Security News Digest
October 03, 2017

October is Cyber Security Awareness Month

There are so many major data breaches in the news that this the ideal time for the
October Breaches Everywhere Quiz

Visit the Security Awareness Cyber Security Awareness Month page at:
http://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/information-security-awareness/cyber-security-awareness-month
The theme this year for the National campaign is "Our Shared Responsibility".

Canada's NAFTA Negotiators Must Do More to Protect Canadians' Data from U.S.: Privacy Experts

https://globalnews.ca/news/3777464/canada-urged-to-do-more-to-protect-data-from-u-s-during-nafta-talks/

Concern is growing that federal negotiators aren't doing enough to protect the personal information of Canadians from prying U.S. interests at the North American Free Trade Agreement negotiations.
Information technology companies and other digital economy insiders say federal negotiators appeared unprepared during this week's third round of talks to counter an American proposal that would forbid the storage of sensitive data in computing facilities on Canadian soil.
Some warned that Canada appeared soft on the issue and might concede to the American demands in the interest of horse-trading – to potentially win concessions on higher-profile areas of contention, such as autos and agriculture. They say giving in to American demands to open up a freer flow of cross-border data would not only undermine domestic privacy rights, but hamstring the ability of emerging Canadian companies to compete in the growing digital economy. **At issue is so-called "data localization," which would allow the government to protect the sensitive personal information of Canadians – especially health and financial records – from unwanted American intrusion, by storing it in Canada.** A senior federal official, who would only speak on the condition they not be identified, said the government would stand up for Canadians' data and privacy rights at the bargaining table.
Widespread global concern has been stoked by fears of U.S. surveillance on private citizens, and requirements under the post 9-11 Patriot Act that gives American law enforcement access to data stored in U.S. facilities. **Big companies such as Amazon and Microsoft have built servers in Canada to address privacy concerns.** Sources say U.S. negotiators proposed NAFTA terms that banned data localization, lifting language directly from the failed Trans-Pacific Partnership. **The U.S. position contrasts with British Columbia and Nova Scotia laws that require local data storage and appears to conflict with federal policy, which says "sensitive or protected data under government control will be stored on servers that reside in Canada."**
Canada lacks an overall strategy on the data and should not give in to American demands until it develops one, said Keith Millar, senior vice-president of Ottawa-based technology firm Pythian. "Data localization seems not to be negotiated as aggressively as agriculture or auto," said Millar. "Until Canada gets a national strategy together, we should keep it out of NAFTA."
Morgan Elliot, vice-president of Mississauga-based SOTI Inc., said data "is the new gold" of the 21st century economy and giving up access to it in NAFTA could have "catastrophic" consequences for the competitiveness of Canadian companies in the future. "We worry that might be something that could be given up in terms of supporting legacy industries like autos," said Elliot. "The U.S. is playing the long-term game and I just worry that 10 years down the road we go, 'whoops that was more important than we thought."' ….The Canadian Council of Innovators, a group representing small- and medium-sized companies, urged the government prior to the latest round of talks to resist the U.S. proposals, citing concerns over the Patriot Act and "less stringent" restrictions on access to data for U.S. companies.
"Allowing our data to reside across the border will grant the U.S. a significant economic advantage, as they will be able to access and use Canadian data in ways Canadian companies cannot," it said in a letter

to Steve Verheul, Canada's lead negotiator. "This data could be used to identify trends to guide the investment, product development, commercialization and marketing initiatives, creating an un-level playing field."

Former Equifax CEO Details Security Vulnerability; Number of Canadians Affected Slashed

https://beta.theglobeandmail.com/report-on-business/international-business/us-business/equifax-says-cyber-attack-may-have-hit-25-million-more-us-consumers/article36464010/

[Oct.2] Equifax Inc was alerted in March to the software security vulnerability that led to hackers obtaining personal information of more than 140 million Americans but took months to patch it, its former CEO said in testimony to be delivered to Congress on Tuesday. "It appears that the breach occurred because of both human error and technology failures," former CEO Richard Smith said in written testimony released on Monday by the Energy and Commerce Committee. Separately, Equifax said late Monday that an outside review determined about 2.5 million additional U.S. consumers were potentially impacted, for a revised total of 145.5 million. **The company said the review also found that just 8,000 Canadian citizens were impacted, rather than up to 100,000 Canadians, as previously announced. Equifax was alerted to the breach by the U.S. Homeland Security Department on March 9, Smith said in the testimony, but it was not patched.** On March 15, Equifax's information security department ran scans that should have identified any systems that were vulnerable to the software issue but did not, the testimony said. As a result, "the vulnerability remained in an Equifax web application much longer than it should have," Smith said. "It was this unpatched vulnerability that allowed hackers to access personal identifying information."

In his testimony, Smith said it appears the first date hackers accessed sensitive information may have been on May 13. He said "between May 13 and July 30, there is evidence to suggest that the attacker(s) continued to access sensitive information." Smith said security personnel noticed suspicious activity on July 29 and disabled the web application on July 30, ending the hacking. He said he was alerted the following day, but was not aware of the scope of the stolen data. On Aug. 2, the company alerted the FBI and retained a law firm and consulting firm to provide advice. Smith notified the board's lead director on Aug. 22.

Smith, 57, said he was retiring last week and would forgo this year's bonus as **criticism mounts over the attack, which was not made public until Sept. 7 and has prompted investigations by multiple federal and state agencies, including a criminal probe by the U.S. Justice Department**. "I am here today to apologize to the American people myself," he said. Smith also apologized for the company's response after the data breach was made public, including the "rollout of our website and call centers, which in many cases added to the frustration of American consumers." He also said another well-known, independent expert consulting firm "has been retained to perform a top-to-bottom assessment of the company's information security systems." Smith will testify at three separate congressional hearings this week.

Phone Scammers Spoofing Numbers to Fool People into Thinking their Loved Ones are at Risk

https://globalnews.ca/news/3773151/phone-spoofing-scam/

It's not something she's proud of, but Virginia Jamil of Mississauga says it's important to tell people that she almost gave $3,000 to a phone scammer. She said the scammer convinced her that her daughter was in serious legal trouble. "He is evil, he is the devil," Jamil said, with tears welling in her eyes. "He needs to be caught." Jamil's 22-year-old daughter Alexis Jamil goes to school in Windsor, so most of the family's contact with her is over the phone. **When Virginia's phone rang Friday morning, she thought it was a routine call from her daughter.** "So I said, 'Hi Alexis, how are you?' The call took a very sour turn from there.

"They said, 'This is not Alexis.' I said, 'Who are you?' He said, 'we have Alexis.' I said, 'Where's my daughter? She's okay?' and he said, 'Well, she got arrested. We're from immigration and the police, we're holding your daughter,'" Virginia recalled. "I said, 'Let me talk to my daughter.' He said, 'You can't talk to your daughter.'"

The scammer on the other end, who Virginia said sounded very official and authoritative, told her she had to go to the bank and send $3,000 to free Alexis or they would potentially lock her up for 25 years. She said they also convinced her they were tracking her phone and could see her every

move to make sure she didn't go astray. Virginia said she's not the most tech- or law-savvy person. Even though her daughter was born and raised in Canada, which would rule out any immigration concerns, given where she goes to school she thought perhaps she ran into trouble while crossing the U.S. border nearby. "Sometimes she can go across to visit friends or… to go shopping, and that's why I was believing it," Virginia said.

With the phone call still connected, Virginia rushed out of the house and got into her car, at first driving aimlessly, unsure of what to do. Finally, she said **she made the decision to drive to the local Peel Regional Police station flagging two police officers and discreetly explaining the situation the man on the other end of the phone was putting her through**. That's when an officer took her phone and spoke directly to the fraudster. "I heard the police officer say, 'Who are you?' And [the man on the phone] said he's from the immigration police office, and [the police officer] said, 'Well, give me your badge number.'" Virginia said that was enough to scare the fraudster into hanging up. She said it's left her with lasting trauma. She says she feels a sense of panic every time the phone rings, especially when her daughter's number comes up on the call display. "It's going to take a long time to clear it out from my mind. Every time now my kids call me I'm like, 'Are you sure this is my son or my daughter?'"

It may seem like a new type of scam, but both law enforcement and cybersecurity experts say it happens more often than we hear about. Just a couple weeks ago Global News received a report from a woman in York Region, who did not want to be interviewed on the record, of an incident in which she claims she received a call from her husband's cell number. When she answered, she said the person on the other end claimed to be the police and told her they arrested her husband, whom they mentioned by name. The "officer" wanted to meet her at a bank, where he would have her take out money to pay for her husband's release. Luckily she had a hunch it was fake and didn't comply. She hung up on the scammer and called her husband who assured her he was fine.

"It resembles a version of an emergency scam that are documented on a daily basis," Peel Regional Police crime prevention services Const. Heather Cannon said. "Caller ID spoofing has been on our radar for many years."

Police advise anyone who feels they've been victimized by a phone fraudster to report it to the Canadian Anti-Fraud Centre and to lessen your chances of being a victim by not giving out personal information or passwords over the phone.

Those tips may seem like common sense, but in the heat of the moment with the information fraudsters can sometimes have at their fingertips, that call can seem all too real. "In most cases, you see these things (names, phone numbers, schools, locations, etc.) just posted publicly," Sycomp global security manager Kellman Meghu said. "It's really the information we share daily on social media." It's possible the person who called Virginia Friday might have researched her daughter's social media accounts first to build a convincing profile.

Once they have the information they need, Meghu said it's not hard for anyone with a little know-how to use software that lets them mimic someone else's phone number. "**Validate the person, not the phone number**," he urged. "For example, you get the phone call from someone saying, 'I'm so and so from your (mobile) carrier. I'd like to ask you a few questions.' Say, 'Great, what's your switchboard number? I want to call you back. I want a piece of information that I can verify to validate.'"

Looking back now, Virginia admits feeling a little foolish for almost falling for the scam. But she said she's telling her story to make others aware so they don't learn a hard lesson the way she did. "Do not believe it, go straight to the police and let police deal (with it)," she said.

[Note: Scammers can spoof (falsify) caller ID numbers, email addresses and URLs. Always be on alert, and listen to your intuition. Every month is cyber security awareness month – October just brings everyone's attention to this important issue!]

'Can You Hear Me?': Don't Say 'Yes' in New Telephone Scam

https://globalnews.ca/news/3221328/can-you-hear-me-dont-say-yes-in-new-telephone-scam/

Telemarketing calls are annoying enough, but now authorities are warning consumers about the risk of having their words on the phone used against them. It's called the 'Can you hear me' scam and reports in the U.S. suggest it's growing in popularity as fraudsters use it to try to get your money. "He said, 'This is Tony Moore, can you hear me clearly?'" Gail Worth, a homeowner who got one of the calls, said. She immediately hung up, but **had she said, 'Yes,' her answer might have been edited and used to prove she had willingly subscribed to a service contract or to buy an unwanted product**. Telemarketing

organizations typically call back consumers for verification calls and rely on those to ensure the consumer pays.
“Keep in mind, a scammer may already have gotten their hands on some of your personal information, such as credit card numbers, which they can use in tandem with your recorded affirmation to push through charges,” warned the Better Business Bureau of Southfield, Mich. It recently issued a warning to businesses and consumers. In some cases, the calls may be placed by a live person. But frequently, the calls are automated. “We have seen these robocalls get more sophisticated and even mimic things like background noise to convince you, as the recipient of the phone call, that it is a real person,” Ryan Kalember, senior vice president with the California cyber-security consulting company Proofpoint, said. “If you answer, ‘Yes,’ there’s a possibility that the scam artist behind the phone call has recorded you and will use your agreement to sign you up for a product or service and then demand payment. If you refuse, the caller may produce your recorded ‘yes’ response to confirm your purchase agreement,” the BBB cautioned. The U.S. Federal Trade Commission warns people to never provide personal information over the telephone and to hang up if they answer a pre-recorded sales call.
So far, there are no reports any Canadians have been defrauded as a result of the scam. [It’s just a matter of time before reports are received….]

'Terrified' 60-Year-Old Woman Told to Pay Up for Illegally Downloading Porn

http://www.cbc.ca/news/business/copyright-infringement-notice-government-piracy-porn-1.4313769
Debra is worried sick after receiving two copyright-infringement notices. An anti-piracy company has informed the 60-year-old that her internet account was used to illegally download pornography, and that she could wind up in court if she doesn't pay a settlement fee. "I've never done porno downloads in my life," says Debra, who lives in Ontario and has asked CBC News to withhold her last name. "I'm terrified. I'm worried someone's going to come after me, I'm going to have a giant lawsuit on my hands."
"Threatening" copyright-infringement notices asking for settlement fees are creating "consumer anxiety" and "could lead to abuses," says an internal 2016 federal government report. It also states that such notices aren't in line with the government's piracy notice program, which is meant to be educational, not punitive. However, almost a year after the report was written, the threatening notices continue. "The inaction is really difficult to understand," says Michael Geist, a University of Ottawa professor and internet law expert. He obtained the government report through an access to information request. **"We've got thousands of Canadians who are being abused through these notices."**
In 2015, the government started requiring that all internet providers forward copyright-infringement notices to customers suspected of illegally downloading content like TV shows and movies. Some anti-piracy companies, working on behalf of production studios, have added to the notices a demand for a settlement fee. It typically amounts to hundreds of dollars, and recipients are told they could face legal action and bigger fines if they don't pay up. The thing is, those companies don't know the suspect's actual identity, only the IP address linked to the illegal download. **Also, no one is obligated to pay a settlement fee. The government and internet providers have tried to spread that message, but some people are still unsure of their rights.**

Every Single Yahoo Account was Hacked - 3 Billion in All

http://money.cnn.com/2017/10/03/technology/business/yahoo-breach-3-billion-accounts/index.html
Sitting down? An epic and historic data breach at Yahoo in August 2013 affected every single customer account that existed at the time, Yahoo parent company Verizon said on Tuesday. [This news just arrived!] That's three billion accounts, including email, Tumblr, Fantasy and Flickr - **or three times as many as the company initially reported in 2016**. Names, email addresses and passwords, but not financial information, were breached, Yahoo said last year.
The new disclosure comes four months after Verizon acquired Yahoo's core internet assets for $4.48 billion. Yahoo is part of Verizon's digital media company, which is called Oath. Verizon revised the number of breached accounts to three billion after receiving new information. "The company recently obtained new intelligence and now believes, following an investigation with the assistance of outside forensic experts, that all Yahoo user accounts were affected by the August 2013 theft," Verizon said in a statement. Verizon would not provide any information about who the outside forensics experts are.
Yahoo will send emails to the additional affected accounts. Following the hacking revelations last year, Yahoo required password changes and invalidated unencrypted security questions to protect user information.

Mattel Gadget Listens to Babies, Setting Off Privacy Alarms

https://www.bloomberg.com/news/articles/2017-09-29/mattel-nursery-gadget-listens-to-babies-sets-off-privacy-alarms

Toymaker Mattel Inc. has announced plans to sell a nursery gadget that will listen to infants and watch over them, record their sleep patterns, and even play a lullaby should they awaken. Put another way: It eavesdrops on kids. Skeptics are asking if the device, similar to Amazon[dot]com's Echo with its Alexa voice assistant, will violate children's privacy and deepen a trend of surrendering intimate human connections to technology that talks and listens.

"**The kid tech industry sees kids' bedrooms as an economic bonanza**," said Jeff Chester, executive director of the Center for Digital Democracy, a Washington-based policy group that advocates for privacy protections. "They can get all kinds of profile information - the kid likes to eat this kind of food, the kid likes to listen to this kind of music, and we'll have this kind of information that we can share with partners and advertisers." The toymaker announced Aristotle in January as a "connected kids room platform." The device includes a speaker, camera and lights. It's powered by processors from Qualcomm Inc., and it uses programming from Microsoft Corp. to collect crib-side data and respond to a baby's needs. Aristotle can be programmed to launch into a lullaby, emit white noise, or turn on a night light to soothe a waking baby back to sleep. The monitor sends data on nap times and diaper changes to a corresponding smartphone app and, with permission, uploads it to the cloud.

The device can help purchase diapers, reinforce good manners in kids (by requiring the word "please" in voice commands) and even help kids learn a foreign language, the company said in a press release. Aristotle was to be introduced at retail in the summer with a recommended price of $299, according to Mattel's January news release. The product didn't turn up in a search of Mattel's shopping website on Thursday and the company hasn't said when it will be available or if it's been delayed. Alex Clark, a spokesman for Mattel, said in an email the company is "committed to ensuring every product we make meets or exceeds all applicable laws and regulations, including connected products intended for children's use." Aristotle wasn't designed to store or record audio or video, Clark said. No third parties will have access to any personally-identifiable information, and any data shared is entirely anonymous and fully encrypted, he said.

Listening Machines. The trend toward talking, listening machines is accelerating. Amazon, girding for competition from Apple Inc. and Google in the race to equip homes with smart devices, this week unveiled a slew of consumer gadgets including an Alexa-powered digital-home hub and a smaller and cheaper Echo speaker. Mattel is investing in internet-connected toys under a new leader recruited from Google. "Alexa and Echo have prepared us to say this is OK - to see something that's actually quite shocking as OK," Sherry Turkle, a professor at the Massachusetts Institute of Technology, said in an interview. She called Aristotle's lullaby capability "exactly the wrong thing for a computer to be doing," because the machine can't provide the comfort a human would.

In Congress, two lawmakers in a letter Thursday asked Mattel for details on how Aristotle will gather and store information. **"It appears that never before has a device had the capability to so intimately look into the life of a child,"** Senator Ed Markey, a Massachusetts Democrat, and Representative Joe Barton, a Texas Republican, said in the letter. "Consumers should know how this product will work, and what measures Mattel will take to protect families' privacy and secure their data," the lawmakers wrote. **Their questions included whether Aristotle will always be on to record children, and how Mattel will store and protect the information.** Mattel is "carefully reviewing" the letter, said Clark, the company spokesman.

The El Segundo, California-based toymaker in its announcement of the product said it paid "special attention" to federal law that requires websites and apps targeted at children to gain parental consent to collect and use children's personal information. But Chester, with the Center for Digital Democracy, said **the law doesn't protect children once parents give permission**. Mattel Chief Executive Officer Margo Georgiadis, hired from Alphabet Inc.'s Google early this year, has laid out a vision for the 72-year-old company that **puts more emphasis on internet-connected devices over traditional toys**.

This mission has taken on new urgency as interest appears to be waning in once-powerful brands such as Thomas and American Girl. Shares have dropped by more than 40 percent this year. But electronics come with implications far beyond selling wooden train sets or dress-up dolls. "A young child's bedroom should not be a place for corporate surveillance and data-gathering," said Josh Golin, executive director of the Campaign for a Commercial-Free Childhood policy group.

U.S. Cyber Command Launched DDoS Attack Against North Korea: Report

http://www.securityweek.com/us-cyber-command-launched-ddos-attack-against-north-korea-report

The United States Cyber Command has reportedly been engaged in offensive activity, namely a DDoS attack, against North Korea's military spy agency, the Reconnaissance General Bureau (RGB). The attack is thought to have commenced on September 22, and continued until September 30. The attack occurred just five weeks after President Trump elevated U.S. Cyber Command to a Unified Combatant Command. At the time, Trump said, "The elevation of United States Cyber Command demonstrates our increased resolve against cyberspace threats and will help reassure our allies and partners and deter our adversaries. Through United States Cyber Command, we will tackle our cyberspace challenges in coordination with like-minded allies and partners as we strive to respond rapidly to evolving cyberspace security threats and opportunities globally."

The few details currently available on this DDoS attack come from a Washington Post report published Saturday. **The report says that the Reconnaissance General Bureau was targeted, "by barraging their computer servers with traffic that choked off Internet access." The effects were temporary and non-destructive."** Nonetheless, some North Korean hackers griped that lack of access to the Internet was interfering with their work, according to another [anonymous] U.S. official." The action seems to be partly in response to North Korean cyberattacks, and partly an aspect of a wide-ranging diplomatic offensive led by Secretary of State Rex Tillerson, who was in Beijing on Saturday. "What I can tell you," said a senior administration official to the Washington Post, "is that North Korea has itself been guilty of cyberattacks, and we are going to take appropriate measures to defend our networks and systems."

That this cyberattack was non-destructive and temporary suggests it could be considered more as a warning than a punishment. It is Cyber Command telling North Korea that it has its range and is capable of much stronger action. By being non-destructive it is probably hoped that it won't provoke kinetic retaliation; although it is quite likely to provoke cyber retaliation from North Korean hacking groups.

In July 2017, researchers from Recorded Future monitored internet traffic from North Korea. One of its conclusions was that "most state-sponsored activity is perpetrated from abroad." Recorded Future suggested that North Korean malicious activity most like originates from countries such as India, Malaysia, New Zealand, Nepal, Kenya, Mozambique, and Indonesia. Under these circumstances, it is unlikely that DDoSing the homeland would have much effect on the actual hackers; although it would disrupt coordinating control from the RGB.

"DDoSing the Reconnaissance General Bureau might not affect the hackers outside of North Korea directly," F-Secure's security adviser Sean Sullivan told *SecurityWeek*, "but it could possibly hamper communications, forcing them to use other (potentially monitored?) channels." His colleague, Tom Van de Wiele, agreed and added, "Or as an extra bonus, to see what procedures they would go for versus what kind of panicky moves the organization makes, that [Cyber Command] could later abuse, monitor or exploit." The suggestion here is that it wasn't just a warning shot to North Korea, but an elaborate cyber reconnaissance project.

One thing not yet known is whether China had any involvement or collusion in the action. Since Tillerson was in Beijing at the time, and since all internet traffic into and out of North Korea is through China via a China Unicom link operating since 2010, it is a tempting thought. Either way, however, this potential choke point against North Korean cyber access is in the process of weakening.

Russia, on Sunday, started providing a second internet route for North Korea. The link started showing on Dyn Research peer observance tables at around 0900 UTC on October 1. Connectivity was clearly unstable for about three hours, but stabilized after that. **In effect, it went live with a stable link between Russia and North Korea shortly after the U.S. Cyber Command action finished.** The route is supplied by Russian telecommunications company TransTeleCom. TransTeleCom is a subsidiary of the Russian railway operator, and lays its fiber optic lines alongside the railway tracks. A map on the company website shows a cable running to the North Korean border. It is assumed that this cable now connects Russia and North Korea via the Friendship Bridge across the Tumen River - the only point at which the two countries connect.

The cabling has apparently been in place under an agreement between TransTeleCom and Korea Posts and Telecommunications Corp since 2009. The timing coincidence of it becoming live now could imply that opening the link between the two countries is in response to the U.S. Cyber Command attack. Alternatively, it could lend weight to the F-Secure hypothesis. If Cyber Command was aware that this would be happening, the DDoS attack could have been an attempt to provoke the Reconnaissance

General Bureau into revealing channels to its overseas hacking groups prior to the Russian link giving North Korea additional communications options.

Report: Thousands of Macs and PCs May Be Vulnerable to a Sophisticated Kind of Computer Attack

https://www.washingtonpost.com/news/the-switch/wp/2017/09/29/report-thousands-of-macs-and-pcs-may-be-vulnerable-to-a-sophisticated-kind-of-computer-attack/

An analysis of more than 70,000 Mac computers being used in businesses and organizations has revealed a firmware vulnerability that could be exploited by a determined, well-resourced attacker such as a foreign government, according to security researchers. Thousands of computers, if not more, are potentially in danger. While Apple devices were the focus of the study released Friday by the firm Duo Security, experts at the company said that Windows-based machines are even more likely to be at risk, because of the range of manufacturers involved in building those types of PCs.

The flaw outlined by Duo Security researchers Rich Smith and Pepijn Bruienne **concerns Apple's Extensible Firmware Interface, or EFI, which helps computers boot up and run the main operating system**. Because all subsequent hardware and software operations are dependent on the EFI, allowing hijackers to gain control of it could prove disastrous. The investigation that led to the discovery began when Smith and Pepijn looked at how many Macs were running outdated firmware. Macs are supposed to update their firmware automatically to the latest versions whenever a user updates the main operating system, insulating them from firmware attacks. But Duo Security's study found that 4.2 percent of surveyed machines were running an outdated version of the firmware. In other words, some computers appear not to be updating their firmware when they're supposed to.

As a result, some machines may be running an up-to-date operating system but problematic firmware. The researchers described the problem as "software secure, firmware insecure." The firmware discrepancies appear to affect different models of Mac computers to varying degrees. As many as 16 models have never received any firmware updates, the report showed. Certain iMacs from late 2015 were the worst offenders, with 43 percent of those systems running an outdated version of firmware. "The number of systems that weren't reflective of the expected good state was actually quite surprising to us," Smith said. "We went back and checked our data several times to make sure we weren't being led to the wrong conclusions." In Duo Security's sample alone - which drew from sectors as diverse as higher education, technology and international groups - more than 3,000 machines were affected by the flaw. All those vulnerable devices could become juicy targets for state-sponsored hackers engaging in corporate or government espionage. Expand that to all enterprises worldwide, and you begin to get an idea of the potential scale of the problem.

Most home users don't have to worry about this type of attack, Smith said, because they aren't likely to become targets. Instead, the most vulnerable may be government agencies, industrial groups or corporations - those with a great deal more to lose and who might be deliberately targeted by foreign actors. To help businesses and organizations check the health of their systems, Duo Security said it's providing several tools for IT administrators to use.

The cybersecurity firm contacted Apple in June to discuss the findings, and the tech giant not only accepted the results and methodology, Smith said, but has been working closely with the security firm to understand the problem. **So far, neither company has been able to figure out why some computers are refusing to apply the updates**.

Apple didn't respond to a request for comment from The Washington Post, but some of its employees have been active about addressing firmware vulnerabilities. A series of (now-deleted) tweets this week from an Apple engineer highlighted **a new feature in the latest version of macOS, High Sierra, that runs in the background and checks every week to see whether a Mac is using outdated firmware**. If the check passes, users won't see any difference. If it fails, users will be prompted to notify Apple.

"The level of security they're applying to 10.13 [macOS High Sierra] is definitely a step forward for EFI security overall," Smith said. "It might not address everything we've found in the paper - certainly not the legacy and historical problems we've found - but it's going in the right direction, which is great to see."

SEC Says Personal Information Compromised in 2016 Hack

http://money.cnn.com/2017/10/02/technology/business/sec-hack-2016-data-stolen/index.html

Hackers compromised the personal information of at least two people in a recently disclosed breach of the Securities and Exchange Commission's corporate filing system. In a statement on

Monday, SEC Chairman Jay Clayton said "the names, dates of birth and Social Security numbers of two individuals" were exposed. The agency is notifying them and will provide identity theft protection services. The SEC added it is investigating whether other personal information has been compromised. Although the SEC didn't say whose personal information was breached, it was probably not a member of the general public. Most of the people who file information about stock sales in the system are top executives and directors of public companies.

Last month, the SEC disclosed a 2016 hack of its Edgar filing system, a database of information all publicly traded companies have to file with federal regulators, like company earnings, mergers and acquisitions, and executives' share dealings. Hackers accessed the information through a software flaw. Previously, the agency said no personal information had been compromised. It said the hackers may have made money using the corporate information they stole. "The 2016 intrusion and its ramifications concern me deeply," Clayton said in a statement. "I am focused on getting to the bottom of the matter and, importantly, lifting our cybersecurity efforts moving forward." Those efforts include an investigation into any illegal trading off the hack, a possible upgrade of the corporate filing system and a review of all agency systems. Clayton has authorized hiring more staff and consultants to strengthen cybersecurity.

The List Grows: Whole Foods Hit by Hackers [and Sonic, and Wendy's and Chipotle..]

http://money.cnn.com/2017/09/28/technology/business/whole-foods-data-breach/index.html

Another day, another cybersecurity breach. Whole Foods Market - which was recently acquired by tech giant Amazon - said Thursday that **hackers were able to gain access to credit card information for customers who made purchases at some of its in-store taprooms and restaurants**. The company did not disclose details about the locations that were targeted or how many customers might have been effected. The tap rooms and restaurants use different payment systems than Whole Foods check-out counters, the company said. "Amazon.com systems do not connect to these systems," the company clarified in a press release. Amazon did not return a request for comment.

"When Whole Foods Market learned of this, the company launched an investigation, obtained the help of a leading cyber security forensics firm, contacted law enforcement, and is taking appropriate measures to address the issue," the company said. Whole Foods says it plans to provide updates throughout the investigation. **Hackers targeted "point of sale systems" - or the machines where customers swipe or insert their cards - in order to steal the data**, according to the press release.

Sound familiar? The news comes just one day after reports that **Sonic, the drive-in restaurant chain, suffered a strikingly similar problem**. KrebsOnSecurity, a notable cybersecurity blog, had identified a potential breach at some Sonic restaurants that was likely executed the same way Whole Foods says it was hacked - remotely via point of sale systems. Krebs estimates millions of credit and debit card numbers could have been stolen in that hack.

Two other restaurants - Wendy's and Chipotle - suffered breaches earlier this year for similar reasons. Wendy's said in July that point of sale systems at more than 1,000 of its U.S. restaurants were targeted by hackers, compromising an unknown number of credit and debit cards. Chipotle was hit in March and April. The company said in May that "most, but not all" of its restaurants may have been involved in a credit-card theft scheme carried out by hackers who installed malware on cash registers.

Europol Warns Ransomware has Taken Cybercrime 'To Another Level'

https://www.tripwire.com/state-of-security/security-data-protection/europol-ransomware-warning/

Europol, the European Union's police agency, has warned of the significantly rising threat posed by ransomware. As *Associated Press* reports, delegates at an international conference were told by Europol Executive Director Rob Wainwright that ransomware had taken the cybercrime threat to "another level." An 80-page report published by the agency highlighted the growing threat posed by ransomware attacks: "Ransomware attacks have eclipsed most other global cybercrime threats, with the first half of 2017 witnessing ransomware attacks on a scale previously unseen **following the emergence of self-propagating 'ransomworms'**, as observed in the WannaCry and Petya/NotPetya cases. Moreover, while information-stealing malware such as banking Trojans remain a key threat, they often have a limited target profile." "Ransomware has widened the range of potential malware victims, impacting victims indiscriminately across multiple industries in both the private and public sectors, and highlighting how connectivity and poor digital hygiene and security practices can allow such a threat to quickly spread and expand the attack vector."

Europol is right to highlight the significant impact that ransomware is having on business and home computers alike. As we have previously discussed, multinationals like household goods manufacturer Reckitt Benckiser, and the Maersk shipping conglomerate have reported that the attacks have caused $100 million and $300 million in lost revenue respectively. Meanwhile the impact felt by the WannaCry ransomware earlier in the year on the UK's National Health Service and other large organisations is well-documented. It's no wonder that Europol is calling for more resources to be put in place around the world to target cybercrime gangs, and for greater co-ordination between law enforcement agencies.

As *The Register* reports, a similar message of the rise of ransomware has come from the UK's Metropolitan Police's cybercrime-fighting division speaking at the Cyber Security in Healthcare event in London: "Three years ago [the main threat] was the inception of DDoS attacks or the criminal damage of computers; two years ago it was data breaches like TalkTalk, this year it has been the use of ransomware attacks on individuals and corporate systems. Next year it will be more of the same."

We can talk long and hard about the need for companies and home computer users to have better protection in place, to keep a strict regime of patching against vulnerabilities, and to make sure that a secure backup regime is in place. But Europol argues that we also need to tackle the rampant rise of ransomware from the other end of the problem. That means giving law enforcement agencies more resources to investigate organised multinational cybercrime gangs in order to bring the perpetrators to justice.

Moscow Deploys Facial Recognition to Spy on Citizens in Streets

https://www.bloomberg.com/news/articles/2017-09-28/moscow-deploys-facial-recognition-to-spy-on-citizens-in-streets

Moscow is adding facial-recognition technology to its network of 170,000 surveillance cameras across the city in a move to identify criminals and boost security. Since 2012, CCTV recordings have been held for five days after they're captured, with about 20 million hours of video stored at any one time. "We soon found it impossible to process such volumes of data by police officers alone," said Artem Ermolaev, head of the department of information technology in Moscow. "We needed an artificial intelligence to help find what we are looking for."

Moscow says the city's centralized surveillance network is the world's largest of its kind. The U.K. is one of the most notorious for its use of CCTV cameras but precise figures are difficult to obtain. However, a 2013 report by the British Security Industry Association estimated there were as many as 70,000 cameras operated by the government across the nation.

Moscow's facial-recognition technology was designed by Russian start-up N-Tech.Lab Ltd. The system cross-references a digital fingerprint of images from the Interior Ministry's database against those captured by cameras at entrances to apartment buildings, Ermolaev said. A two-month trial of the system earlier this year resulted in 6 criminals being detained from a federal "wanted" list, he said.

N-Tech.Lab's accuracy has been recognized by the U.S. Department of Commerce and the University of Washington. The Moscow-based company released a mobile app called FindFace last year that became a big hit in Russia. Consumers would take a photograph of strangers in public spaces and the tool would identify those in the picture by matching their faces to profiles on Russia's largest social network, VKontakte, with a reported 70 percent accuracy rate.

Facial recognition technology has been creeping into the consumer market for a number of years, with increasing accuracy and acceptance by users. Microsoft Corp.'s Windows 10 operating system can be unlocked when an authorized user sits in front of a computer's webcam and Samsung Electronics Co. includes a similar technology in its smartphones. More recently, Apple Inc. announced its flagship iPhone X would dispense with a fingerprint security sensor in favor of facial recognition.

CCTV Cost. Ermolaev said the Moscow government is already spending about 5 billion rubles ($86 million) a year to maintain its video surveillance system. Deploying facial-recognition to all of 170,000 cameras would have tripled these costs, he said, so the technology will be applied selectively within districts where it's currently most needed. Such systems are legal in Russia, says Mikhail Zyuzin, an IT expert at the Moscow-based Academy of Information Systems. It causes concerns about personal privacy, however. "If the system is hacked by third parties, they could potentially get access to information on where you live, where you go and what routes you take," he said. Ermolaev says the data is kept in a closed system accessible only to a limited number of users. Additionally, the software will only compare images from CCTV cameras to information already in police databases.

Google to End 'First Click Free' Policy on Media Sites

http://www.cbc.ca/news/business/google-publishers-free-clicks-1.4316254

Google will try to help newspapers and other publishers boost subscriptions by ending a decade-old policy that required them to provide a limited amount of free content before users of the world's biggest search engine could be asked to pay for it. Google's "first click free" policy was loathed by publishers and media because while the stories, videos and images appearing on Google have been free for its users, it is expensive to produce.

Publishers had been required to provide at least three free items under the search engine's previous policy. Publishers will now be allowed to decide how many, if any, free articles they want to offer readers before charging a fee, Richard Gingras, vice-president of news at Google Inc., wrote Monday in a company blog post. For people who intentionally sought to skirt paywalls, the policy allowed readers to type a headline into Google and get free access to a story without having it count against a monthly free article limit, said Kinsey Wilson, an adviser to New York Times CEO Mark Thompson.

In months of testing with Google, reducing those free clicks from three to zero "generally improved" conversion to subscriptions, Wilson said. But he added the Times continues to assess whether to actually reduce the number of free clicks now that it can. He said it was "not simply a mechanical decision" because the Times' mission was in part to make sure its news was available to a wide audience and to set the news agenda.

Among the changes announced by Google: (1) Click for free is over. Publishers decide what and if they want to provide for free. (2) Google will produce a suite of products and services aimed at broadening the audience for publishers in an attempt to drive subscriptions and revenue. (3) Streamline payment methods so that readers can tailor their own experience. That would include access to a publication's digital content with one click. That content could then be accessed anywhere - whether it's on a publisher's website or mobile app, or on Google Newsstand, Google Search or Google News.

Newspapers and magazines have shut down in droves or have been forced to shrink operations drastically worldwide because of the influx of stories, images and video jettisoned across the internet, largely at no charge. Technological changes have fractured the advertising market and constrained revenues for almost all established media. Much of the content, created and paid for by media companies, travels through Google's Chrome, which captured nearly 60 per cent of all searches in September, according to NetMarketShare. [see article for discussion on this story]

And Now, This:

Leave It to Sex Toy Flaws to Show the Sad State of Bluetooth LE Implementations

https://www.bleepingcomputer.com/news/security/leave-it-to-sex-toy-flaws-to-show-the-sad-state-of-bluetooth-le-implementations/

[Okay readers – this is a BC government-produced news digest, however, the Internet of Things includes the most intimate of "things". **This Bluetooth issue needs to be understood**, and consumers need to be made aware of security threats and risks. Manufacturers don't care, but we do!]

A security firm's investigation of modern smart sex toys has revealed just how exposed most IoT devices running BLE (Bluetooth Low Energy) really are. **The issue at the heart of this problem is the use of Bluetooth LE for most of today's smart sex toys and a vast majority of other IoT devices.** Vendors choose Bluetooth LE over classic Bluetooth because of the LE part of BLE. Smart devices running over BLE consume less battery and last longer. The problem is that **BLE has fewer security features** compared to classic Bluetooth, and as Alex Lomas, a security researcher at Pen Test Partners, points out based on his expertise, **"when [BLE security] is implemented it's often done poorly."** This became evidently clear during one of Pen Test Partners' (PTP) most recent investigations.

PTP, a well-known UK-based company specialized in security audits of smart devices, has discovered almost the same BLE-related security flaws in several smart toys, such as …[see article for product names]. Experts say the process that allows these smart sex toys to pair with a local smartphone via BLE is wide open to anyone sitting near the devices. "Note that there is no PIN or password protection, or the PIN is static and generic (0000 / 1234 etc) on these devices," Lomas said. "In fact, we've found this issue in every Bluetooth adult toy we've looked at!"

For example, when a user pairs a smart device, such as a smart home alarm, with a smartphone, the homeowner is asked to enter a PIN on the smart home alarm keypad. "The challenge is the lack of a UI to enter a classic Bluetooth pairing PIN," Lomas explains.

Smart sex toys are broadcasting their location. The other issue is that some of these devices have been so poorly designed that they have the same identifier which they broadcast to nearby users looking to pair up. ….Lomas says that an attacker could drive around a city with a powerful antenna and map out all sex toys ready to pair up…..

Issues present in other BLE devices. But the issues are not restricted to smart sex toys alone. For example, **Lomas says he found the same poor design choices in the deployment of BLE in smart hearing aids used by his father**. "These things cost £3500 and need to be programmed by an audiologist so not only could an attacker damage or deprive someone of their hearing, but it's going to cost them to get it fixed," the expert said.

Expert proposes mitigations. Fixing the issues Lomas found is a problem of teaching vendors about better security design choices. For example, Lomas proposes that for smart devices where you can't deploy a UI for entering pairing PINs, vendors at least implement a hold-down button to allow a pairing operation to take place. Another proposition is that IoT vendors tone down BLE signal strength, at least for some sensitive devices such as smart sex toys, so an attacker would need to be physically adjacent to the device in order to pair. Lomas also proposes that vendors use unique pairing PINs per device, which come at the small cost of placing a sticker on the device's box. To prevent triangulation and identification, Lomas also proposes that smart sex toys advertise their nearby presence by using fake names, disguising themselves as printers or other devices. **Better security and privacy protections are needed, especially since the upcoming version of the Bluetooth standard - version 4.2 - would allow more than one person to pair with a BLE device, meaning an attacker wouldn't even need to wait for the device owner to disconnect**.

Feel free to forward the Digest to others that might be interested.
Click Unsubscribe to stop receiving the Digest.

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