BRITISH COLUMBIA OCIO Office of the Chief Information Officer

Security News Digest

March 27, 2018

March is Fraud Awareness Month

Take our quiz and test your knowledge

On this day in history (March 27th)

1964 - B.C. tsunami's disaster: Residents of Port Alberni, BC pick up the pieces following 1964's massive tsunami.

This week's stories:

- **Best Way To Fight The Rise Of The Machines? 'Human Skills', Study Says** 🇨🇦
- **Spy agency chief says new powers would help stop cyberattacks before they happen** 🇨🇦
- **Bitcoin 'I just want my money back.' Couple had $100K wire stuck for months after trying to buy Bitcoin** 🇨🇦
- **The Top Vulnerabilities Exploited by Cybercriminals**
- **Facebook's data scandal should be a wake-up call about our online footprint**
- **DHS: Some GE Imaging Devices Are Vulnerable**
- **Elon Musk reveals the real reason why he deleted Tesla & SpaceX pages on Facebook**
- **Expedia's Orbitz says 880,000 payment cards hit in breach**
- **A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try**
- **Dog That Shoplifted a Book on 'Abandonment' is Given the Love it was Asking For**

Best Way to Fight the Rise of the Machines? 'Human Skills', Study Says 🇨🇦

https://www.huffingtonpost.ca/2018/03/26/automation-human-skills_a_23395371/

OTTAWA — A year into its effort to help equip youth for the rapidly evolving workforce, one of the country's largest banks says enhancing young Canadians' human skills will be critical in navigating the machine-led disruption that lies ahead. In a new study, the Royal Bank of Canada is calling for a national review of post-secondary programs to ensure they place more of a focus on "human skills" — from active listening, to critical thinking, to social perceptiveness. The research argues these foundational skills will help future workers remain nimble and position them to complement increasingly pervasive technologies like robots and machines, rather than compete with them. And it warns that without action Canadians will not be ready for inevitable changes over the next decade or two. Many say the transformation is already underway.

Governments have poured energy and funding into efforts to prepare workers for a significantly altered labour force, which will be driven by technological advances, such as automation and artificial intelligence. For example, the federal government has emphasized the importance of promoting the fields of STEM — science, technology, engineering and mathematics — to help youth prepare for the future workforce. In its recent budget, Ottawa also noted that one million students will learn coding and digital skills through its CanCode program. But the RBC study found that while digital literacy is increasingly critical for all workers, it won't be as crucial for everyone to learn a specific expertise like coding. Foundational human skills, on the other hand, can truly improve a worker's opportunities and mobility.

"To help Canada's next generation do the disrupting instead of being disrupted, we need to start with 21st-century skills — skills they can use to grasp new opportunities and surf the waves of technology and innovation that are changing the world," said the report titled, "Humans Wanted," to be released Monday. "We need to stop telling them that work revolves only around degrees, qualifications and jobs." RBC president and CEO Dave McKay said in an interview that if policy-makers and employers don't do more to start preparing now, then Canada could run into a lot of challenges — from competitiveness obstacles to social-cohesion issues. "We believe there's a national dialogue that's lacking around this issue," said McKay, who noted the study estimated more than 25 per cent of Canadian jobs will be heavily disrupted in the next decade and half will require far different skills than they do now. He said Canada currently spends a lot of money as a society to train people in skills and roles that won't be needed down the road or, at the very least, will be a significant mismatch. "It won't be good enough if we keep training ourselves on the same old, same old going forward — machines can do a lot of what we're training students for," McKay said.

Canada, like many countries, suffers from a shortage in skills in their young people, like leadership, decision making, communication and emotional intelligence, he said. The report also recommends a national target to provide work-integrated learning, like internships and apprenticeships, for 100 per cent of undergraduate students. The federal government has committed funds to work-integrated learning. Last year, for example, it announced a program to help create work placements for 60,000 students over the next five years. Asked about federal efforts to prepare the next generation, McKay said it's not enough, so he wants to work with Ottawa. "They seem to be small and I don't have the actual execution plans, so yes, there's money that they put aside, but to do exactly what?" McKay said of Ottawa's promises. "We have a plan and a vision of what success looks like. We hope the two will come together." The report is part of RBC's 10-year, $500-million commitment toward helping young people prepare for the future workforce.

The hunt for solutions to the impending workforce skills challenges have been preoccupying governments and business leaders for several years. Later this week, several federal cabinet ministers will host a G7 meeting in Montreal to explore how best to prepare for jobs of the future with their counterparts from other member countries.

The Canadian Chamber of Commerce released a report last week that said businesses should invest now in the skills development and lifelong learning to ensure their workers will have the tools to face the coming disruptions from AI, advanced robotics and automation. It's better to re-train workers now rather than waiting until after these new technologies have taken their jobs, the organization said. If properly harnessed, new advances can improve production and boost economic growth and even create jobs. The Chamber's report also noted the importance of social skills. It said people interviewed for the document praised British Columbia's school system for its new curriculum emphasizing areas like social skills, communication, and creative and critical thinking. The report said these lessons are being integrated with lessons for traditional skills, such as numeracy and literacy.

‘I just want my money back.’ Couple had $100K wire stuck for months after trying to buy Bitcoin

https://globalnews.ca/news/4090875/100k-wire-transfer-bitcoin-canada-quadriga-cx/?utm_source=GlobalNews&utm_medium=Facebook

Michelle Yi and her husband Min Jae Kim of Coquitlam, B.C., thought they’d found a relatively low-risk way to make money with Bitcoin. Like many others, the Coquitlam, B.C., couple decided to put money into Bitcoin after the cryptocurrency surged to an all-time high of nearly $19,000 U.S ($24,500 Canadian) at the end of last year. Yi, an accountant, had read about the extreme volatility of digital money, but the investment they had in mind seemed to have little to do with that. The plan was to buy Bitcoin in order to sell it in South Korea, where the digital money was trading at a premium of 40 per cent to 50 per cent compared to the North American market. It seemed like an easy and relatively low-risk way to make a hefty profit. So the couple sent a $100,000 wire transfer to Vancouver-based cryptocurrency exchange Quadriga CX on Jan. 9. That’s when their money seemingly vanished into thin air. “I just want my money back,” Yi told Global News via telephone on March 16. Over two months had passed, and the couple still had no idea where the funds had gone.

The couple were eventually reunited with their money a few days later. After Global News got in touch with Quadriga about the issue, the company swiftly processed the wire transfer, waived a $2,000 processing fee and, upon Yi’s request, returned the funds to Kim’s bank account. **But Yi and Kim’s story illustrates another set of risks facing Canadians who invest in Bitcoin and other digital tokens — one that has little to do with gyrations of the crypto market, hackers, or criminals using virtual currencies to buy and sell contraband.**

Global News spoke to several other sources who said transactions to and from Quadriga accounts took weeks or months to process. Some are still waiting to see their money reappear. The issue seems to be only in part due to customer service problems at Quadriga, which is one of Canada’s two established cyrptocurrency exchanges, along with Toronto-based Coinsquare. A lack of banking support for cryptocurrency-based companies is causing technical difficulties, Quadriga told Global News. And Canada’s financial regulators are of little help when things go wrong. When Yi and Kim’s $100,000 failed to materialize into Yi’s Quadriga account, the couple said it tried in vain to contact Quadriga about it. The company doesn’t have a publicly available phone number and asks customers to get in touch with customer service through electronic tickets. Yi submitted multiple support requests but only received auto-reply emails, she told Global News. Either Quadriga is a “scam” or “they have beyond bad customer service,” Yi said in a telephone interview before Global News contacted Quadriga. Luckily, it turned out not to be a scam.   The wire wasn’t processed because the couple had sent the wire from a Toronto-Dominion (TD) bank account in Kim’s name, which didn’t match the recipient account, which was in Yi’s name, Quadriga CEO Gerald Cotten told Global News. “We make it very clear that we don’t accept wires from third parties,” Cotten said. “We do that because we want to prevent fraud.” Yi and Kim had realized their mistake shortly after sending the wire but weren’t able to communicate that to Quadriga.

The company told Global News it didn’t process the couple’s support requests because they did not follow instructions at the bottom of its auto-replies that read: “If this email and Support Centre content didn’t provide the answer you were looking for, please reply back with ‘the content within this email and Support Centre didn’t help, please assist’ and your ticket will be positioned back in the queue for a support agent to respond to.” Yi said she simply didn’t notice the instructions, which came after 800 words of text that walks Quadriga customers through common customer support issues, according to a Quadriga auto-reply viewed by Global News. *[Read the rest of the article online to learn more about this story]*

Spy agency chief says new powers would help stop cyberattacks before they happen 🇨🇦

https://www.canadiansecuritymag.com/news/data-security/spy-agency-chief-says-new-powers-would-help-stop-cyberattacks-before-they-happen

OTTAWA — The head of Canada's cyberspy agency says new powers proposed by the Trudeau government would let her institution stop cyberattacks before they are launched — instead of having to sit back and wait for them to happen. Communications Security Establishment chief Greta Bossenmaier made the comments to a parliamentary committee in which she revealed the agency has been working overtime to block attacks on federal networks. The problem includes up to one billion attempts to compromise federal government information systems every day, which includes everything from poking to malware to dedicated hacking.

Bossenmaier says Bill C-59 would help nip some of those attacks in the bud as well as target terrorist groups and support military missions by giving the CSE the power to launch its own offensive cyber operations. The government's plan to let the CSE to launch cyberattacks has raised a variety of questions over the last year, including the process for authorizing such an operation and how the agency will ensure it doesn't target Canadians. Defence Minister Harjit Sajjan and CSE officials told the committee that there were strict approval processes and oversight provisions within the legislation, and that the law forbids any action against Canadians or targets in Canada.

The Top Vulnerabilities Exploited by Cybercriminals

https://www.securityweek.com/top-vulnerabilities-exploited-cybercriminals

Cybercriminals are shifting their focus from Adobe to Microsoft consumer products, and are now concentrating more on targeted attacks than on web-based exploit kits. Each year, Recorded Future provides an analysis of criminal chatter on the dark web in its Top Ten Vulnerabilities Report. It does this because it perceives a weakness in traditional vulnerability databases and scanning tools -- they do not indicate which vulnerabilities are currently being exploited, nor to what extent. Reliance on vulnerability lists alone cannot say where patching and remediation efforts should be prioritized. "We do this analysis because the sale and use of exploits is a for-profit industry," Recorded Future's VP of technical solutions, Scott Donnelly told *SecurityWeek*. This means that exploit developers have to sell their products, while other criminals have to buy them -- and this leads to the chatter that Recorded Future analyzes. "If you're a cybercriminal trying to make money, you have to discuss it. If you hold back too much you're not going to make any money; so, there's a necessity for the criminals to stick their heads up a little bit -- and we can take advantage of that and call out some of the big conversations." It assumes a correlation between chatter about a vulnerability with active exploitation of that vulnerability -- an assumption that common sense rather than science suggests is reasonable.

Donnelly is confident that his firm's knowledge of and access to the dark web is statistically valid. Nation-state activity is specifically excluded from this analysis, because, he says, "If you're a nation-state with an exploit, or if you're a third-party supplier of exploits to a nation state, you're less likely to talk about it in a general criminal forum." **At the macro level, this year's analysis highlights a move away from Adobe vulnerabilities towards Microsoft consumer product vulnerabilities. While Flash exploits have dominated earlier annual reports, seven of the top ten (including the top five) most discussed vulnerabilities are now Microsoft vulnerabilities. "As Adobe Flash Player has begun to see its usage significantly drop, this year we find that it's a lot of Microsoft consumer products that are seeing heavy exploitation,"** says Donnelly.

The three most used vulnerabilities are CVE-2017-0199 (which allows attackers to download and execute a Visual Basic script containing PowerShell commands from a malicious document), CVE-2016-0189 (which is an old Internet Explorer vulnerability that allows attackers to use an exploit kit to drop malware, such as ransomware), and CVE-2017-0022 (which enables data theft).

A second major takeaway from the analysis is that 2017 has seen a significant drop in the development of new exploit kits. "This has been noticed before," Donnelly told *SecurityWeek*, "but mainly because researchers simply haven't seen them in action. This is now evidence that the criminals themselves aren't talking about or trying to sell that many new kits." In raw numbers, Recorded Future's analysis noted 26 new kits in 2016, but only 10 new kits in 2017 (from a total list of 158 EKs). "The observed drop in exploit kit activity," suggests Donnelly, "overlaps with the rapid decline of Flash Player usage. Users have shifted to more secure browsers, and attackers have shifted as well. Spikes in cryptocurrency mining malware and more targeted victim attacks have filled the void."

At the micro level, the big takeaway from this report is the anomalous position of CVE-2017-0022. It is the third most discussed vulnerability on the dark web forums, yet in relation to just two pieces of malware: exploit kits Astrum (aka Stegano) and Neutrino. This is the lowest number of associated malware in the top ten vulnerabilities -- both of the two more popular vulnerabilities are associated with ten different pieces of malware. CVE-2017-0199 is associated with malware including Hancitor, Dridex and FinFisher, while CVE-2016-0189 is associated with nine different exploit kits and the Magniber ransomware.

But it's not just in malware associations that CVE-2017-0022 is anomalous. It has a Common Vulnerability Scoring System (CVSS) rating of just 4.3. The next lowest rating in the top ten vulnerabilities is 7.6, while the top two are rated at 9.3 and 7.6. CVSS defines a 4.3 score as medium risk; and yet Recorded Future's research shows it to be the third most exploited vulnerability, commenting, "'In the wild' severity does not always correlate with the Common Vulnerability Scoring System (CVSS) score." This is a prime example of the reason for the analysis. Security teams could check the CVSS score and conclude on this evidence alone that the vulnerability does not require expedited remediation or patching. As the third most exploited vulnerability, Recorded Future's latest threat analysis suggests otherwise. Boston, Mass.-based Recorded Future raised $25 million in a Series E funding round led by Insight Venture Partners in October 2017 -- bringing the total funding raised to $57.9 million

Facebook’s data scandal should be a wake-up call about our online footprint

(A CNBC commentary by Arjun Kharpal)
https://www.cnbc.com/2018/03/27/facebook-data-scandal-should-be-a-wake-up-call-about-online-footprint.html

- Facebook is still suffering the fallout from the Cambridge Analytica data scandal.
- The episode highlighted a big problem: We download apps and allow services to collect information about us without a second thought.
- The good to come out of this Facebook scandal is that people could get smarter about their online footprint.

Believe it or not, something good for consumers could come out of the Facebook data scandal. To recap, a quiz app harvested 50 million Facebook profiles for data which were then sent over to Cambridge Analytica, a firm that was caught claiming it handled the digital aspects of President Donald Trump's 2016 election campaign. The data was collected from people without their knowledge, but Facebook said that users had their privacy settings on to allow it. Even as someone who covers technology extensively, it was a real eye-opener seeing what information Facebook is collecting, even though we give it permission to by signing up, then checking in to a place, or uploading a picture. Like many, I have recently downloaded a file that contains the information Facebook holds about me.

And on the weekend, Ars Technica highlighted a tweet from New Zealand man Dylan McKay who posted a picture of his call history with his partner's mum that Facebook had collected. On Sunday, the social network said this was done with users' permission. **This is the problem: We download apps and allow services to collect information about us without a second thought. The good to come out of this Facebook episode is that people get smarter about their online footprint. Users should be checking what data services have access to. It's not just Facebook of course, other big technology firms are in the business of collecting data which is central to their business models. The Facebook episode should be a wake-up call for people when it comes to learning about the information out there about them**. And it seems to be so. An article on CNBC titled "How to download a copy of everything Facebook knows about you," which was written last week, was still one of the top read pieces on our site Monday. But the onus is not just on users. **Big tech firms need to step** up. When a user is signing up for a service or downloading an app, the information being collected and how it will be used needs to be clearly stated. And it must be easy for users to change how their data is accessed. Tech firms should also be more responsible in the way they word messages asking for consent. Often they will ask to track some information because it provides a "better experience". It may do, but the price you are paying is invaluable data that will make these firms money. It's irresponsible for tech giants to ask people for consent in this way.

Taking control of your data has never been more important. Facebook CEO Mark Zuckerberg has talked up the potential of machine learning and artificial intelligence. This is potentially scary technology that can read and use data in ways like never before. With such a prospect ahead, **understanding your online life, owning your data and restricting it where necessary, should be your number one priority**.

Elon Musk reveals the real reason why he deleted Tesla & SpaceX pages on Facebook

https://www.moneycontrol.com/news/technology/elon-musk-reveals-the-real-reason-why-he-deleted-tesla-spacex-pages-on-facebook-2536641.html

Elon Musk, the CEO of Tesla Motors and SpaceX, said on Saturday in a tweet that Facebook gives him a feeling of nervousness and fear. Replying to a news report about Tesla and SpaceX deleting their Facebook pages, he said, “It’s not a political statement and I didn’t do this because someone dared me to do it.” “Just don’t like Facebook. Gives me the willies. Sorry”.

Elon Musk had promised to delete the Facebook accounts of SpaceX and Tesla Motors (which he acted upon) on a suggestion of one of the Twitter users. He had then said that he didn’t know there were any Facebook pages of the organisations he owns. The #deletefacebook movement started on social media after one of the founders of WhatsApp Brian Acton tweeted that it was time to delete Facebook in the wake of sweeping user data leak revelations.

Many other companies have also deleted or deactivated their Facebook pages. Mozilla Foundation which develops Mozilla browser and Thunderbird, an email and news client said in a blog post last week, "We're taking a break from Facebook." It said it is "pressing pause" on its Facebook advertising and won't be posting on its Facebook page. But it did not delete its page and said it will consider returning if Facebook takes stronger actions to protect users' data and improves privacy settings.

German bank Commerzbank also said it was putting Facebook advertising "on hold" as it evaluates data security. And Sonos, which makes speakers and other electronics, said it is pulling advertising from Facebook, Instagram, Google, and Twitter for a week. The widespread reaction is following the revelations of a major leak of user data to political consultants namely Cambridge Analytica associated with the 2016 Trump campaign. Share prices of Mark Zuckerberg led company tanked over 13 percent last week.

DHS: Some GE Imaging Devices Are Vulnerable

https://www.databreachtoday.com/dhs-some-ge-imaging-devices-are-vulnerable-a-10727

A recent alert from the Department of Homeland Security warning of vulnerabilities in certain medical imaging product lines from GE Healthcare also serves as a reminder to other medical device makers and healthcare entities about the risks posed by hardcoded and default credentials.
In a March 13 advisory, DHS's Industrial Control Systems Cyber Emergency Response Team says independent researcher Scott Erven contacted the agency regarding the potential use of default or hardcoded credentials in certain GE Healthcare imaging products. "Successful exploitation of this vulnerability may allow a remote attacker to bypass authentication and gain access to the affected devices," the alert notes. The risks posed by medical devices left vulnerable due to hardcoded and default passwords are substantial, says Phil Curran, chief information assurance officer and chief privacy officer at Cooper University Health Care in Camden, New Jersey. "Depending on what function the user ID/password provides within the code, the range goes from affecting how the device operates - a patient safety issue - to changing data - integrity - to complete shutdown to accessing patient information," he says.

Following the researcher's report about the findings, GE performed a self-assessment and validated that some imaging products use default or hard-coded credentials, ICS-CERT says. "GE has reviewed the capability to change passwords identified by the researcher within the product documentation, and users are advised to contact GE Service for assistance in changing passwords."

Among the GE Healthcare devices included in the ICS-CERT advisory are various imaging systems in the company's Optima, Discovery, Revolution, Centricity, THUNIS, eNTEGRA, CADStream, GEMNet, Infinia, Millenium, Precision MP/i, and Xeleris product families. ICS-CERT notes in the advisory that according to GE, the affected products are deployed across the healthcare sector worldwide. But some of the products included on the list, such as the Optima 680, the Image Vault 3.x, and the THUNIS-800+, have very limited or no use in the U.S. or Canada, ICS-CERT notes.

In a statement provided to ISMG, GE Healthcare says it is "aware of the recent ... ICS-CERT advisory, which provides an update from a previously published US-CERT bulletin that addresses the use of default credentials in certain products. We are working closely with customers to implement best practices for security and supporting requests for assistance in changing passwords." Medical device cybersecurity researcher Billy Rios tells ISMG: "Hardcoded passwords are a huge problem in healthcare cybersecurity." In fact, it was the discovery by Rios and a fellow researcher, Terry McCorkle of security vendor Cylance, of 300 hardcoded passwords in medical devices from 40 vendors several years ago that served as a catalyst for the Food and Drug Administration to issue pre-market guidance to medical device manufacturers in 2013, Rios notes (see *Medical Device Vulnerability Alert Issued*).

At the same time ICS-CERT issued an alert about the discovery by Rios and McCorkle about the medical device hardcoded passwords, the FDA also issued draft guidance recommending that manufacturers design and build cybersecurity into their medical devices (see *FDA Drafts Medical Device Guidance*).

"We've already witnessed malware like the Mirai botnet utilizing default passwords in devices to exploit them; it's only a matter of time before a similar strategy is used for medical devices," Rios tells ISMG. "In most cases, these passwords are used by service technicians to service medical devices," he says. To address the problem, "hospitals can take the research provided by [Erven] and use that data to disable the interfaces associated with the technical interfaces," Rios says. "If the device needs to be serviced, hospitals can enable the technician interface during service activity and disable the interface when the service activity is completed." *[Read the rest of the article online to learn more about this story]*

Expedia's Orbitz says 880,000 payment cards hit in breach

https://www.reuters.com/article/us-orbitz-cyber/expedias-orbitz-says-880000-payment-cards-hit-in-breach-idUSKBN1GW23V

(Reuters) - **Orbitz, a subsidiary of online travel agency Expedia Inc (EXPE.O), said on Tuesday that hackers may have accessed personal information from about 880,000 payment cards**. The unit said an investigation showed that the breach may have occurred between Jan. 1, 2016 and Dec. 22, 2017 for its partner platform and between Jan. 1, 2016 and June 22, 2016 for its consumer platform.

Information such as names, phone numbers, email and billing addresses may have been accessed, the travel website operator said, adding that its website, Orbitz.com, was not impacted. "To date, we do not have direct evidence that this personal information was actually taken from the platform and there has been no evidence of access to other types of personal information, including passport and travel itinerary information," Orbitz said.

For U.S. customers, social security numbers were not involved in this incident, the company said. The company said it has addressed the breach after it was discovered in March this year. Credit card issuer American Express Co (AXP.N) said in a statement that the attack did not compromise its platforms. The breach is the latest in the travel sector and follows attacks on global hotel chain InterContinental Hotels Group Plc (IHG.L) and Hyatt Hotels Corp (H.N) last year. Expedia's shares fell as much as 1.9 percent to $108.99.

A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try

https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html

In August, a petrochemical company with a plant in Saudi Arabia was hit by a new kind of cyberassault. **The attack was not designed to simply destroy data or shut down the plant, investigators believe. It was meant to sabotage the firm's operations and trigger an explosion. The attack was a dangerous escalation in international hacking, as faceless enemies demonstrated both the drive and the ability to inflict serious physical damage.** And United States government officials, their allies and cybersecurity researchers worry that the culprits could replicate it in other countries, since thousands of industrial plants all over the world rely on the same American-engineered computer systems that were compromised.

Investigators have been tight-lipped about the August attack. They still won't identify the company or the country where it is based and have not identified the culprits. But the attackers were sophisticated and had plenty of time and resources, an indication that they were most likely supported by a government, according to more than a dozen people, including cybersecurity experts who have looked into the attack and asked not to be identified because of the confidentiality of the continuing investigation. The assault was the most alarming in a string of hacking attacks on petrochemical plants in Saudi Arabia. In January 2017, computers went dark at the National Industrialization Company, Tasnee for short, which is one of the few privately owned Saudi petrochemical companies. Computers also crashed 15 miles away at Sadara Chemical Company, a joint venture between the oil and chemical giants Saudi Aramco and Dow Chemical.

Within minutes of the attack at Tasnee, the hard drives inside the company's computers were destroyed and their data wiped clean, replaced with an image of Alan Kurdi, the small Syrian child who drowned off the coast of Turkey during his family's attempt to flee that country's civil war. The intent of the January attacks, Tasnee officials and researchers at the security company Symantec believe, was to inflict lasting damage on the petrochemical companies and send a political message. Recovery took months. Energy experts said the August attack could have been an attempt to complicate Crown Prince Mohammed bin

Salman's plans to encourage foreign and domestic private investment to diversify the Saudi economy and produce jobs for the country's growing youth population. "Not only is it an attack on the private sector, which is being touted to help promote growth in the Saudi economy, but it is also focused on the petrochemical sector, which is a core part of the Saudi economy," said Amy Myers Jaffe, an expert on Middle East energy at the Council on Foreign Relations.

Saudi Arabia has cut oil exports in recent years to support global oil prices, a strategy central to its efforts to make a potential public offering of shares of government-controlled Saudi Aramco more attractive to international investors. The kingdom has tried to compensate for its lost revenue by expanding its petrochemical and refining industry. Some technical details of the attack in August have been previously reported, but this is the first time the earlier attacks on Tasnee and other Saudi petrochemical companies have been reported. Security analysts at Mandiant, a division of the security firm FireEye, are still investigating what happened in August, with the help of several companies in the United States that investigate cyberattacks on industrial control systems
.
A team at Schneider Electric, which made the industrial systems that were targeted, called Triconex safety controllers, is also looking into the attack, the people who spoke to The Times said. So are the National Security Agency, the F.B.I., the Department of Homeland Security and the Pentagon's Defense Advanced Research Projects Agency, which has been supporting research into forensic tools designed to assist hacking investigations. **All of the investigators believe the attack was most likely intended to cause an explosion that would have killed people. In the last few years, explosions at petrochemical plants in China and Mexico — though not triggered by hackers — have killed several employees, injured hundreds and forced evacuations of surrounding communities.**

What worries investigators and intelligence analysts the most is that the attackers compromised Schneider's Triconex controllers, which keep equipment operating safely by performing tasks like regulating voltage, pressure and temperatures. Those controllers are used in about 18,000 plants around the world, including nuclear and water treatment facilities, oil and gas refineries, and chemical plants. "If attackers developed a technique against Schneider equipment in Saudi Arabia, they could very well deploy the same technique here in the United States," said James A. Lewis, a cybersecurity expert at the Center for Strategic and International Studies, a Washington think tank. The Triconex system was believed to be a "lock and key operation." In other words, the safety controllers could be tweaked or dismantled only with physical contact.

So how did the hackers get in? Investigators found an odd digital file in a computer at an engineering workstation that looked like a legitimate part of the Schneider controllers but was designed to sabotage the system. Investigators will not say how it got there, but they do not believe it was an inside job. This was the first time these systems were sabotaged remotely. **The only thing that prevented significant damage was a bug in the attackers' computer code that inadvertently shut down the plant's production systems.** Investigators believe that the hackers have probably fixed their mistake by now, and that it is only a matter of time before they deploy the same technique against another industrial control system. A different group could also use those tools for its own attack.
[Read the rest of the article online to learn more about this story]

And Now this:

Dog That Shoplifted a Book on 'Abandonment' is Given the Love it was Asking For

https://www.goodnewsnetwork.org/dog-shoplifts-book-on-abandonment/

Instead of being disciplined for his misdeeds, this unlikely shoplifter is being given more love and attention than ever before. Last week, a stray dog was caught on camera sneaking into the Feevale University bookshop in Novo Hamburgo, Brazil. After managing to get past the front desk, the pup grabs a book in its mouth and trots out of the store. But it wasn't just any book – it was a book entitled "The Days of Abandonment"; a pretty relatable topic for many stray animals. Before the dog had a chance to read the pages, one of the campus students retrieved the book and gave it to the astonished cashier who was working the front desk. The bookshop staff was so tickled by the sneaky dog, they posted a video of the heist to Facebook where it later went viral.

As fate would have it, a group of local animal rescuers saw the video, stopped by the bookshop, and checked the dog into their care. The dog was given a bath, its vaccinations, and a foster home for him to live happily ever after until he finds a forever home.

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

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.

****