BRITISH COLUMBIA OCIO Office of the Chief Information Officer

Security News Digest

Special Edition – The Lists for 2016/2017

A Look Back and A Look Ahead

Looking Back: Security Realities in 2016

The 10 Biggest Hacks, Breaches, and Security Stories of 2016

http://www.pcworld.com/article/3152367/security/the-10-biggest-hacks-breaches-and-security-stories-of-2016.html

[with thanks to Ian Paul] It's been a long, depressing, breach-filled year in the world of computer security. Yahoo broke the record for allowing the largest hack in history - twice. Millions of zombified webcams and DVRs took down the Internet for users in the United States. Russia was accused of "hacking the vote," and a new type of malware earned a tidy profit extorting unsuspecting users for Bitcoin. What was it John Oliver said about 2016, again? [NSFW – not suitable for work; language warning…you were warned…your choice…]

(1) Hackers Turn Yahoo into Yahoos

In September, Yahoo shocked the world when it revealed that at least 500 million user accounts had been breached. At the time, the breach was believed to be the largest theft of personal data from a major technology company ever. Making matters even worse, Yahoo later disclosed that the hack itself had happened in 2014 but only came to light in 2016, so the attackers had access to user information for *years*. But it turns out that was just the warm-up. In mid-December, Yahoo dropped the jaw-dropping revelation that a separate hack occurred around August 2013 that leaked the data of one billion users - double the record-breaking hack from September. This is why strong, unique passwords for every site and service you use is important, people.

(2) Rampant Ransomware

The one threat that defined 2016 more than any other has to be ransomware. This nasty malware encrypts your files and then holds them hostage, demanding payment - usually in semi-anonymous Bitcoin - before decrypting your stuff. Many, many, many ransomware variants made headlines in 2016, including Locky, DMA Locker, Surprise, and an amateurish (yet effective) version called Ranscam that takes your money but deletes your files anyway. There was even mobile ransomware, and in July researchers found a version of Locky that could operate offline to be even more effective. In August, a study by Malwarebytes said ransomware was so common it was hitting nearly half of all U.S. businesses.

(3) Dyn DDoS

In October, a botnet kicked off a massive distributed denial of service (DDoS) attack against Dyn, a major domain name system (DNS) provider. DNS is the web routing system that turns a website name like google.com into a numerical Internet Protocol address such as 172.217.21.110 for computers to read. Without DNS a web browser cannot find the website you want to see - and that's exactly what happened to millions in the United States during the DDoS attack. Access to major sites such as Twitter, GitHub, and Netflix went up and down throughout the day. Several days later we learned the botnet that wreaked the DNS havoc consisted of about 100,000 household devices (such as webcams and DVRs) infected with the Mirai malware. Yes, an army of dumb, insecure smart devices attacked the web.

(4) Apple Stops Patching QuickTime

QuickTime used to be one of the most ubiquitous pieces of software on a PC. It was vital for watching many early videos, especially in iTunes. Over time, however, QuickTime has become less and less important, and now it's borderline unnecessary. Earlier this year, after two critical vulnerabilities were discovered for the software, Apple apparently decided to deprecate QuickTime for Windows rather than fix the issues. In other words, if you're still running QuickTime on your Windows machine uninstall it now.

(5) Distributed Guessing

Your credit card's security measures aren't as secure as you'd think. Researchers at Newcastle University in the United Kingdom demonstrated that discovering a credit card's expiration date and card

verification value (CVV) number can actually be relatively simple. The researchers came up with a novel way to guess these low-digit numbers using a technique called "distributed guessing." Basically, a laptop carries out hundreds of guesses simultaneously on various payment sites, using slightly different expiration date and CVV details for the card. Within about six seconds you'll find the right numerical sequence to unlock a credit card's secret codes, the researchers said. The weakness is a failure to properly limit attempts at filling out payment details, and credit card systems that don't actively monitor for simultaneous incorrect credit card detail attempts.

(6) DNC Hack

This year, computer hacking graduated from harassing businesses and government agencies to direct intervention in the U.S. presidential election. The first instance was a breach of the computer network of the Democratic National Committee. Wikileaks published a trove of documents in July that included nearly 20,000 emails and thousands of attachments from DNC staffers. Several scandals sprung up in the aftermath, including implications that the DNC actively tried to work against Bernie Sanders' campaign to support frontrunner Hillary Clinton as the Democratic nominee. DNC Chair Debbie Wasserman Schultz was forced to resign as a result of that revelation. A hacker going by the name Guccifer 2.0 claimed responsibility for the data theft, but American investigators believed it was the work of Russian state actors.

(7) Russian Dirty Deeds

In September, U.S. investigators looked into the possibility that Russia was trying to undermine or disrupt the election. Toward the end of 2016, the Central Intelligence Agency and other American intelligence agencies concluded with "high confidence" that Russia tried to covertly influence the election. The concern wasn't over hacking voting machines but that Russian hackers had infiltrated the computer systems of both major U.S. political parties, possibly with direct involvement from Russian President Vladimir Putin. As of mid-December, the Office of the Director of National Intelligence (ODNI) - the head of the American intelligence community - had not endorsed that assessment, according to Reuters.

(8) The San Bernardino iPhone

In December 2015, Islamic extremists committed a terrorist attack in San Bernardino, California, killing 14 people and seriously injuring another 22. The couple later died in a gunfight with police. In 2016, an iPhone belonging to one of the terrorists took center stage because it used Apple's built-in security tools to protect the device from unauthorized access. The FBI wanted Apple to create special software to allow investigators to get into the phone. Apple refused, arguing the FBI wanted the company to, in effect, "custom-build malware" to undermine the company's own security features. The FBI eventually dropped its request to Apple after a security firm was able to help investigators access data on the phone. The case's legacy lives on as lawmakers consider what kind of help companies with encryption-capable products should provide to law enforcement.

(9) NSA Hacked

In August, an anonymous hacker group called the Shadow Brokers said it had obtained hacking tools from the Equation Group, a cyber-espionage team linked to the National Security Agency. During the infiltration the Shadow Brokers grabbed sophisticated exploits that were reportedly used by the NSA. The tools were capable of infecting device firmware and remaining on an infected system even after a complete operating system refresh. After revealing a portion of their treasure trove, the Shadow Brokers attempted to sell other hacking tools they'd obtained, but as of early October the sale had generated little interest.

(10) SWIFT Hack

It started as a single $81 million malware attack against a Bangladeshi bank targeting the SWIFT (Society for Worldwide Interbank Financial Telecommunications) transaction software. By late May, however, up to a dozen banks around the world were investigating potential hacks against the SWIFT system. In July, SWIFT was seeking help from outside security professionals to control the widening hacking epidemic.

These Were the Biggest Hacks, Leaks and Data Breaches of 2016

http://www.zdnet.com/pictures/biggest-hacks-security-data-breaches-2016/

[with thanks to Zack Whittaker] This was the year when many historical hacks came back to bite millions just as they were least expecting it. The uptick in delayed reporting contributed to almost 3,000 publicly disclosed data breaches this year alone - exposing more than 2.2 billion records. And the year isn't even

over yet. Even as we approach December 31, there's no sign of it ending. Let's take a look back at some of the biggest - and most dangerous - hacks and leaks so far.

(1) MySpace Hack Puts Another 427 Million Passwords Up for Sale

Time Inc. has confirmed the theft of 427 million passwords from MySpace, the aging social networking site the media company acquired just three months ago. The records were offered for sale on the dark web by the same hacker who posted for sale a trove of 117 million stolen LinkedIn passwords nearly two weeks ago. The posted price for MySpace credentials is 6 bit coins or about $3,200 at today's rate.

(2) A Hacker Claims to be Selling Millions of Twitter Accounts

A Russian seller, who goes by the name Tessa88, claimed in an encrypted chat, to have obtained the database, which includes email addresses (and sometimes two per person), usernames, and plain-text passwords. Tessa88 is selling the cache for 10 bitcoins, or about $5,820 at the time of writing. LeakedSource said it was unlikely Twitter was breached. "The explanation for this is that tens of millions of people have become infected by malware, and the malware sent every saved username and password from browsers like Chrome and Firefox back to the hackers from all websites including Twitter".

(3) One of the Biggest Hacks Happened Last Year, but Nobody Noticed

Hackers last year quietly stole a database containing the details of over 57 million people. The breach has only come to light this week [in May2016], after the stolen data was put up for sale on the dark web. The breach data contains data spanning three years between 2012 and 2015, including usernames, email addresses, and passwords that were hashed with the MD5 algorithm, which nowadays is easy to crack. Many cell phone numbers and Facebook usernames are also in the cache. ..A grey-hat hacker, who goes by the name Peace, obtained a copy of the stolen data from Russian hackers, and provided a number of files containing the breached data to ZDNet earlier this week. Security expert Troy Hunt, who runs breach notification site Have I Been Pwned, helped analyze and verify the data. Hunt found over 52.5 million unique emails in the cache, suggesting the vast majority of data has not been previously leaked. *But here's the twist: nobody can say for sure where the data came from* [despite many efforts].

(4) 100 Million VK.com Accounts Stolen by Hackers

A hacker has obtained 171 million user accounts associated with social networking giant, VK.com. The stolen database contains full names, email addresses and plain-text passwords, and in many cases locations and phone numbers. The St. Petersburg, Russia-headquartered social network - formerly known as VKontakte - is said to be the largest in Europe, with over 350 million users at the last count. The hack is thought to have been carried out in late-2012 or early 2013, but the hacker who is selling the data could not be more precise.

(5) Hacker Puts 51 Million File Sharing Accounts for Sale on Dark Web

User accounts for iMesh, a now-defunct file sharing service, are for sale on the dark web. The New York-based music and video sharing company was a peer-to-peer service, which rose to fame in the file sharing era of the early-2000s, riding the waves of the aftermath of the "dotcom" boom. After the Recording Industry Association of America (RIAA) sued the company in 2003 for encouraging copyright infringement, the company was given status as the first "approved" peer-to-peer service.

(6) Ubuntu Forums Hack Exposes 2 Million Users

The company that builds Ubuntu, a popular Linux distribution, has said its forums were hacked Thursday. Canonical, which develops the operating system, said in a statement on Friday [in July2016] that two million usernames, email addresses, and IP addresses associated with the Ubuntu Forums were taken by an unnamed attacker. The attacker was able to exploit an SQL injection vulnerability in an add-on used by older vBulletin forum software.

(7) Oracle Investigating Data Breach at Micros Point-of-Sale Division

Oracle has confirmed that it is investigating a breach of its Micros division. Security journalist Brian Krebs, who first covered the story, said that hackers had compromised hundreds of systems at the software giant's point-of-sale division, and broken into a support portal used by customers of the devices. Oracle confirmed the breach in an email to ZDNet, saying it had "detected and addressed malicious code in certain legacy Micros systems," but added that Oracle's own systems, corporate network, and other cloud and service offers were not impacted.

(8) Epic's Forums Hacked Again, with Thousands of Logins Stolen

A hacker has stolen hundreds of thousands of forum accounts associated with Unreal Engine and its maker, Epic Games. More than 808,000 accounts were stolen in the attack - with more than half a million from Unreal Engine's forums alone. Breach notification site LeakedSource.com, which obtained a copy of the database, said the attack was carried out August 11. The hacker, whose name isn't known, exploited

a known SQL injection vulnerability found in an older vBulletin forum software, which allowed the hacker to get access to the full database. The hacker acquired usernames, scrambled passwords, email addresses, IP addresses, birthdates, join dates, their full history of posts and comments including private messages, and other user activity data from both sets of forums. Facebook access tokens were stolen for those who signed in with their social account. But most of the passwords were scrambled in a way that were not readily or easily crackable.

(9) Millions of Steam Game Keys Stolen After Hacker Breaches Gaming Site

A little over nine million keys used to redeem and activate games on the Steam platform were stolen by a hacker who breached a gaming news site last month. The site, DLH.net, provides news, reviews, cheat codes, and forums, was breached on July 31 by an unnamed hacker, whose name isn't known but was also responsible for the Dota 2 forum breach. The site also allows users to share redeemable game keys through its forums, which along with the main site has around 3.3 million unique registered users, according to breach notification site LeakedSource.com, which obtained a copy of the database. A known vulnerability found in older vBulletin forum software, which powers the site's community, allowed the hacker to access the databases. The data stolen from the forum includes full names, usernames, scrambled passwords, email addresses, dates of birth, join dates, avatars, Steam usernames, and user activity data. Facebook access tokens were stolen for those who signed in with their social account.

(10) Hackers Stole Over 43 Million Last.fm Accounts in 2012 Breach

New details about a historical hack of music website Last.fm have come to light [in Sept2016]. Last.fm, owned by CBS (which also owns ZDNet and sister website CNET), suffered a data breach in 2012, but details of the attack were not disclosed. Reports suggested the service had an estimated 40 million users at the time. On Thursday, breach notification site LeakedSource, which obtained a copy of the database and posted details of the hack in a blog post, said more than 43.5 million accounts were stolen. LeakedSource was able to confirm that usernames, email addresses, join date, and other internal records, such as newsletter sign-ups and ad-related data, were stolen in the breach. The database also contained hashed passwords, scrambled with the MD5 algorithm that nowadays is easy to crack. LeakedSource said that the algorithm is "so insecure" that it was able to decipher over 96 percent of passwords in just two hours. ZDNet was able to independently verify the legitimacy of the data.

Top Celebrity Online Security Screw-ups in 2016

http://www.csoonline.com/article/3150035/data-protection/top-celebrity-online-security-screwups-in-2016.html

[with thanks to CSO staff] Password manager Dashlane has compiled a list of celebrities who have run afoul of basic security rules in 2016 and, like TMZ, are publicly shaming them. *The company's goal in releasing the P@ssholes List is to draw attention to many high-profile, yet common, password gaffes that are often easily preventable*. The company says while it can be amusing to have a little tongue-in-cheek fun at the expense of celebrities, *the fact of the matter is that most people are guilty of making the same errors*. Whether it's using a weak and easily guessed password, or reusing a password that was leaked in a previous breach, all of these P@sshole cases highlight *the important role passwords play in our digital lives*.

Below are the Top 10 P@ssholes of 2016. The list is random and not in order of rank.

(1) Drake, Katy Perry and others were OurMine Victims - If you're reading this, it's too late... Summer 2016 saw dozens of celebrities suffer Twitter takeovers by the OurMine hackers. The cause? Weak and reused passwords from old MySpace accounts.

(2) National Football League - The NFL had to scramble like Russell Wilson to secure their Twitter account after hackers announced that Commissioner Roger Goodell was dead. They could have blocked the breach attempt if they tackled passwords the proper way as unsportsmanlike hackers got in by cracking the email of an employee who handles social media.

(3) Big Websites: AdultFriendFinder, Dropbox, MySpace, LinkedIn, Yahoo - Remember MySpace? Hackers do, and said yahoo when they took advantage of the more than 2 billion usernames, passwords, and email addresses that stemmed from breaches at these companies. Millions of people had to update their passwords to avoid putting their friends, reputations, and connections, both professional and private, at risk.

(4) John Podesta - The chairman of Hillary Clinton's presidential campaign was the victim of a classic phishing email. As a result, his Gmail account was leaked for the world to see - an event that probably

altered the course of the U.S. presidential election. This classic case shows that firewalls can't keep all of the intruders out.
(5) Kylie Jenner - The youngest member of the Kardashian-Jenner clan also had her Twitter account hacked by the OurMine hacker group. In keeping up with terrible celebrity PR moves, she immediately took to Snapchat to proclaim, "I don't really care, I'm just letting them (hackers) have fun."
(6) Tech Leaders: Mark Zuckerberg, Sundar Pichai, Daniel Elk, Jack Dorsey, Travis Kalanick - We trust tech companies to secure our personal data, but that faith is put to the test when the leaders of some of the world's most popular companies use bad passwords to protect their own accounts. Mark Zuckerberg of Facebook made headlines this year for presumably using his daughter's first words to protect his Twitter and Pinterest accounts. But let's not forget about Sundar Pichai (Google), Daniel Elk (Spotify), Jack Dorsey (Twitter), and Travis Kalanick (Uber) - who all had their social media accounts hacked this year.
(7) Houston Astros – The Houston Astros of Major League Baseball had their online database of player statistics hacked by a former executive of the St. Louis Cardinals. The hacker, Christopher Correa, who was recently convicted on federal charges, used the password of a former Cardinals employee who had recently joined the Astros. This is a grand slam password fail.
(8) Harry Styles - While no one is iPerfect, protecting your iCloud account with a weak password will only take you in One Direction; hacked. This year, people got access to Styles' files when an iCloud account associated with him was breached. Rough seas were ahead for Harry, as pictures from an intimate boating trip with Kendall Jenner were splashed around the world.
(9) Jack Johnson - More like Hack Johnson. One-half of the pop-rap duo Jack & Jack (and not the affable adult alternative artist), had one of the worst password stunts of the year when he requested that his 4+ million Twitter followers send him their passwords so he could put a personalized video in their feeds.
(10) Tom Hiddleston - Less than a week after joining Instagram, his account was promptly hacked. Hopefully, he can shake off his password mistake and come back in cybersecurity style.
Dashlane says celebrities, like the rest of us, must deal with a broken system that demands human beings memorize passwords for all of the accounts we have. To be completely secure, you need a strong, unique password for each online
account.
Password hygiene Below are four actions everyone can take to ensure the best password hygiene. *[Because the Information Security Branch takes every opportunity to remind our readers.]*
Strong passwords – Your passwords should be like Kanye West album titles… completely random and impossible to guess. Never use passwords that are easy to guess, such as ones with common names or things people know about you. Your passwords should be at least eight characters long and include a mix of random letters, numbers, and symbols.
Different password for every account – Treat your passwords like a celebrity treats an outfit; never use it twice. If a hacker gets access to a password that you're reusing then they have access to all of your accounts. Having a unique password for every account ensures that even if one is breached, others will be secure.
Two-factor authentication – This is like hiring another bodyguard, and ensures that even if someone does get your password, they can't access your account without a second form of authentication, such as a text message code or email link.
Get a password manager!– Password managers simplify all of the items above by creating and storing strong passwords for all of your accounts.

The Top 10 Tech Stories of 2016: Post-PC, Post-Reality

http://www.networkworld.com/article/3149705/security/the-top-10-tech-stories-of-2016-post-pc-post-reality.html
[with thanks to Marc Ferranti, IDG News Service]

(1) Election of Trump Brings Fake News to the Fore

The U.S. presidential election highlighted the internet's power to disseminate false information, fueling a fierce debate over the role of social networks in the media landscape and how Facebook, Google and Twitter should police "fake news." The election was the number one news topic on Facebook this year, and that "news" included blatantly false stories, including one that Hillary Clinton was running a child porn ring out of a Washington, D.C., pizza parlor (with considerable harassment for the parlor owner).

(2) Mirai Botnet Pokes Holes in IoT Security

The Internet of Things (IoT) promises to revolutionize industry and enhance all sorts of web-connected services, but thanks to the Mirai botnet, it also represents a global security risk. Mirai was designed to scan the internet for devices like cameras and DVRs, then access and control them. In addition to other attacks, Mirai was responsible in September for a DDoS attack that overwhelmed cloud provider Akamai and brought down the website of security expert Brian Krebs. In October, it hit DNS (Domain Name System) service provider Dyn and disrupted dozens of major websites. Security experts are warning that more botnets like Mirai will appear unless the hardware industry moves away from default passwords.

(3) Qualcomm Buys NXP: The Incredible Shrinking Chip Industry

Mergers and acquisitions are a great window on how tech evolves, and this year's $38 billion deal for Qualcomm to buy NXP Semiconductors, announced in October, was a signpost pointing to how the chip industry is consolidating around IoT. Qualcomm wants to expand beyond a stagnating mobile phone industry, getting into NXP's market for chips for cars and IoT devices.

(4) Intel Axes 12,000 as It Breaks Away from PCs

In another confirmation that we're living in a post-PC world, Intel announced in April that it would lay off 12,000 people, a whopping 11 percent of its worldwide workforce. The slowdown in PC shipments has hurt Intel, and the company needs to evolve to better serve the cloud and IoT. Data-center equipment will be Intel's growth area growing forward, along with the rapidly increasing number of sensors and connected devices.

(5) HoloLens Goes on Sale: The VR Future is Here

The release of Microsoft's HoloLens Development Edition at the end of March, and the later release of the hardware to non-developers worldwide, marked a major milestone for the burgeoning markets for both virtual and augmented reality. Other bellwether VR events included the releases of the Oculus Rift and HTC Vive VR headsets. But it seems Microsoft is leading the charge to bring VR and AR to the masses, promising a Windows Holographic software update to Windows 10 next year, a move that could make it easier to blend physical and digital reality on any PC.

(6) The DNC hack: Cyberespionage Shapes an Election

The revelation in June that hacking groups with likely Russian ties had hacked into the U.S. Democratic National Committee's computer network sent shockwaves through the global security community. Emails made public by WikiLeaks caused embarrassment among Democrats, led to the resignation of several DNC officials and allowed Hillary Clinton's opponents to portray her and the party's infighting in an unflattering light. The assessment of intelligence officials that Russian hackers intervened to sabotage Clinton's campaign, taking cyberespionage to a new level, has created a rift between Trump and the intelligence agencies, a blow to smooth U.S. intelligence operations.

(7) Samsung's Note7 Recall: Epic Fail

When Samsung released the stylish Galaxy Note7 in August, gushing reviewers found a lot to like. But soon enough, if you called it a "hot" product you'd be accused of committing a bad pun. Users started reporting problems with overheating and even outright fires. Samsung started recalling the device, and in October it finally threw in the towel, stopping production. The Note7 recall has been both a public-relations and a financial debacle for Samsung, and one of the tech industry's epic fails of all time: The company has reported that third-quarter operating profit fell 95 percent, largely as a result of the Note7 recall.

(8) AlphaGo Dominates, Humans Get Worried

Google DeepMind's AlphaGo artificial-intelligence program overwhelmed 18-time world champion Go player Lee Se-dol in March, beating him 4 games to one in a Seoul match watched around the world. The AlphaGo program's ability to learn from its experience apparently explained its unexpected and far-from-human moves. It was arguably the biggest AI v. man event since IBM's Deep Blue defeated Garry Kasparov in chess in 1997. As a wide variety of films and TV series around the world attest, concerns about AI have entered the zeitgeist, and no wonder: Milestones keep happening as AI is incorporated into everyday tech products. Google CEO Sundar Pichai said, "We've evolving from a mobile-first to an 'AI-first' world." That is exactly what has humans worried.

(9) Apple Kills Headphone Jack: Courage or Arrogance?

When Apple announced in September it was eliminating the 3.5mm headphone jack in the iPhone 7 to pave the way to a wireless future, users around the world fumed. Getting rid of USB ports in the new MacBooks added insult to injury for many. Now, uncountable peripherals will no longer directly work with

Apple devices. Apple's Phil Schiller said it took "courage" for Apple to move on from legacy ports, but many users said the change showed that Apple cares more about its own vision than about consumers.

(10) Apple v. FBI: Encryption Debate Intensifies

In February, Apple was ordered by a federal judge in California to provide assistance to the Federal Bureau of Investigation to search a locked iPhone 5c that was used by Syed Rizwan Farook in the December 2015 attack in San Bernardino, California, that left more than a dozen people dead. The order crystallized a long-running debate about public access to encrypted devices, including whether tech companies should help law enforcement crack encrypted devices. In March, the judicial order was vacated after the FBI was able to hack the iPhone with the help of an unidentified third party. With law enforcement officials around the world dealing with an increasing number of encrypted devices in criminal cases, though, the debate over encryption is far from over.

The 20 Biggest Tech Disasters of All Time

http://www.techrepublic.com/pictures/the-20-biggest-tech-disasters-of-all-time/

[with thanks to Conner Forrest] Sometimes, a small tech problem can lead to something much worse. Here are some of *the most critical problems ever caused by faulty software, hardware, and other errors*.

(20) Bendgate. When the iPhone 6 and 6 Plus first launched in 2014, some users reported that the phone bent after normal use, leading Apple to replace the affected devices. However, some reports said that the incidents were blown out of proportion.

(19) Windows Vista. In late 2006, Microsoft introduced the Windows Vista operating system. Vista would later go down in history as one of the worst Windows operating systems of all time, with numerous problems around activation, security, performance, pricing, and more.

(18) Blackberry Outage. A BlackBerry service outage in 2011 left some customers in Europe, the Middle East, Africa, South America, the United States, and Canada without text messaging or internet access for a few days. The outage eventually led many customers to switch to iOS or Android devices.

(17) Southwest Outage. After a router failure in July 2016, Southwest Airlines was forced to cancel 2,300 flights and delay and additional 7,000. A similar outage happened to Delta Airlines a month later, and then to United Airlines soon after.

(16) Knight Capital Group Stock Error. An error in Knight Capital Group's stock trading software algorithm caused the program to send through millions of unapproved trades, leading the company to lose $440 million in 30 minutes. According to Bloomberg, the loss was greater than the company's market cap at the time in 2012.

(15) Target Breach. In late 2013, retail giant Target announced that it had been the subject of a massive data breach. It was estimated that personal information and credit card numbers from up to 70 million customers could have been leaked.

(14) Sony DRM Malware. In 2005, it was discovered that some Sony music CDs were installing unwanted software, without a user's permission, on the computer they were played on. This led to a massive class action lawsuit and recall.

(13) Pepsi Bottling Number Glitch. In the early 1990s, a Pepsi promotion in the Philippines claimed that the lucky customer to find a bottle with the number 349 printed under its cap would win a large sum of money. Unfortunately, a computer glitch caused thousands of number 349 caps to be printed, leading to riots in the streets and even a bombing of a Pepsi plant in the country.

(12) EDS Child Support System Error. Incompatible software, mismanaged payments, and additional errors led to a £1.1 billion cost for the UK's Child Support Agency (CSA), because of a poor system built for the agency by Electronic Data Systems (EDS). This disaster led to a backlog of 300,000 child support cases, with an additional 36,000 cases stuck in the system.

(11) LAX Network Problem. In 2007, a computer outage at Los Angeles International Airport led to the standing of 17,000 passengers on international flights for 10 hours. The problem occurred because US Customs authorities couldn't screen the passengers without the software.

(10) Lenovo Superfish Malware. In 2015, it was discovered that many Lenovo laptops were shipped with a software called Superfish that allowed for a user's browser traffic, including confidential communications, to be snooped on. The issue devolved into the involved companies pointing fingers at each other and trying to shift the blame.

(9) AT&T Network Collapse. A faulty line of code in a software patch for AT&T's switching system caused half of the entire network to crash in 1990. It started in New York, when one system went down for routine maintenance, but incorrect messages led to an enormous outage.
(8) Ariane 5 Explosion. A software error in 1996 caused the explosion of the $7 billion Ariane rocket in Kourou, French Guiana. The core issue was found to be a conversion error when the software attempted to convert a 64-bit floating point number to 16 bits.
(7) Dell Battery Explosions. Certain Dell laptop models in the mid-2000s had a bad habit of catching fire or exploding, due to their batteries. This led to a recall of 4.1 million laptop batteries, which were actually manufactured by Sony.
(6) Healthcare.gov Launch. After the Patient Protection and Affordable Care Act was signed into law, the US government launched the HealthCare.gov website in 2013. However, numerous issues plagued the site, including long wait times and information going missing. By some estimates, only 1% of users were actually able to enroll in a healthcare program during the early days.
(5) Apple's Antennagate. The iPhone 4 launch in June 2010 quickly gave rise to a problem known as Antennagate, in which the antenna placement on the device could be easily covered by a user's hand, leading to poor reception. Apple eventually agreed to pay qualified users $15 to purchase a bumper case for the phone.
(4) TJX Hack. A network flaw allowed hackers to steal close to 46 million credit card numbers in 2007 from TJX, the parent company of T.J. Maxx, Marshalls, HomeGoods, A.J. Wright, and others. It is believed that weak security around the company's wireless LAN was the problem.
(3) Mars Climate Orbiter Lost in Space. In 1999, the Mars Climate Orbiter was lost in space, at an estimated cost of $193 million. The problem stemmed from software developed by Lockheed Martin that converted a certain set of numbers into the wrong units.
(2) Soviet Nuclear Warning System False Alarm. In 1983, a Soviet Union nuclear early warning system nearly caused World War Three. A computer at the Serpukhov-15 bunker in Moscow falsely reported that the US had fired a missile at the Soviet Union. Lieutenant colonel Stanislav Petrov correctly interpreted it as a false alarm, potentially preventing a world war.
(1) Samsung Galaxy Note7 Exploding Batteries. A few weeks after its launch, the Samsung Galaxy Note7 smartphone began experiencing overheating and exploding batteries. After numerous recalls and temporary fixes, the company stopped production and discontinued the line. The fiasco cost the company billions of dollars in potential profits.

Looking Ahead: Security Predictions for 2017

2017 Security Predictions

http://www.networkworld.com/article/3145730/security/2017-security-predictions.html

[with thanks to Sharon Florentine, CIO] If you thought 2016 was bad, fasten your seat belts - next year is going to be even worse. We asked two leading cybersecurity experts, Matt Dircks, CEO of secure access software company Bomgar and Scott Millis, CTO at secure device management and mobile security company Cyber adAPT, what to expect in 2017.

(1) Passwords 'Grow Up'

The recent DDoS attack that wreaked havoc on a huge portion of the internet on Oct. 21 was at least partly enabled by unchanged default passwords on IoT devices, says Dircks, which hackers were able to exploit. Don't think you're immune; how many of your users have simple, common or outdated passwords? In 2017, Dircks says better password management services will gain traction as businesses understand how vulnerable they are.

(2) Privilege Gains Power

Hackers want high-level access, which they get through targeting the credentials of privileged users like IT professionals, CEOs and vendors, Dircks says. And while organizations have applied security to the systems, applications and data that are most critical to their business, these preventative measures simply aren't enough anymore. In 2017, he says, savvy organizations will finally get serious about protecting not just systems, but privileged users by identifying them, monitoring their access and closing off access to what they don't need.

(3) The Security Blame Game will Heat Up
When a breach occurs, even with layers of security, the question of who "owns" it and who had or has power to do something about it will create intense reactions and finger-pointing. Companies can head off this blame game by ensuring open communication between IT and business leadership to understand the potential threats, options for security and safety and the challenges and constraints that exist within the organization, Dircks says.
(4) Ransomware will Spin Out of Control
Since January 1, 2016, Symantec's Security Response group has seen an average of more than 4,000 ransomware attacks per day: a 300 percent increase over 2015, according to its 2016 Internet Security Threat Report. Most organizations rely on low-overhead prevention techniques, such as firewall and antivirus solutions or intrusion prevention to mitigate threats like these, says Cyber adAPT's Scott Millis. However, these tools are insufficient, and breach data shows that detection and incident response must be improved. And as attackers continue to use social engineering and social networks to target sensitive roles or individuals within an organization to get to data, the need for comprehensive security education becomes even more critical, he says. ..Finally, new attack surfaces - for example, IaaS, SaaS and IoT - are still so new that organizations haven't yet figure out the best way to secure them, he says.
(5) Dwell Times will See No Significant Improvement
Dwell time, or the interval between a successful attack and its discovery by the victim, will see zero significant improvement in 2017, Millis says. In some extreme cases, dwell times can reach as high as two years and can cost a company millions per breach. "Why so long? In my view, this is annoyingly simple - there's little or no focus on true attack activity detection. At the advent of the 'malware era', companies, vendors and individuals were rightly concerned about 'keeping out the bad guys', and a whole industry grew quickly to focus on two basic themes: 'Defense-in-depth', which I view as layering prevention tactics in-line to make penetration from the outside more difficult; and 'Malware identification', which manifested itself as an arms race towards 100-percent-reliable identification of malware," Millis says. While response technologies and remediation capabilities, improved, victims were able to isolate and repair damage very quickly. The problem is these technologies didn't help reduce dwell time; unless response teams stumbled upon something malicious or randomly discovered an anomaly, Millis says.
(6) Mobile will Continue to Rise as a Point of Entry
At least one, if not more, major enterprise breaches will be attributed to mobile devices in 2017, Millis predicts. A Ponemon Institute report found that for an enterprise, the economic risk of mobile data breaches can be as high as $26.4 million and 67 percent of organizations surveyed reported having had a data breach as a result of employees using their mobile devices to access the company's sensitive and confidential information. People and their mobile devices are now moving around way too much, and much too fast, for old-fashioned cybersecurity strategies to be effective, Millis says. Add to that an increasing sense of entitlement by users with regards to the devices they choose to use, and you have a situation ripe for exploitation.
(7) Internet of Threats?
IoT vulnerabilities and attacks will rise and will increase the need for standardization for various security measures - hackers at this year's Def Con found 47 new vulnerabilities affecting 23 devices from 21 manufacturers. And, of course, in October 2016 the massive DDoS attack on major global websites including Twitter, Netflix, Reddit and the UK government's sites - was reportedly powered by the Mirai botnet made up of insecure IoT devices. "A lot of attention is focused on 'smart devices' as proof of IoT's growing influence. The reality is a connected device doesn't make it a smart device. The 'things' that are being connected often 'fire-and-forget' in their simplicity, or are built-in features and tools we may not even know are there - like the routers used in the Mirai botnet. This leads to a mindset of ignoring these 'dumb' devices without paying attention to the fact that these devices, while inherently 'dumb', are connected to the biggest party-line ever made: the internet," says Bomgar's Matt Dircks.

McAfee Labs Predicts 14 Security Developments for 2017

https://www.helpnetsecurity.com/2016/11/29/security-developments-2017/
Intel Security released its McAfee Labs 2017 Threats Predictions Report, which identifies 14 threat trends to watch in 2017.
(1) Ransomware attacks will decrease in volume and effectiveness in the second half of 2017.
(2) Windows vulnerability exploits will continue to decline, while those targeting infrastructure software and virtualization software will increase.

(3) Hardware and firmware will be increasingly targeted by sophisticated attackers.
(4) Hackers using software running on laptops will attempt dronejackings for a variety of criminal or hacktivist purposes.
(5) Mobile attacks will combine mobile device locks with credential theft, allowing cyber thieves to access such things as banks accounts and credit cards.
(6) IoT malware will open backdoors into the connected home that could go undetected for years.
(7) Machine learning will accelerate the proliferation of and increase the sophistication of social engineering attacks.
(8) Fake ads and purchased "likes" will continue to proliferate and erode trust.
(9) Ad wars will escalate and new techniques used by advertisers to deliver ads will be copied by attackers to boost malware delivery capabilities.
(10) Hacktivists will play an important role in exposing privacy issues.
(11) Leveraging increased cooperation between law enforcement and industry, law enforcement takedown operations will put a dent in cybercrime.
(12) Threat intelligence sharing will make great developmental strides in 2017.
(13) Cyber espionage will become as common in the private sector and criminal underworld as it is among nation-states.
(14) Physical and cybersecurity industry players will collaborate to harden products against digital threats.

_____

8 Boldest Security Predictions for 2017

http://www.darkreading.com/endpoint/8-boldest-security-predictions-for-2017/d/d-id/1327759

[with thanks to Erica Chickowski] Scary, funny and maybe even a little outlandish, these industry predictions come from prognosticators who didn't mince words.

(1) Rubber Ducky, You Make Bot Time Lots Of Fun

In light of the rise of the Mirai botnet this year, we weren't surprised to see many industry insiders predicting a ramp-up in weaponization of the Internet of Things (IoT) to carry out wide-scale DDoS attacks in 2017. This isn't a brand new phenomenon, just a burgeoning one; in fact it was one of the boldest predictions we made for 2016 that actually came true. One security fortune teller, however, was extremely specific with his IoT botnet predictions. "We expect to see hackers continue to exploit IoT device vulnerabilities to launch attacks, and they will likely use Edwin, the app-connected smart duck [this is a real educational toy for small children] who will be the biggest security threat of the year," says Jeff Harris, vice president of solutions for Ixia. "Hackers will leverage Edwin to launch the "Rubber Ducky Botnet Army" of 2017, making it critical for organizations to better defend their networks to prevent the strong DDoS attacks made possible through a yellow ducky."

(2) Drone Jacking Reaches New Heights

Speaking of IoT security, some of the most interesting expectations for attacks in this field involved unmanned aerial vehicles. Namely, that as drones become more widely used by businesses for deliveries, filming, surveillance, and more, attackers are going to see them as a prime hijacking candidate. "Drones have their own unique identity but they could be considered mobile as well as IoT devices as they start connecting with other devices," says Mandeep Khera, CMO of Arxan. "As drones start getting more used for deliveries of goods, expect dronejacking and other attacks. Hackers can also cause drones to malfunction with malware, resulting in injuries."

(3) The Internet Takes An Unscheduled Sick Day

No, if you type Google into Google you cannot shut down the Internet. But with the right kind of attack against DNS, attackers might be able to do some real damage. This year saw some unprecedented DDoS attacks when it came to the size, scope and target of attacks. DNS providers were hit hard by some epic floods of traffic, and attackers used methods like reflective attacks to barrage victim networks with some of the biggest attacks on record, tipping the scales at over 1 Tbps of traffic. Given that, maybe it's not so crazy for James Carder, CISO of LogRhythm, to predict that in 2017 we could be in for a total shut down of the Internet for up to 24 hours. "We'll see a rise in attacks on fundamental protocols of Internet communications. We already started seeing it with DNS," Carder says. "In 2017, we're going to see it hit big sometime, somewhere. If the Internet goes down, financial markets will tank."

(4) Ransomware At Your Service

One of the more interesting forecasts was that ransomware is likely to grow even more user-friendly - or should we say victim-friendly? "As awareness around ransomware grows and fewer people click on links, ransomware operators will need to take steps to improve their ransomware conversation rate by making it easier for ransomware victims to pay up. In 2017, we'll see the widespread availability of ransomware customer support with more attackers offering FAQs, tech support forums, and even call centers to walk victims through paying and restoring their data," says Todd O'Boyle, co-founder and CTO of Percipient Networks. "And to increase their chances of being paid, many ransomware operators will lower their prices, be open to negotiation, and offer discounts."

(5) Not A Movie Title: Return Of The Worm

A number of prognosticators weighed in on new possibilities for the resurgence of worm attacks in various guises. "2017 will be the return of the worm," says Lamar Bailey, senior director of security R&D at Tripwire, specifically pointing to IoT applications as prime targets. "The inherent insecurity in the majority of IoT devices, due to the fact vendors are valuing time to market over security, makes them ripe for exploit. Consumers are buying and installing these devices in record numbers to make their life easier but in many cases they are opening up their homes to complete external surveillance and control." Most recently, academic researchers showed how smart lighting fixtures in large cities could be attacked by a worm to essentially create a chain reaction attack against a smart city's infrastructure.

In a similar vein, one forecaster believes that 2017 will see a potential rise of the Wi-Fi worm, something that was first proof-of-concepted in 2014. "Basically, an infected device would contain code that attempts to copy itself to routers via Wi-Fi connections. Once a router becomes infected, the worm then attempts to find and replicate itself to more routers," says Sean Sullivan, security advisor for F-Secure. "A Wi-Fi worm is a logical extension of what we've seen with Mirai, and I think current technologies and tactics have put this within reach."

(6) Containerization Can't Contain Breaches

With the rise of DevOps and increasingly automated IT provisioning, containerization has rocketed into the limelight within developer circles. But for the most part, containerization has been contained to development and test environments. That is going to change, says Rick Fitz, senior vice president of IT markets for Splunk. "The reluctance to run containers in production environments will stop meeting resistance next year thanks to the maturation of tools such as Mesos container management and Kubernetes orchestration," Fitz says. "Running container-based apps in production will move the benefits of microservices from promise to actualization." With that change, expect containerization to grow as an attack vector. 2017 will likely bear that out, says Tyler Reguly, manager of software development at Tripwire, who predicts that at least one major breach will be caused due to some kind of containerization problem.

(7) Minority Report: Infosec Edition

Machine learning and behavioral analytics have been the holy grail of detection and prevention technologies over the past five years. According to some, the capabilities in this arena have greatly advanced lately. "Math, machine learning and artificial intelligence will be baked more into security solutions. Security solutions will learn from the past, and essentially predict attack vectors and behavior based on that historical data," says Cunningham, who is director of cyber operations for A10. "This means security solutions will be able to more accurately and intelligently identify and predict attacks by using event data and marrying it to real-world attacks."

(8) JScript Takes 'The Most Attacked' Mantle From Flash

The more things change, the more they stay the same. And according to at least one expert, a drift away from Flash could put JScript in the spotlight for all the wrong reasons. "As Flash phases out, JScript will take its place as the leading browser-exploitation vector. Attackers will continue to use browsers as their first choice of attack vehicle. After all, browser exploitation is still the most convenient attack vector since it requires less manual intervention and easily hits the masses," says Udi Yavo, CTO and founder of enSilo.

The Biggest Security Threats Coming in 2017

https://www.wired.com/2017/01/biggest-security-threats-coming-2017/

[with thanks to the staff at WIRED Magazine] Whether it was a billion compromised Yahoo accounts or state-sponsored Russian hackers muscling in on the US election, this past year saw hacks of unprecedented scale and temerity. And if history is any guide, next year should yield more of the same. It's hard to know

for certain what lies ahead, but some themes began to present themselves toward the end of 2016 that will almost certainly continue well into next year. And the more we can anticipate them, the better we can prepare. Here's what we think 2017 will hold.

(1) Consumer Drones Get Weaponized

Given how frequently the US has used massive flying robots to kill people, perhaps it's no surprise that smaller drones are now turning deadly, too - this time in the hands of America's enemies. In October the New York Times reported that in the first known case, US-allied Kurdish soldiers were killed by a small drone the size of a model airplane, rigged with explosives. As drones become smaller, cheaper, and more powerful, the next year will see that experiment widened into a full-blown tactic for guerrilla warfare and terrorism. What better way to deliver deadly ordnance across enemy lines or into secure zones of cities than with remote-controlled accuracy and off-the-shelf hardware that offers no easy way to trace the perpetrator? The US government is already buying drone-jamming hardware. But as with all IEDs, the arms race between flying consumer grade bombs and the defenses against them will likely be a violent game of cat-and-mouse.

(2) Another iPhone Encryption Clash

When the FBI earlier this year demanded that Apple write new software to help crack its own device - the iPhone 5c of dead San Bernardino terrorist Rizwan Farook - it fired the first shots in a new chapter of the decades-long war between law enforcement and encryption. And when it backed off that request, saying it had found its own technique to crack the phone, it only delayed any resolution. It's only a matter of time until the FBI or other cops make another legal demand that an encryption-maker assist in cracking its protections for users, setting the conflict in motion again. In fact, in October the FBI revealed in October that another ISIS-linked terrorist, the man who stabbed ten people in a Minnesota mall, used an iPhone. Depending on what model iPhone it is, that locked device could spark Apple vs. FBI, round two, if the bureau is determined enough to access the terrorist's data. (It took three months after the San Bernardino attack for the FBI's conflict with Apple to become public, and that window hasn't passed in the Minnesota case.) Sooner or later, expect another crypto clash.

(3) Russian Hackers Run Amok

Two months have passed since the Office of the Director of National Intelligence and the Department of Homeland Security stated what most of the private sector cybersecurity world already believed: That the Kremlin hacked the American election, breaching the Democratic National Committee and Democratic Congressional Campaign Committee and spilling their guts to WikiLeaks. Since then, the White House has promised a response to put Russia back in check, but none has surfaced. And with less than a month until the inauguration of Putin's preferred candidate - one who has buddied up to the Russian government at every opportunity and promised to weaken America's NATO commitments - any deterrent effect of a retaliation would be temporary at best. In fact, the apparent success of Russia's efforts - if, as CIA and FBI officials have now both told the Washington Post, Trump's election was the hackers' goal - will only embolden Russia's digital intruders to try new targets and techniques. Expect them to replicate their influence operations ahead of elections next year in Germany, the Netherlands, and France, and potentially to even try new tricks like data sabotage or attacks on physical infrastructure.

(4) A Growing Rift Between the President and the Intelligence Community

Though the US intelligence community - including the FBI, NSA, and CIA - has unanimously attributed multiple incidents of political hacking to Russian government-sponsored attackers, President-elect Donald Trump has remained skeptical. Furthermore, he has repeatedly cast doubt on digital forensics as an intelligence discipline, saying things like, "Once they hack, if you don't catch them in the act you're not going to catch them. They have no idea if it's Russia or China or somebody." Trump has also caused a stir by declining daily intelligence briefings. Beyond just the current situation with Russia, Trump's casual dismissal of intelligence agency findings is creating an unprecedented dissonance between the Office of the President and the groups that bring it vital information about the world. Current and former members of the intelligence community told WIRED in mid-December that they find Trump's attitude disturbing and deeply concerning. If the President-elect permanently adopts this posture, it could irrevocably hinder the role of intelligence agencies in government. President Obama, for one, says he is hopeful that the situation is temporary, since Trump has not yet felt the full responsibility of the presidency. "I think there is a sobering process when you walk into the Oval Office," Obama said recently in a press conference. "There is just a whole different attitude and vibe when you're not in power as when you are in power." If Trump does eventually embrace the intelligence community more fully, the next question will be whether it can move on from what has already transpired.

(5) DDoS Attacks Will Crash the Internet Again (And Again, And Again)

This was the year of Internet of Things botnets, in which malware infects inconspicuous devices like routers and DVRs and then coordinates them to overwhelm an online target with a glut of internet traffic, in what's known as a disrupted denial of service attack (DDoS). Botnets have traditionally been built with compromised PCs, but poor IoT security has made embedded devices an appealing next frontier for hackers, who have been building massive IoT botnets. The most well-known example in 2016, called Mirai, was used this fall to attack and temporarily bring down individual websites, but was also turned on Internet Service Providers and internet-backbone companies, causing connectivity interruptions around the world. DDoS attacks are used by script kiddies and nation states alike, and as long as the pool of unsecured computing devices endlessly grows, a diverse array of attackers will have no disincentive from turning their DDoS cannons on internet infrastructure. And it's not just internet connectivity itself. Hackers already used a DDoS attack to knock out central heating in some buildings in Finland in November. The versatility of DDoS attacks is precisely what makes them so dangerous. In 2017, they'll be more prevalent than ever.

(6) Ransomware Expands Its Targets

Ransomware attacks have become a billion-dollar business for cybercriminals and are on the rise for individuals and institutions alike. Attackers already use ransomware to extort money from hospitals and corporations that need to regain control of their systems quickly, and the more success attackers have, the more they are willing to invest in development of new techniques. A recent ransomware version called Popcorn Time, for example, was experimenting with offering victims an alternative to paying up - if they could successfully infect two other devices with the ransomware. And more innovation, plus more disruption, will come in 2017. Ransomware attacks on financial firms have already been rising, and attackers may be emboldened to take on large banks and central financial institutions. And IoT ransomware could crop up in 2017, too [it has already attacked a smart TV]. It may not make sense for a surveillance camera, which might not even have an interface for users to pay the ransom, but could be effective for devices that sync with smartphones or tie in to a corporate network. Attackers could also demand money in exchange for ceasing an IoT botnet-driven DDoS attack. In other words, ransomware attacks are going to get bigger in every possible sense of the word.

If you read this all the way to the end (13 Word pages) – thanks for your intellectual curiosity and your patience. Belated Happy New Year!

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 Technology, Innovation and Citizens' Services
4000 Seymour Place, Victoria, BC V8X 4S8
http://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/information-security-awareness

OCIOSecurity@gov.bc.ca