Security News Digest
September 12, 2017

Do you "live on your mobile device"? Then you should take the quiz:
September Living Mobile Quiz

Wednesday, September 13 is Programmer's Day - the 256th (hexadecimal 100th, or the 2^8th) day of each year. https://www.daysoftheyear.com/days/programmers-day/
Computers, technology and software makes the modern world go around – but for every piece of clever software, there's a programmer (and often teams of programmers) behind the scenes, solving problems with clever code, cloud security solutions, and intense development projects. Programmers' Day is celebrated on the 256th day of the year – chosen because this is the number of distinct values that can be represented with an eight-bit byte, and the highest power of two which is less than 365 (obviously!).

And Oops, missed it last week, but **Friday, September 8th was Star Trek Day!** – founded in 1966! https://www.daysoftheyear.com/days/star-trek-day/ Long ago, in the depths of the cold war, America had a prophet arrive. He spoke not of religious texts and damnation, but instead provided us with a vision of the future so hope-filled, so compelling, that it has indelibly marked the imaginations of human-kind ever since. Star Trek Day celebrates that vision, and the man who created it, Gene Roddenberry.

Equifax Hacked: Canadians Among Those Exposed by Credit Monitoring Company's Data Breach

http://globalnews.ca/news/3726259/equifax-data-breach-143-million-americans-hack/
Credit monitoring company Equifax has been hit by a high-tech heist that exposed sensitive information of about 143 million Americans, and an unknown number of Canadians. [The population of the U.S. was about 324 million as of Jan. 1, 2017, according to the U.S. Census Bureau, which means the Equifax incident affects a huge portion of the United States.] Now the unwitting victims have to worry about the threat of having their identities stolen.
The Atlanta-based company, one of three major U.S. credit bureaus, said Thursday that "criminals" exploited a U.S. website application vulnerability to access files between mid-May and July of this year. The theft obtained consumers' names, Social Security numbers, birth dates, addresses and, in some cases, driver's license numbers. The purloined data can be enough for crooks to hijack the identities of people whose credentials were stolen through no fault of their own, potentially wreaking havoc on their lives.
Equifax said its core credit-reporting databases don't appear to have been breached. "On a scale of one to 10, this is a 10 in terms of potential identity theft," said Gartner security analyst Avivah Litan. "Credit bureaus keep so much data about us that affects almost everything we do." Lenders rely on the information collected by the credit bureaus to help them decide whether to approve financing for homes, cars and credit cards. Credit checks are even sometimes done by employers when deciding whom to hire for a job.
Equifax discovered the hack July 29, but waited until Thursday to warn consumers. ..The company established a website, https://www.equifaxsecurity2017.com/ , where people can check to see if their personal information may have been stolen. Consumers can also call 866-447-7559 for more information. Experian is also offering free credit monitoring to all U.S. consumers for a year.
….Equifax's security lapse could be the largest theft involving Social Security numbers, one of the most common methods used to confirm a person's identity in the U.S. It eclipses a 2015 hack at health insurer Anthem Inc. that involved the Social Security numbers of about 80 million people. Any data breach threatens to tarnish a company's reputation, but it is especially mortifying for Equifax, whose entire business revolves around providing a clear financial profile of consumers that lenders and other businesses can trust. "This really undermines their credibility," Litan said. It also could undermine the

integrity of the information stockpiled by two other major credit bureaus, Experian and TransUnion, since they hold virtually all the data that Equifax does, Litan said.
….In addition to the personal information stolen in its breach, Equifax said the credit card numbers for about 209,000 U.S. consumers were also taken, as were "certain dispute documents" containing personal information for approximately 182,000 U.S. individuals. Equifax warned that hackers also may have some "limited personal information" about British and Canadian residents. The company doesn't believe that consumers from any other countries were affected.

Class Action Suits Filed Against Equifax for Data Breach, 'Bogus' Arbitration Clause Waived

http://globalnews.ca/news/3735982/class-action-equifax-arbitration-clause/

While Equifax is still reeling from one of "the most impactful" data breaches ever, it's also being attacked on a legal front. Last week, Equifax revealed that more that 143 million American's and an unknown number of Canadian's sensitive information (like Social insurance numbers or credit card numbers) might have been stolen in a security breach on July 29. At least 30 class action lawsuits have been filed against the credit reporting company in the U.S., and two have been filed in Canada.
Saskatchewan-based lawyer Tony Merchant of the Merchant Law Group said he **filed a lawsuit in B.C.** on Friday and in Quebec on Monday, and he plans to file another in Ontario Tuesday. He says Equifax unsafely stored the information all in one location - rather than on multiple file servers for greater protection. "It might not be the biggest, but it's the most impactful hack ever," Merchant said, explaining that the nature of the data made it so important.
Both the Office of the Privacy Commissioner of Canada and the New York States Attorney's office are investigating the breach. **If you think you've been affected**, the Financial Consumer Agency of Canada recommends contacting Equifax, and the other Canadian credit monitoring company TransUnion, and asking for them to place a fraud alert on your information. That way, if someone tries to apply for a mortgage, the companies will alert you first to make sure it is a legitimate transaction.
'Bogus' arbitration clause waived. Savvy social media users have shone a light on a clause Merchant called "bogus" and unfair. The arbitration clause, which is buried in the legalese of a contract, normally wouldn't allow for the customer to participate in a class action lawsuit. It has to do with the credit monitoring the credit report company offers - the ones specifically targeted at those who might have had their sensitive data accessed by hackers. After Equifax disclosed the security breach, it offered customers a chance to see if their data was part of the compromised information on its website. Once they checked, the company offered one year of credit monitoring free to see if their information was used fraudulently.
But in the fine print of that credit monitoring software contract, lay the arbitration clause. After outrage on social media and in the news, Equifax waived the clause, first by saying consumers could opt out if they chose, but eventually, officials took the clause out of the contract entirely. A request for comment from Global News was not returned, but officials told *the Washington Post* they had waived the clause. "To be as clear as possible, we will not apply any arbitration clause or class action waiver against consumers for claims related to the free products offered in response to the cybersecurity incident or for claims related to the cybersecurity incident itself," officials told *the Post.* Merchant said he will be advising those who are part of the class to contact Equifax to opt out.

Equifax Data Breach: Tips for Canadians Whose Info May Have Been Hacked

http://globalnews.ca/news/3727677/equifax-data-hack-canada/

Credit reporting giant Equifax has yet to reveal how many Canadians had their personal information hacked over the spring and summer when the company's database was breached. Equifax discovered the hack July 29 but waited until Thursday to warn consumers that criminals exploited a U.S. website application to access files between mid-May and July of this year. The breach exposed the information of an "unknown" number of people living in Canada and the United Kingdom. Hackers were able to get consumers' names, social insurance numbers, birth dates, addresses, credit card information and, in some cases, driver's license numbers. This information is enough for the thieves to hijack the identities of people whose credentials were stolen.
"There are 26 million people who have credit scores in Canada," financial literacy and credit score expert, Chantal Chapman said. "With the information that was taken, a person could fill out a mortgage application or buy a cellphone. It's pretty scary."

Have you been hacked? Equifax established a website where people can check to see if their personal information may have been stolen. Consumers can also call 1-866-447-7559 for more information. Equifax said it will send direct mail notices to consumers whose credit card numbers or dispute documents with personal identifying information were impacted.

What to do if your information has been hacked. If you do find your personal information may have been impacted, there are a few steps you can take to protect yourself from identity theft.

(1) Monitor your Equifax credit score. You should watch your credit score as soon as possible and keep an eye on it to make sure nothing suspicious is happening, Chapman said. There are a number of free credit monitoring services out there, like Mogo. If you monitor your score monthly and then see your credit rating drop, it's an indication something has happened, she added.

(2) Watch your credit inquiry. "Anytime someone checks credit it's a hit on your credit score," Chapman said. There can be a soft hit (when you check your own credit) and then there's a hard hit (applying for a credit card). You can order a credit inquiry through Equifax.

(3) Freeze your credit reports. You can freeze your Equifax account, consumer advocate and chairman of security firm CyberScout, told Marketwatch. This restricts access to your credit report, which helps prevent other credit card companies from accessing it to open up new accounts.

(4) If your SIN was stolen, file a police report. A social insurance number is the Holy Grail of identity theft, according to finance magazine, Kiplinger. You should file an identity theft police report and send a copy of it to Equifax.

(5) Check your bank and credit card statements. Keep a close eye on your credit statements for suspicious activity over the past several months. Report any suspicious charges and cancel your compromised card for a new one.

(6) Alert bank and strengthen your password. Let your bank, or any other company overseeing another financial account, know about the breach. You should also change your password with a two-factor authentication (password and confirmation via phone number).

How many Canadians? The breach exposed the information of an "unknown" number of people living in Canada. .."Equifax will work with U.K. and Canadian regulators to determine appropriate next steps," the credit monitoring company said in a statement.

Why did Equifax wait to tell the public? Equifax waited six weeks to disclose that sensitive information was hacked in a data breach. "Equifax discovered the unauthorized access on July 29 of this year and acted immediately to stop the intrusion," Equifax said in a statement. "The company promptly engaged a leading independent cybersecurity firm that has been conducting a comprehensive forensic review to determine the scope of the intrusion, including the specific data impacted. "Equifax also reported the criminal access to law enforcement and continues to work with authorities. While the company's investigation is substantially complete, it remains ongoing and is expected to be completed in the coming weeks." The Atlanta-based company declined to comment on that delay or anything else beyond its published statement.

Three Equifax executives sold shares worth a combined $1.8 million just a few days after the company discovered it had been hacked, according to documents filed with securities regulators. In a subsequent statement, Equifax said the three executives "had no knowledge that an intrusion had occurred at the time they sold their shares."

Equifax handles data on more than 820 million consumers and more than 91 million businesses worldwide and manages a database with employee information from more than 7,100 employers, according to its website.

When Do Canadian Spies Disclose the Software Flaws They Find? There's a Policy, But Few Details 

http://www.cbc.ca/news/technology/canada-cse-spies-zero-day-software-vulnerabilities-1.4276007

When a crippling ransomware attack wreaked havoc on computers around the world earlier this year, it did so with alarming, worm-like speed. It didn't take long for security researchers to find out why. The highly sophisticated code that was used to sneak silently into computers, largely undetected, had been stolen from the NSA. The incident thrust a long-simmering debate about the disclosure of previously undiscovered software flaws into the spotlight: how should government agencies decide which vulnerabilities to report, and which ones to keep secret for future use?

In the U.S., the policy governing this careful weighing of stakes is known as the Vulnerabilities Equities Process, or VEP. In Canada, spies have for the first time acknowledged that a similar process exists

here, too. "CSE (Canada's electronic spy service) has a rigorous process in place to review and assess software vulnerabilities," wrote Communications Security Establishment spokesperson Ryan Foreman in an email, in response to a list of questions about the handling of zero-day vulnerabilities sent by CBC News. "This longstanding assessment process is carried out by a panel of experts from across CSE." According to Foreman, the panel meets "regularly," though he declined to say how often, nor how many times they have met in recent years. CSE's policy is not public, and the agency declined to even give the policy's formal name, citing "operational specifics." "We would want the policy itself to be public and scrutinizable," says Brenda McPhail, privacy director for the Canadian Civil Liberties Association (CCLA). A copy of the U.S. government's own vulnerability handling policy was only obtained through a Freedom of Information Act lawsuit filed by the digital rights group Electronic Frontier Foundation in 2014, after the NSA declined to publicly release its policy.

The risk of 'stockpiling'. In the U.S., the VEP was created to help different government agencies weigh the risk of keeping newly discovered software vulnerabilities secret, so that they can be exploited by law enforcement or intelligence agencies to gather intelligence from computers and phones without detection. So-called zero-day vulnerabilities are considered especially serious because no patches have been developed to fix them, and software developers - be it Microsoft, Apple, Google, or others - don't know the flaws exist. As a result, some are worried that keeping the discovery of zero-day vulnerabilities secret unnecessarily puts users around the world at risk - especially if knowledge of the vulnerability is obtained or discovered by someone else first. That concern was realized in May when previously undisclosed software vulnerabilities discovered by the NSA were stolen, and later used to infect computers with a particularly nasty strain of ransomware called WannaCry.

Government of Canada Publishes Proposed "Breach of Security Safeguards Regulations"

http://www.jdsupra.com/legalnews/government-of-canada-publishes-proposed-27654/

On September 2, 2017, the Government of Canada published proposed "Breach of Security Safeguards Regulations". The proposed regulations relate to the provisions in Canada's *Personal Information Protection and Electronic Documents Act* ("*PIPEDA*"), which are not yet in force. The *PIPEDA* provisions will require an organization to notify affected individuals, and report to the Office of the Privacy Commissioner of Canada ("OPC"), as soon as feasible, regarding any data breach which poses a "real risk of significant harm" to any individual whose personal information was involved in the breach. The breach provisions in *PIPEDA* specify that such notification and reporting must be done in accordance with regulations passed pursuant to *PIPEDA.* Representations on the proposed regulations may be submitted up to October 2, 2017.

Failure to notify the OPC of a security breach, as required by the *PIPEDA* provisions yet to come into force, is an offence, punishable by a fine of up to $100,000. *PIPEDA* also contains a private right of action for affected individuals, which could result in damages being awarded by the Federal Court of Canada for failure to notify affected individuals. This private right of action also opens the door to potential class actions for an organization's failure to comply with the breach notification provisions in *PIPEDA*. The breach provisions in *PIPEDA* also require organizations to notify any other organization that may be able to mitigate harm to affected individuals, for example, service providers and law enforcement entities. In addition, organizations must maintain a record of any data breach and provide the record to the OPC upon request. [see article for more details]

Cybersecurity and Cloud are Top IT Concerns for Canadian Organizations

http://www.itworldcanada.com/article/cybersecurity-and-cloud-are-top-it-concerns-for-canadian-organizations/396338

Intrusion prevention and ransomware are key areas of focus for Canadian organizations, according to a new survey by CDW Canada, while at the same time they are following through with their cloud strategies. As security threats to data have become inherently persistent, survey respondents indicated they are keeping a close eye on their security practices and technologies, with 39 per cent citing intrusion prevention as a top priority, while 35 per cent cited ransomware protection.

Despite the omnipresent security threats, Canadian organizations are putting a great deal of effort into growing their cloud deployments with half of businesses surveyed indicating their cloud strategy for 2017 includes hybrid solutions and moving workloads over time. A small number (16 per cent) said they were planning to be a "cloud-first" organization going forward. Priorities in the data centre, meanwhile, include redundancy (29 per cent), expansion and scalability (27 per cent) and cost reduction (26 per cent).

Despite a move to the cloud, only 10 per cent of survey respondents said they would replace current legacy tools and applications with new technologies, while just over a quarter of respondents said they would continue to use current tools and applications. Nearly a third of Canadian organizations said their unified communications strategies include integration of new features or products into current tools and applications. Analytics and big data are also on the minds of Canadian organizations, with 28 per cent citing them as the emerging technologies that will have the most impact on their business, while 27 per cent cited the Internet of Things.

North Korea Is Dodging Sanctions With a Secret Bitcoin Stash

https://www.bloomberg.com/news/articles/2017-09-11/north-korea-hackers-step-up-bitcoin-attacks-amid-rising-tensions

North Korea appears to be stepping up efforts to secure bitcoin and other cryptocurrencies, which could be used to avoid trade restrictions including new sanctions approved by the United Nations Security Council. Hackers from Kim Jong Un's regime are increasing their attacks on cryptocurrency exchanges in South Korea and related sites, according to a new report from security researcher FireEye Inc. They also breached an English-language bitcoin news website and collected bitcoin ransom payments from global victims of the malware WannaCry, according to the researcher.

Kim's apparent interest in cryptocurrencies comes amid rising prices and popularity. The same factors that have driven their success - lack of state control and secretiveness - would make them useful fund-raising and money laundering tools for a man threatening to use nuclear weapons against the U.S. With tightening sanctions and usage of cryptocurrencies broadening, security experts say North Korea's embrace of digital cash will only increase.

"We definitely see sanctions being a big lever driving this sort of activity," said Luke McNamara, a researcher at FireEye and author of the new report. "They probably see it as a very low-cost solution to bring in hard cash." The 15-member Security Council on Monday approved sanctions aimed at punishing North Korea for its latest missile and nuclear tests. U.S. officials said the new measures would cut the country's textile exports by 90 percent, restricting its ability to get hard currency.

So far this year, FireEye has confirmed attacks on at least three South Korean exchanges, including one in May that was successful. Around the same time, local media reported that Seoul-based exchange Yapizon lost more than 3,800 bitcoins (worth about $15 million at current rates) due to theft, although FireEye said there are not clear indications of North Korean involvement. North Korea's telecommunications ministry didn't respond to an emailed request for comments. The country's diplomats and official media have denied the country played any role in cyberattacks, including the hacking of Sony Pictures Entertainment in 2014.

Russia-Linked Hackers Infiltrated U.S. and European Energy Companies, Security Firm Finds

http://www.cbc.ca/news/technology/russia-dragonfly-energetic-bear-hacking-energy-us-symantec-1.4276999

A group of malicious hackers believed to be linked to the Russian government have spent nearly two years collecting intelligence inside the computer networks of energy companies in the United States, Turkey and Switzerland - but to what end is unclear. The campaign is just the latest in a string of intrusions targeting energy companies around the world in recent years. Russia is believed to have launched a pair of cyberattacks in 2014 and 2015 against the Ukrainian energy grid, plunging hundreds of thousands of residents into temporary darkness. And the U.S. government has found Russian-linked malware on the computers of American utility operations on a number of occasions - most recently in July.

In this case, security company Symantec attributed the attacks to a group called Dragonfly - also known as Energetic Bear - but declined to link Dragonfly with any particular government or nation state. However, the U.S. Department of Homeland Security and the Federal Bureau of Investigation have previously linked Dragonfly to Russia. "What is clear is that Dragonfly is a highly experienced threat actor, capable of compromising numerous organizations, stealing information, and gaining access to key systems," states a Symantec report, published Wednesday. "What it plans to do with all this intelligence has yet to become clear, but its capabilities do extend to materially disrupting targeted organizations should it choose to do so."

The group was active between 2011 and 2014, and after a lull, re-emerged with its most recent campaign starting in late 2015. However, the Symantec researchers noticed a "distinct increase in activity" this

year. Symantec did not mention any of the energy companies targeted by name. The attackers used a range of techniques to gain access to energy company computers - including phishing emails disguised as a New Year's Eve party invite, and malicious email attachments disguised as business-related documents.

"The attackers also used watering hole attacks to harvest network credentials, by compromising websites that were likely to be visited by those involved in the energy sector," the report says. Once the attackers established remote access to the company's network, those account credentials could be used to compromise other computers inside the network. Symantec says Dragonfly is still active, although for now the group's actions appear limited to reconnaissance. But in possible hint of things to come, the attackers were observed taking screen captures of operational systems, which the Symantec report suggests could even be control systems, based on how the screen capture files are named.

Operation Likely Based in Russia Spent $100,000 on Ads Promoting Divisive Messages: Facebook

https://beta.theglobeandmail.com/news/world/operation-likely-based-in-russia-spent-100000-on-ads-promoting-divisive-messages-facebook/article36191975/

Facebook Inc said on Wednesday it had found that an operation likely based in Russia spent $100,000 on thousands of U.S. ads promoting divisive social and political messages in a two-year-period through May. Facebook, the dominant social media network, said 3,000 ads and 470 "inauthentic" accounts and pages spread polarizing views on topics including immigration, race and gay rights. Another $50,000 was spent on 2,200 "potentially politically related" ads, likely by Russians, Facebook said.

U.S. election law bars foreign nationals and foreign entities from spending money to expressly advocate the election or defeat of a candidate. Non-U.S. citizens may generally advertise on issues. Other ads, such as those that mention a candidate but do not call for the candidate's election or defeat, fall into what lawyers have called a legal gray area.

Facebook announced the findings in a blog post by its chief security officer, Alex Stamos, and said that it was cooperating with federal inquiries into influence operations during the 2016 U.S. presidential election. Facebook briefed members of both the Senate and House of Representatives intelligence committees on Wednesday about the suspected Russia advertising, according to a congressional source familiar with the matter. Both committees are conducting probes into alleged Russian interference in the 2016 U.S. election, including potential collusion between the campaign of President Donald Trump and Moscow. Facebook also gave its findings to Robert Mueller, the special counsel in charge of investigating alleged Russian interference in last year's presidential election, a source familiar with the matter said. The company produced copies of advertisements as well as data about the buyers, the source said. Mueller's office declined to comment.

Facebook said it found no link between the Russian-purchased advertising and any specific presidential campaign. The ads were mostly national in their focus and did not appear to reflect targeting of political swing-states, the company said. Even if no laws were violated, Facebook said the 470 accounts and pages associated with the ads ran afoul of the social network's requirements for authenticity and have since been suspended. Facebook did not print the names of any of the suspended pages, but some of them included such words as "refugee" and "patriot."

More than $1-billion was spent on political ads during the 2016 presidential campaign, thousands of times more than the presumed Russian spending identified by Facebook's security team. But the findings buttress U.S. intelligence agency conclusions that Russia was actively involved in shaping the election. Facebook previously published a white paper on influence operations, including what it said were fake "amplifier" accounts for propaganda, and said it was cracking down. As recently as June, Facebook told journalists that it had not found any evidence of Russian operatives buying election-related ads on its platform.

"Troll Factory" Connection. Representative Adam Schiff, the top Democrat on the House Intelligence Committee, called the Facebook report "deeply disturbing and yet fully consistent with the unclassified assessment of the intelligence community." "We are keenly interested in Russia's use of social media platforms, both the use of bots and trolls to spread disinformation and propaganda, including through the use of paid online advertising," he said in a statement. A Facebook employee said Wednesday that there were unspecified connections between the divisive issue ads and a well-known Russian "troll factory" in St. Petersburg that publishes comments on social media.

Ellen Weintraub, a member of the U.S. Federal Election Commission, said U.S. voters deserve to know where the ads are coming from and that the money behind them is legal. "It is unlawful for foreign nationals to be spending money in connection with any federal, state or local election, directly or indirectly," Weintraub said in a phone interview. She declined to comment on the Facebook ads, saying she could not discuss subjects that could come before the agency.
Facebook declined to release the ads themselves, prompting a sharp rebuke on Twitter from Pierre Omidyar, the billionaire founder of First Look Media, a producer of feature and documentary films, television and podcasts. "Facebook keeps the targeted political ads it publishes secret, emboldening criminals," wrote Omidyar, the eBay founder who also provided funding to launch media organization The Intercept. "I don't see how that can possibly be legal."
Facebook's disclosure may be the first time a private entity has pointed to receiving Russian money related to U.S. elections, said Brendan Fischer, a program director at the Campaign Legal Center, a Washington non-profit that advocates for more transparency. "Whoever may have provided assistance to Russia in buying these Facebook ads is very likely in violation of the law," he said, adding that Facebook has a legal duty to act if it is aware of similar activity in the future.

Man Sentenced for Stealing Identity of Deceased Baby in 1996

https://www.canadiansecuritymag.com/news/industry-news/man-sentenced-for-stealing-identity-of-deceased-baby-in-1996

A Pennsylvania man who assumed the identity of a baby who died in Texas in 1972 has been sentenced to more than two years in federal prison after the baby's aunt discovered the ruse on Ancestry.com. Forty-five-year-old Jon Vincent, of Lansdale, was sentenced Thursday after pleading guilty in May to Social Security fraud and aggravated identify theft. Prosecutors say Vincent escaped from a Texas halfway house in 1996 and stole Nathan Laskoski's identity after searching a cemetery for a similar birthdate. Prosecutors say he also lived in Mississippi and Tennessee under his assumed name, holding jobs, getting drivers' licenses, and even getting married and divorced. Laskoski's aunt was doing an Ancestry.com search when she found a leaf on the family tree linking him to her dead nephew.

And Now, This:

Japanese Develop Robot Dog That Sniffs Out Smelly Feet

http://www.nzherald.co.nz/technology/news/article.cfm?c_id=5&objectid=11920635

Do your feet smell bad? Just a little or absolutely awful? If you don't dare to ask a friend, one Japanese start-up might have the answer with a new robot dog that will sniff your feet and give you a pitilessly honest verdict - even fainting if the stink is especially strong, reported the UK's Daily Mail.
Malodorous feet can be socially awkward in Japan where shoes are removed at the entrance to every home. Hana-chan - a play on the Japanese word for "nose" and a common girl's nickname - is a helpful little robot mutt who will bark if she detects moderately whiffy toes, but will keel over if the pong is particularly pungent. The 15-centimeter (6-inch) dog, equipped with an odor detection sensor for a nose, also sprays air freshener to resolve the situation if the aroma is unbearable.
Manufacturers Next Technology created the robot in response to a request from a man who was desperate to know if he had a problem. "He told us his daughter had said his feet were smelly," employee Kimika Tsuji said. "But he didn't want to know how bad the odor was because he would feel hurt. That's why we developed this cute robot." Tsuji said smells are becoming more of an issue in Japan, a place where subjecting others to your honking body can even be considered harassment.
Next Technology plans to start selling the robot dog early next year, with a price tag of more than 100,000 yen (New Zealand $1276). But this isn't the only device designed to detect body odor. In July, Konica Minolta, a Japanese tech company, began pre-sales of a pocket-sized device that allows people to self-test three categories of smell on a scale from 0 to 100. It can recognise perspiration odor, aging odor and middle fat odor. The device is currently only available in Japan, with no plans to sell it outside of Japan, and costs 30,000 yen (NZ$383).

****

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

****