurry when it comes to the power imbalance inherent in employee-employer relationships. As we've seen in the rollout of bring-your-own-device programs, employers have offered employees the supposed benefit of using their own phones and computers for work in exchange for comprehensive monitoring rights. A similar dynamic exists in employer wellness programs. Employees who refuse to participate in a program not only face the stigma of being marked as not being a team player, but they also could end up paying more for their health insurance.

Consent is offered as the solution to these problems, but the contours of what constitutes as or how to obtain meaningful consent to be chipped is unclear. Certainly, an employer would require a potential chipped employee to sign a detailed consent form and waive liability for any allergic reaction or installation mishap, but a rote authorization form seems inadequate for giving away body real estate and a measure of autonomy, all so an employee can wave their hands in front of a vending machine….

Safety and security considerations. Finally, it's an open question of how secure RFID chips are. *RFID chips are notorious for leaking information and are, by design, susceptible to eavesdropping and skimming. Companies deploying embedded technologies will need to establish and maintain a reasonable information security program and, in the case of RFID chips, minimize the information stored on the chips themselves*.

What protections are in place to protect employees' privacy when the company changes hands or the employee finds a new job? Beyond removing the RFID chip, which one would hope is a given, what kind of control will an employee have over the data they leave behind? Removing a RFID chip is likely not the most invasive of surgeries, but it is enough to make most people squeamish. Exit interviews, chip removal and a bandage on top probably won't make anyone's last day on the job more pleasant. As we move toward a world where "chipping in" could become part of getting a job, employers, companies and policymakers need to ask and attempt to answer these questions. Employee voices also need to be heard. Certainly, some workers are excited "to be part of the future," but care should be taken to ensure technology is not used as a tool to exacerbate power imbalances in the workplace.

HBO Hacked, Stolen Episode Scripts Leaked Online

http://www.cbc.ca/news/entertainment/hbo-hack-game-of-thrones-ballers-room-104-1.4229173

HBO is the latest entertainment company to suffer a major data breach, as episodes of upcoming television shows were leaked online. According to Entertainment Weekly, *hackers claim to have stolen 1.5 terabytes of data from the prestige TV network*, and leaked the scripts for *Ballers* and *Room 104*. The hackers promised more script leaks, possibly including an upcoming episode of HBO's ratings behemoth *Game of Thrones*. *An anonymous email was sent Sunday to reporters announcing the hack*. "Hi to all mankind. The greatest leak of cyber space era is happening. What's its name? Oh I forget to tell. Its HBO and *Game of Thrones*……!!!!!!" it read.

HBO spokesperson Jeff Cusson would not tell The Associated Press which specific TV episodes, movies or other video the hackers made off with. "HBO recently experienced a cyber incident, which resulted in the compromise of proprietary information," the network said in a statement. "We immediately began investigating the incident and are working with law enforcement and outside cybersecurity firms. Data protection is a top priority at HBO, and we take seriously our responsibility to protect the data we hold." ….HBO has been sensitive to potential hacks that threaten to spoil the plots of upcoming shows, especially the massively popular *Game of Thrones*, which counts shocking moments of betrayal among its highest selling points. In 2015, four episodes of the show's fifth season were leaked online, supposedly from advance screener copies sent to press. HBO has refrained from sending episodes in advance to press ever since.

At Hacker Summit, A New Focus on Preventing Brazen Attacks

https://www.canadiansecuritymag.com/news/data-security/at-hacker-summit-a-new-focus-on-preventing-brazen-attacks

Against a backdrop of cyberattacks that amount to full-fledged sabotage, Facebook chief security officer Alex Stamos brought a sobering message to the hackers and security experts assembled at the Black Hat conference in Las Vegas. In effect, he said, it's time to grow up. *Too many security researchers, he suggested, are focused on "really sexy, difficult problems" that don't address the common vulnerabilities that allow malware attacks to wreak havoc. And too many security-minded hackers seem intent on demonstrating newly discovered hacks, such as making an ATM spit out cash or taking remote control of an internet-controlled car, rather than shoring up more mundane defences*. While part of that reflects the healthy intellectual curiosity of hackers, it's also driven by marketing and economic incentives, Stamos said. "I appreciate the showmanship, but we need a little more thoughtfulness, a little less showmanship in our field," he told reporters after his speech.

Global attacks, serious damage. Since May, the world has been rocked by two major international cyberattacks - the ransomware WannaCry and a likely state-sponsored attack called NotPetya that spread out of Ukraine. Those and other recent digital assaults have paralyzed hospitals, disrupted commerce, caused blackouts and interfered with national elections. Stamos himself was formerly the chief security officer at Yahoo, which last year disclosed breaches of more than a billion user accounts that dated back to 2013 and 2014. *Black Hat, now in its 20th year*, has matured since what Stamos, a long-time attendee of the computer security conference, described as its “edgy and transgressive” early days. It has grown more professional and corporate over time.

Stamos called for a culture change among hackers and more emphasis on defence - and basic digital hygiene - over the thrilling hunt for undiscovered vulnerabilities. And he called for diversifying an industry that skews white and male, and generally showing more empathy for the people whom security professionals are tasked to protect. “It's unfair for us to say that users should be better,” said Stamos, challenging his profession to find better ways to help people solve the most common vulnerabilities, such as reuse of passwords, email phishing attempts, and not updating devices to patch bugs.

Sweden Accidentally Leaks Personal Details of Nearly All Citizens

https://amp.thehackernews.com/thn/2017/07/sweden-data-breach.html

[July 24 - Another Day, Another Data Breach!] This time sensitive and personal data of millions of transporters in Sweden, along with the nation's military secrets, have been exposed, putting every individual's as well as national security at risk. Who exposed the sensitive data? The Swedish government itself.

Swedish media is reporting of a massive data breach in the Swedish Transport Agency (Transportstyrelsen) *after the agency mishandled an outsourcing deal with IBM, which led to the leak of the private data about every vehicle in the country, including those used by both police and military*. *The data breach exposed the names, photos and home addresses of millions of Swedish citizen, including fighter pilots of Swedish air force, members of the military's most secretive units, police suspects, people under the witness relocation programme, the weight capacity of all roads and bridges, and much more*.

The incident is believed to be one of the worst government information security disasters ever.

Here's what and How it Happened:

In 2015, the Swedish Transport Agency hand over to IBM an IT maintenance contract to manage its databases and networks. However, the Swedish Transport Agency uploaded IBM's entire database onto cloud servers, which covered details on every vehicle in the country, including police and military registrations, and individuals on witness protection programs. The transport agency then emailed the entire database in messages to marketers that subscribe to it. And what’s terrible is that the messages were sent in clear text. When the error was discovered, the transport agency merely thought of sending a new list in another email, asking the subscribers to delete the old list themselves.

If you think the scandal ends there, you are wrong. *The outsourcing deal gave IBM staff outside Sweden access to the Swedish transport agency's systems without undergoing proper security clearance checks*. *IBM administrators in the Czech Republic were also given full access to all data and logs*, according to Swedish newspaper Dagens Nyheter (DN), which analysed the Säpo investigation documents.

According to Pirate Party founder and now head of privacy at VPN provider Private Internet Access, Rick Falkvinge, who brought details of this scandal, the incident "exposed and leaked every conceivable top secret database: fighter pilots, SEAL team operators, police suspects, people under witness relocation."

Tons of Sensitive Info Exposed about Both Individuals and Nation's Critical Infrastructures

According to Falkvinge, the leak exposed: The weight capacity of all roads as well as bridges (which is crucial for warfare, and gives a lot idea about what roads are intended to be used as wartime airfields), Names, photos, and home addresses of fighter pilots in the Air Force, Names, photos, and home addresses of everybody in a police register, which are believed to be classified, Names, photos, and residential addresses of all operators in the military's most secret units that are equivalent to the SAS or SEAL teams, Names, photos, and addresses of everybody in a witness relocation program, who has been given protected identity for some reasons, and Type, model, weight, and any defects in all government and military vehicles, including their operator, which reveals much about the structure of military support units.

Although the data breach happened in 2015, Swedish Secret Service discovered it in 2016 and started investigating the incident, which led to the fire of STA director-general Maria Ågren in January 2017. Ågren was also fined half a month's pay (70,000 Swedish krona which equals to $8,500) after finding her guilty of being "careless with secret information," according to the publication. What's the worrying part? *The leaked database may not be secured until the fall*, said the agency's new director-general Jonas Bjelfvenstam. The investigation into the scope of the leak is still ongoing.

Google Ransomware Tracking Finds Vicious Infection Cycle

https://www.usatoday.com/tech/

Ransomware surged last year, becoming a multi-million dollar business that's so profitable it's creating a "vicious cycle" of ever-increasing attacks, say researchers at New York University and Google who tracked the criminals' payment networks. "It's here to stay," said Elie Bursztein, anti-abuse research lead at Google. *The findings suggest that - even though the last two large ransomware attacks, WannaCry and Petya, did not seem to raise that much money - the criminal cyber industry in general has much to gain by exploiting users with these attacks*. The research team was able to track ransomware payment addresses and information via public sales of the digital currency bitcoin, watching more than $25 million in payments over the past two years. They plan to present their research on Wednesday in Las Vegas at Black Hat, one of the country's largest computer security conferences.

<u>Ransomware is malicious software that criminals use to first infect a victim's computer and then encrypt the files on it. To regain access to their files, victims must pay a ransom, typically in anonymous digital currency such as bitcoin.</u> It is increasingly one of the biggest money-makers for cyber criminals, who have been diligently creating new forms of it to boost their earnings. *A recent variant, Cerber, is able to fully encrypt a newly-infected computer in under a minute and has consistently made $200,000 per month over the last year, the researchers found*. "It's a vicious cycle, the more money they make, the more aggressively they spread the malware," said Bursztein.

One popular method is **"ransomware-as-a-service," where criminal organizations rent out ransomware programs and the support system necessary to get paid to other criminals, charging a cut of the profits for the service**, according to a 2017 Verizon report on data breach investigations. Other innovations include time limits after which the criminals delete encrypted files, ransoms that increase the longer the victim takes to pay, ransom prices that vary based on the estimated sensitivity of filenames and a new option that allows victims to decrypt their files for free if they help infect others. Ransomware programs aren't typically "owned" by any one group of criminals. In fact, *the researchers tracked 34 different families of ransomware that are being distributed by criminals*. However, some of those criminals are better at making money off their crimes than others and have developed real expertise in how to push their programs out to more victims and make it easy for victims to pay them, said Damon McCoy, a New York University computer science and engineering professor who researches ransomware.

Criminal innovations: help desks. *This can include amenities such as multi-lingual help desks to assist the victims in buying digital currency to pay the ransom*. *With these new features, infection numbers began to shoot up in the second quarter of 2016 and have stayed high ever since* - and it doesn't seem likely they're going to come down any time soon because it's such a profitable crime, said McCoy. It's also difficult to stop because *it's hard to track where the money's going and thus find the criminals who are receiving it. The research team found that 95% of the ransoms they observed being paid went through BTC-E, a bitcoin exchange platform*. "It's hard for law enforcement to put pressure on BTC-E because it's a Russian-operated bitcoin exchange," said McCoy.

Google has seen concern about ransomware among the public ratchet up significantly in the past year and a half. Searches about ransomware have increased more than ten times, said Berzstein. <u>While the researchers couldn't offer a fix for the overall problem of ransomware, they did have one piece of advice – back data up regularly. A Google survey found that just 37% of people do so, putting them at risk for losing irreplaceable photos and documents forever</u>. "We really really want to encourage people to back up their files," said McCoy.

And Now, This:

Facebook Pulls Plug on AI Bots After They Start Inventing Their Own Language

http://globalnews.ca/news/3634438/facebook-ai-robots-develop-own-language/

Researchers at Facebook recently shut down a pair of AI [artificial intelligence] bots that were designed to communicate with each other in English, after they instead began using a new language by rearranging English words into seemingly gibberish sentences. *Only the sentences weren't completely nonsensical, but actually comprised a coded language that made sense to the bots*, scientists with Facebook AI Research (FAIR) told *Fast Co. Design*.

Here's a sample of the conversation that transpired between the bots, dubbed "Bob" and "Alice":

Bob: i can i i everything else
Alice: balls have zero to me to me to me to me to me to me to me to me to
Bob: you i have everything else
Alice: balls have a ball to me to me to me to me to me to me to me to me

The conversation continues to carry on in a similar vein, according to a screen shot published by *Fast Co. Design*. “Agents will drift off understandable language and invent code words for themselves,” FAIR researcher Dhruv Batra told the magazine. “Like, if I say ‘the’ five times, you interpret that to mean I want five copies of this item. This isn’t so different from the way communities of humans create shorthands.” *In other words, it’s similar to how specialized communities of humans, such as stockbrokers or sailors, develop their own dialects which are functional for their specific environments*. *Batra added that the bots began developing the language because of a programming error which, in effect, gave them an incentive to develop a more efficient language*.

The bots were created as part of a program that aims to teach machines how to negotiate, with a view to ultimately developing personalized digital assistants capable of communicating with humans, FAIR researchers said in a June blog post. “Bob” and “Alice” were shut down not because it was feared that they were plotting to overthrow humans and take over the world, but rather because FAIR researchers want to develop bots capable of talking to people, research scientist Mike Lewis told *Fast Co. Design*.

Feel free to forward the Digest to others that might be interested.
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.

****