BRITISH COLUMBIA OCIO Office of the Chief Information Officer

The Security Professionals are always at work protecting systems and information, troubleshooting, innovating, and anticipating what is to come in the world of cybercrime. Many put together their Lists at the end of the year – the biggest breaches of the past year, and predictions for the year ahead. Who doesn't love Lists! Here are some chosen Lists for your education and your reading pleasure.

Security News Digest

Special Edition – The Lists for 2017/2018

A Look Back and A Look Ahead

Looking Back: Security Realities in 2017

The Hacks that Left Us Exposed in 2017

http://money.cnn.com/2017/12/18/technology/biggest-cyberattacks-of-the-year/index.html

[By Selena Larson] It was the year nothing seemed safe. Bombshell hacks were revealed one after another in 2017, from an Equifax breach that compromised almost half the country to global ransom campaigns that cost companies millions of dollars. The cyberattacks highlighted the alarming vulnerability of our personal information. More tools used by government hackers have become public, and it's easier than ever to create sophisticated ways to spread malware or ransomware or steal data from companies. Companies also frequently fail to patch security flaws in a timely manner. And there's more to come. "As we do more and more of our business online, and as criminals realize the value of the data that organizations are protecting, we're seeing more big-name breaches, more high-profile breaches," says Mark Nunnikhoven, vice president of cloud research at the security company Trend Micro. Here's a look back at the major hacks of 2017.

(1) Equifax.

Cybercriminals penetrated Equifax, one of the largest credit bureaus, in July and stole the personal data of 145 million people. It was considered among the worst breaches of all time because of the amount of sensitive information exposed, including Social Security numbers. The company only revealed the hack two months later. It could have an impact for years because the stolen data could be used for identity theft. The Equifax breach raised concerns over the amount of information data brokers collect on consumers, which can range from public records to mailing addresses, birth dates and other personal details. Firms like Equifax, TransUnion and Experian sell that data to customers, such as banks, landlords and employers, so they can learn more about you. Whether data brokers do enough to keep that private information secure is under scrutiny. Former Equifax CEO Richard Smith, who stepped down after the breach was revealed, testified to Congress and blamed the security failure on one person who had since been fired. The public still doesn't know who is responsible for the hack.

(2) A Yahoo Bombshell.

Parent company Verizon announced in October that every one of Yahoo's 3 billion accounts was hacked in 2013 - three times what was first thought. In November, former Yahoo CEO Marissa Mayer told Congress that the company only found out about the breach in 2016, when it reported that 1 billion accounts were hacked. The company still does not know who was responsible. Separately, a Canadian hacker pleaded guilty this year to his role in another major Yahoo security breach from 2014. That one compromised 500 million Yahoo accounts. He will be sentenced in February.

(3) Leaked Government Tools.

In April, an anonymous group called the Shadow Brokers leaked a suite of hacking tools widely believed to belong to the National Security Agency. The tools allowed hackers to compromise a variety of Windows servers and Windows operating systems, including Windows 7 and Windows 8. Microsoft said it had released patches for the security holes in March. But many businesses had not patched their software. The tools Shadow Brokers leaked were then used in the year's biggest global cyberattacks, including WannaCry. In March, WikiLeaks released documents that claimed to describe hacking tools created by the CIA. Researchers found that many of the exploits were old and imitated hacks that were made public years ago. One tool, according to the documents, was malware that allowed the CIA to listen to targets through Samsung smart TVs, even while the TV was in a "fake off" mode.

(4) WannaCry.

WannaCry, which spanned more than 150 countries, leveraged some of the leaked NSA tools. In May, the ransomware targeted businesses running outdated Windows software and locked down computer systems. The hackers behind WannaCry demanded money to unlock files. More than 300,000 machines were hit across numerous industries, including health care and car companies. There was a human cost: In Britain, hospitals with locked computers were forced to close temporarily. One patient told CNN his cancer surgery was delayed. Nunnikhoven, from Trend Micro, says it's an example of an Internet of Things hack with major consequences. The Internet of Things refers to everyday devices, beyond traditional computers and phones, that connect to the internet. The WannaCry infections were so bad that, in an unusual move, Microsoft released a patch for Windows systems that it had stopped updating. The cyberattack has been linked to North Korea.

(5) NotPetya.

In June, the computer virus NotPetya targeted Ukrainian businesses using compromised tax software. The malware spread to major global businesses, including FedEx, the British advertising agency WPP, the Russian oil and gas giant Rosneft, and the Danish shipping firm Maersk. This virus also spread by leveraging a vulnerability leaked by the Shadow Brokers. In September, FedEx attributed a $300 million loss to the attack. The company's subsidiary TNT Express had to suspend business.

(6) Bad Rabbit.

Another major ransomware campaign, called Bad Rabbit, infiltrated computers by posing as an Adobe Flash installer on news and media websites that hackers had compromised. Once the ransomware infected a machine, it scanned the network for shared folders with common names and attempted to steal user credentials to get on other computers. The ransomware, which hit in October, mostly affected Russia, but experts saw infections in Ukraine, Turkey and Germany. It served as a reminder that people should never download apps or software from pop-up advertisements or sites that don't belong to the software company.

(7) Voter Records Exposed.

In June, a security researcher discovered almost 200 million voter records exposed online after a GOP data firm misconfigured a security setting in its Amazon cloud storage service. It was the latest in a string of major breaches stemming from insecure Amazon servers where data is stored. They are secure by default, but Chris Vickery, a researcher at cybersecurity firm UpGuard, regularly finds that companies set it up wrong. Verizon and the U.S. Department of Defense also had data exposed on Amazon servers.

(8) Hacks Target School Districts.

The U.S. Department of Education warned teachers, parents, and K-12 education staff of a cyberthreat that targeted school districts across the country in October. In one Montana school district, parents and students feared for their safety after a hacker group sent threatening text messages as a part of an extortion campaign. The group, dubbed The Dark Overlord, stole information on students, teachers and other district employees. They asked for money to destroy the files. Schools closed for three days. The same group was responsible for stealing information from Netflix's production partners and leaking episodes of Netflix's "Orange is the New Black" after the company refused to pay ransom.

(9) An Uber Cover-Up.

In 2016, hackers stole the data of 57 million Uber customers, and the company paid them $100,000 to cover it up. The breach wasn't made public until this November, when it was revealed by new Uber CEO Dara Khosrowshahi. Now Uber is facing questions from lawmakers. Three senators introduced a bill that could make executives face jail time for knowingly covering up data breaches. City attorneys in Los Angeles and Chicago and the Washington state attorney general are suing Uber over the breach.

2017 Biggest Data Breaches

https://www.scmagazine.com/2017-biggest-data-breaches/article/720104/

[By Doug Olenick, Online Editor, SC Media]

June – Hackers accessed 8tracks's user database and pilfered information, including email addresses and encrypted passwords, from at least 18 million accounts signed up for the Internet radio service using email.

June – User data on 6 million subscribers to the cash-for-surveys site CashCrate was compromised. User data going back 10 years – including email addresses, names, passwords and street addresses – was stolen in the breach.
July – A third-party vendor working with Verizon left the data of as many as 14 million U.S. customers exposed on a misconfigured server.
July– A misconfigured database on an Amazon S3 server may have exposed the data of between 2 2 million and 4 million Dow Jones & Co. customers.
August – Personal data on more than 1.8 million Chicagoan voters was exposed on a cloud-based storage site, available to anyone for downloading.
September – Four million Time Warner Cable, now known as Spectrum, customers had their information compromised when a third-party vendor misconfigured an Amazon S3 Bucket.
September – Cybercriminals gained unauthorized access to Equifax files in a breach that affected about 143 million consumers in the U.S. In October Equifax reported an additional 2.5 million people were involved bringing the total to 145.5 million.
September – A misconfigured CouchDB containing information on 593,328 Alaskan voters was found opened to the public exposing the data.
October – Yahoo upped number of breached members to 3 billion. Verizon, which purchased Yahoo in 2017, then reported that a 2013 breach of Yahoo!'s network affected all three billion of the company's accounts.
October – A Disqus breach exposes info on 17.5 million users between 2007-2012.
October – The online image sharing website We Heart It told its members that more than 8 million of its accounts were compromised in a data breach that took place four years ago.

The 12 Biggest Hacks, Breaches, and Security Threats of 2017

https://www.pcworld.com/article/3243108/security/biggest-hacks-security-breaches-2017.html
[By Ian Paul, Contributor, PCWorld] Security issues took a turn for the serious in 2017. This time around we still suffered the password breaches, malware annoyances, and stolen credit card numbers that have become commonplace in recent years. But the headlines were dominated by more sobering issues. We saw foreign adversaries trying to infiltrate critical infrastructure; major U.S. government hacking tools exposed; a major breach that called into question the use of social security numbers as identification; the U.S. government turning negative towards online user privacy; and popular consumer software dragged into the world of corporate and state espionage.
Whew. It was a big year for computer security, and some of 2017's events will no doubt reach well into 2018 and beyond. Let's take a look.

(1) Shadow Brokers and Vault7 leaks.

Two of the defining computer security events of 2017 were leaks that exposed closely held hacking secrets of the U.S. government. Wikileaks got the ball rolling in March with the release of its so-called "Vault7" leaks revealing what appeared to be a cache of computer vulnerabilities and operating methods used by the Central Intelligence Agency to infiltrate target devices. Then in April the Shadow Brokers - an anonymous group of hackers that first came to notoriety in 2016 - released a trove of attack tools linked to the National Security Agency. Both releases would have significant impacts on computer device security.

(2) Equifax Breach.

"Jaw-dropping" does not begin to describe the Equifax breach, which came to light in September. Equifax is one of the three major consumer credit reporting agencies in the United States. The hackers struck in the spring, seizing 143 million Social Security numbers - that's more than half of the U.S. population. A failure to install current security patches on its network opened the door to the attack, the company said. Despite the devastating hack Equifax still won an anti-fraud contract from the Internal Revenue Service, though it was later suspended.

(3) ISP Tracking Rules.

In late March, Congress decided to remove the privacy rules passed by the Federal Communications Commission in 2016. The rules had not yet come into effect when they were dumped, but they would have required opt-in permission from broadband customers before ISPs could use their personal information and browsing habits for marketing or analytics purposes. Republicans said the rules unfairly hamstrung Internet Service Providers, while major Internet companies could collect and use all the personal data they wanted. What that argument ignores, however, is that ISP data collection is much harder to mitigate since it controls the very wires and cables you need to get online. Plus, few people are particularly pleased that Facebook and Google have free reign, either.

(4) CCleaner Gets a Backdoor.

In September, security researches at Cisco Talos discovered malicious code buried inside CCleaner, a popular Windows PC utility. The malware was designed to steal personal data from infected machines. Avast added to the intrigue when it discovered that there was a second stage to the malware for infected machines in specific companies such as Cisco, Sony, and HTC. Presumably, the malware was looking to steal company secrets in those organizations. All in all around two million people were believed to be affected by the corrupted versions of CCleaner. The malware has since been removed from the latest versions of the software.

(5) Kaspersky Controversy.

If there's a headline-grabbing computer security controversy of 2017, it has to be the allegation that Kaspersky Anti-virus products are a spying tool for Russian intelligence. In October, *The Wall Street Journal* said hackers working for the Russian government used Kaspersky Anti-Virus to identify and target a National Security Agency contractor in order to steal American hacking secrets. Kaspersky vigorously denied the claims and said the contractor caused the leak by running Kaspersky on a home machine that contained weaponized malware. To help allay fears, Kaspersky announced it would allow third-parties to audit its code - a measure that some experts argue doesn't go far enough. As a result of the reports, and bans of Kaspersky products by the government, Kaspersky's Washington DC office shut down in December, the contractor who brought U.S. hacking secrets home in the first place plead guilty to taking classified documents, and Kaspersky sued the Department of Homeland Security over blacklisting its products.

(6) Game of Leaks.

It's not easy being a fount of popular TV shows - especially when everyone wants to know what you have planned. HBO found that out the hard way in July when hackers claimed to have purloined 1.5 terabytes of data from the pay TV channel. Among the stolen cache were management emails, upcoming episodes for popular HBO shows, and draft scripts of one *Game of Thrones* episode that had not yet been aired. In November, U.S. law enforcement charged an Iranian hacker with the data theft. As for HBO, now it understands that when it comes to computer security you win or you leak.

(7) Yahoo's 2016 Hacks Gets Worse.

Oh boy. Before Yahoo was absorbed into Verizon the Internet giant endured a massive hack exposing usernames and passwords. In fact, it was a record-breaking hack twice over in 2016, but even that wasn't the end of the saga. The company recently amended the number of Yahoo accounts affected by the data breach dating from 2013. By the end of 2016, that number was believed to be one billion accounts, but in October Yahoo updated that number to three billion. Basically, if you had a Yahoo account at any time in 2013, your username and password leaked, once again driving home the importance of using unique passwords for every website.

(8) Ransomware Makes You WannaCry.

In May, a piece of ransomware called WannaCry made a second appearance after first rearing its head in March. The May attacks were more problematic since WannaCry included a "worm-like component" that helped spread the malware. That component was particularly notable since it was derived from an exploit called EternalBlue that was part of the ShadowBrokers leaks in April. The WannaCry attack was so successful because the EternalBlue exploit had either not been patched in a timely manner on infected machines, or the machines were too outdated to receive exploit patches. The WannaCry infection was so pernicious that Microsoft released patches for Windows XP, Windows Server 2013, and Windows 8. The ransomware was eventually halted in May when British security researcher Marcus Hutchins inadvertently discovered a kill switch for the malware. EternalBlue would also appear in NotPetya, another piece of notable ransomware that grabbed headlines in 2017.

(9) Cloudbleed.

Content Delivery Network Cloudflare ended up with a significant bug in February 2017 that affected the way the company parsed HTML. The company often takes regular HTTP webpages from its client websites and turns them into the more secure HTTPS pages. The parser can also carry out tasks such as hiding content from bots, hiding email addresses, and working with Google's AMP system. But the parser system also had a flaw that could potentially leak sensitive information some of which was cached by search engines such as Bing and Google. That sensitive information included items like private messages from dating sites, text chats from popular messaging services, password manager data, and hotel bookings. While the technical causes were different, the results of the Cloud Flare bug were similar to the Heartbleed bug from 2014.

(10) Voters Exposed.

Servers are tricky things. Not only do they have to be patched to keep the bad guys out, but you also have to be careful of misconfigurations that expose private data. A data firm called Deep Root Analytics found that out in June when one of its Amazon S3 servers was misconfigured and exposed the personal information for 198 million voters, according to *Wired*. The misconfigured server was discovered by a security analyst, and presumably the data never fell into malicious hands. Even if it had, the risk might have been minimal. *Wired* noted in a follow-up report that most of the personal data exposed in the flaw could also be accessed from public records.

(11) HP Laptops with Keyloggers.

For HP, 2017 was the year of the keylogger. It all started in May when a Swiss security firm discovered that more than two dozen “HP laptop models were recording users’ keystrokes.” The keylogging software was in the PC’s audio driver existing since at least 2015. The driver was supposed to be alerted when a particular key on the PC was hit, but to do that the driver was capturing *all* keystrokes. Those keystrokes were also stored in an unencrypted file. Potentially exposing passwords, usernames, and private correspondence should the user get hacked. More recently in December, another security researcher found a keylogger in the Synaptics touchpad driver for nearly 500 models of HP notebooks going back to 2012. Luckily, the December keylogger was disabled by default, and in both cases the installation of the keylogger appeared to be either inadvertent or a mistake.

(12) Power Outage Ukraine.

In January 2017, security researchers concluded that hackers caused a power outage in Ukraine during December 2016 - one of the country’s coldest months. This was the second time a ‘cyber attack’ had triggered a power outage in the country. Power outage hacks sound scary and bring up the obvious question of whether they could happen in the U.S. The answer to that is yes, it could. In fact, attacks against American infrastructure have already happened. In mid-December, Reuters reported that hackers had broken into the safety system of an unnamed “critical infrastructure facility.” Before that, in September, Symantec warned that foreign hackers were actively targeting European and American energy facilities, and in some cases had operational access, as reported by Reuters. And oh, yeah, hackers are also targeting American nuclear facilities.

Happy New Year!

Looking Ahead: Security Predictions for 2018

Top Five Trends IT Security Pros Need to Think About Going into 2018

https://www.imperva.com/blog/2017/12/top-five-trends-it-security-pros-need-to-think-about-going-into-2018/

[By Terry Ray at Imperva]   Equipped with Imperva’s own research, interactions with our customers, and a wealth of crowdsourcing data analyzed from installations around the world, we’ve looked ahead to the future of cybersecurity and compiled a few significant trends IT security pros can expect to see in 2018.

(1) Massive Cloud Data Breach.

Companies have moved to cloud data services faster than anticipated even in traditional industries like banking and healthcare where security is a key concern. Take-up of cloud computing will continue to increase, attaining a compound annual growth rate (CAGR) of 19%, from $99B in 2017 to $117B in 2018. In 2018, in parallel with the take-up of cloud computing, we’ll see massive cloud data breaches - primarily because companies are not yet fully aware of the complexities involved with securing cloud data.

Data Breaches: A Troubling Past, A Worrying Future: It is estimated that in 2017 alone, over 99 billion records were exposed because of data breaches. Of the various circumstances behind the breaches, hacking of IT systems is by far the most prevalent cause, followed by poor security, inside jobs, and lost or stolen hardware and media.

Major breaches at healthcare and financial services companies indicate a growing trend of vulnerabilities and exploits in these two vital business sectors. Healthcare was one of the hardest hit sectors in 2017, and that trend is expected to worsen in the coming year. Some 31 million records were stolen, accounting for 2% of the total and up a whopping 423% from just 6 million. The financial services industry is the most popular target for cyber attackers and this dubious distinction is likely to continue in the upcoming year. Finance companies suffered 125 data breaches, 14% of the total, up 29% from the previous six months. Data breaches in various other industries totaled 53, up 13% and accounting for 6% of the total. The number of records involved in these attacks was a staggering 1.34 billion (71% of the total) and significantly up from 14 million. It is estimated that the average cost of a data breach will be over $150 million by 2020, with the global annual cost forecast to be $2.1 trillion.

Critical Cloud-based Security Misconfigurations: Missteps in cloud-based security configurations often lead to data breaches. This is likely to increase as more organizations move some or most of their operations to the cloud. As organizations and business units migrate to public cloud services, centralized IT departments will find it increasingly difficult to control their company's IT infrastructure. These enterprises lack the visibility necessary to manage their cloud environments and don't have the monitoring tools to detect and report on security governance and compliance. Many are not even aware of the specific workloads they've migrated to the cloud. And without a doubt, you can't secure what you can't see. For example, an unsecured Amazon Web Services S3 storage bucket has been an ongoing concern for cloud users. The bucket, which can be configured to allow public access, has in the past leaked highly sensitive information. In one instance of a major security breach, a whopping 111 GB worth was exposed, affecting tens of thousands of consumers. Most significantly, Amazon is aware of the security issue, but is not likely to mitigate it since it is caused by cloud-user misconfigurations.

(2) Cryptocurrency Mining.

We expect to see a growth of cryptocurrency mining attacks where attackers are utilizing endpoint resources (CPU/GPU) [translation: using people's computers without their consent or their awareness] to mine cryptocurrency either by cross-site scripting (XSS) or by malware. It's increasingly likely that remotely vulnerable/hackable IoT devices will also be used as a mining force to further maximize an attacker's profits. Illegal mining operations set up by insiders, which can be difficult to detect, are also on the rise - often carried out by employees with high-level network privileges and the technical skills needed to turn their company's computing infrastructure into a currency mint. These attacks will quickly grow in popularity given their lucrative nature. As long as there is a potential windfall involved, such inside jobs are likely to remain high on the list of cybersecurity challenges faced by companies. Although attacks that attempt to embed crypto-mining malware are currently unsophisticated, we expect to see an increase in the sophistication of attacks as word gets out that this is a lucrative enterprise. We also expect these attacks to target higher-traffic websites, since the potential to profit increases greatly with higher numbers of concurrent site visitors.

(3) Malicious Use of AI/Deception of AI Systems.

The malicious use of artificial intelligence (AI) will continue to grow quickly. The industry has started to see early traces of attackers leveraging AI to learn normal behavior and mimic that behavior to bypass current user and entity behavior analytics (UEBA) solutions. It's still very early stage and will continue to mature beyond 2018. However, it will force current UEBA vendors to come up with a 2.0 approach to identifying anomalous behavior. AI and internet of things (IoT) use cases drive cloud adoption. Artificial intelligence in the cloud promises to be the next great disrupter as computing is evolving from a mobile-first to an artificial intelligence-first model. The proliferation of cloud-based IoT in the marketplace continues to drive cloud demand, as cloud allows for secure storage of massive amounts of structured and unstructured data central to IoT core functions. Without proper awareness and security measures, AI can be easily fooled by adversarial behavior. In 2018 we will see more: Attacks on AI systems (for example, self-driving cars), and Cyber attackers who adapt their attacks to bypass AI-based cybersecurity systems.

(4) Cyber Extortion Targets Business Disruption.

Cyber extortion will be more disruption focused. Encryption, corruption, and exfiltration will still be the leaders in cyber extortion, but disruption will intensify this year, manifesting in disabled networks, internal network denials of service, and crashing email services. In the last few years, attackers have adopted a "traditional" ransomware business model - encrypt, corrupt or exfiltrate the data and extort the owner in order to recover the data or prevent it from leaking. Fortunately, techniques such as deception or machine learning have helped to prevent these types of attacks and made it more difficult for attackers to successfully complete a ransomware attack. From a cost perspective, most of the damage associated with ransomware attacks is not the data loss itself, since many firms have backups, but the downtime. Often in the case of ransomware, attackers will start to leverage a disrupt-and-extort method. DDoS is the classic and most familiar one, but attackers will probably adopt new techniques. Examples include shutting down an internal network (web app to a database, point-of-sale systems, communication between endpoints, etc.), modifying computer configuration to cause software errors, causing software crashes, system restarts, disruption of your corporate email or disruption of any other infrastructure which is mandatory for an organization's employees and/or customers day-to-day functions. Basically, any event that leaves the company unable to conduct business.

While absolute protection is impossible, you can help lower your chance of business interruption due to a cyber-attack. Start by creating a formal, documented risk management plan that addresses the scope, roles, responsibilities, compliance criteria and methodology for performing cyber risk assessments. This plan should include a characterization of all systems used at the organization based on their functions, the data they store and process, and their importance to the organization.

(5) Breach by Insiders.

Businesses are relying more on data which means more people within the business have access to it. The result is a corresponding increase in data breaches by insiders either through intentional (stealing) or unintentional (negligent) behavior of employees and partners. While the most sensational headlines typically involve infiltrating an ironclad security system or an enormous and well-funded team of insurgents, **the truth of how hackers are able to penetrate your system is more boring: it's your employees**. A new IT security report paints a bleak picture of the actual gravity of the situation. Researchers found that IT workers in the government sector overwhelmingly think that employees are actually the biggest threat to cybersecurity. In fact, 100% of respondents said so. Fortunately, security-focused companies have begun identifying these traditionally difficult to detect breaches using data monitoring, analytics, and expertise. The difference being that in 2018, more companies will invest in technology to identify this behavior where previously they were blind.

In fact, 75% of IT employees in government reported that rather than their organization having dedicated cybersecurity personnel on staff (which is becoming more and more necessary with each passing year), an overworked IT team was left to deal with security and employee compliance. As a result, 57% reported that they didn't even have enough time to implement stronger security measures while 54% cited too small of a budget. Here's another fact for you: insider threats are the cause of the biggest security breaches out there, and they are very costly to remediate. According to a 2017 Insider Threat Report, 53% of companies estimate remediation costs of $100,000 and more, with 12% estimating a cost of more than $1 million. The same report suggests that 74% of companies feel that they are vulnerable to insider threats, with seven percent reporting extreme vulnerability.

These are the steps every company should take to minimize insider threats: Background checks, Watch employee behavior, Use the principle of least privilege, Control user access, Monitor user actions, and Educate employees. Insider threats are one of the top cybersecurity threats and a force to be reckoned with. Every company will face insider-related breaches sooner or later regardless of whether it is caused by a malicious action or an honest mistake. And it's much better to put the necessary security measures in place now than to spend millions of dollars later.

5 Information Security Threats that Will Dominate 2018

https://www.cio.com/article/3237784/security/5-information-security-threats-that-will-dominate-2018.html

[By Thor Olavsrud Senior Writer, CIO] If you thought 2017 was a dire year for data breaches, wait until 2018. The Information Security Forum (ISF), a global, independent information security body that focuses on cyber security and information risk management, forecasts an increase in the number and impact of data breaches, thanks in large part to five key global security threats that organizations will face in 2018.

(1) Crime-as-a-Service (CaaS) – will expand available tools and services.

Last year, ISF predicted CaaS would take a quantum leap forward, with criminal syndicates further developing complex hierarchies, partnerships and collaborations that mimic large private sector organizations. Steve Durbin, managing director of the ISF says that prediction proved prescient, as 2017 has seen a "huge increase in cybercrime, particularly crime-as-a-service." The ISF predicts that process will continue in 2018, with criminal organizations further diversifying into new markets and commodifying their activities at a global level. Some organizations will have roots in existing criminal structures, the ISF says, while others will emerge that are focused solely on cybercrime. The biggest difference? In 2018, CaaS will allow "aspirant cybercriminals" without much technical knowledge to buy tools and services that allow them to conduct attacks they would otherwise not be able to undertake.

(2) The Internet of Things (IoT) - will further add unmanaged risks.

Organizations are increasingly adopting IoT devices, but most IoT devices are not secure by design. Additionally, the ISF warns there will be an increasing lack of transparency in the rapidly evolving IoT ecosystem, with vague terms and conditions that allow organizations to use personal data in ways customers did not intend. On the enterprise side, it will be problematic for organizations to know what information is leaving their networks or what data is being secretly captured and transmitted by devices like smartphones and smart TVs. When data breaches do occur, or transparency violations are revealed, organizations are likely to be held liable by regulators and customers. And in a worst-case scenario, security compromises of IoT devices embedded in industrial control systems could lead to physical harm and death.

(3) The Supply Chain - will remain the weakest link in risk management.

The ISF has been raising the issue of the vulnerability of the supply chain for years. As the organization notes, a range of valuable and sensitive information is often shared with suppliers. When that information is shared, direct control is lost. That means increased risk of compromise of that information's confidentiality, integrity or availability. "Last year we started to see big manufacturing organizations losing manufacturing capability because they were locked out and their supply was being affected," Durbin says. "It doesn't matter what line of business you're in. We all have supply chains," he adds. "The challenge we face is how do we really know where our information is at each and every stage of the lifecycle? How do we protect the integrity of that information as it's being shared?" In 2018, organizations will need to focus on the weakest spots in their supply chains, the ISF says. While not every security compromise can be prevented ahead of time, you and your suppliers will have to be proactive. Durbin recommends adopting strong, scalable and repeatable processes with assurance proportional to the risk faced. Organizations must embed supply chain information risk management within existing procurement and vendor management processes.

(4) Regulation (GDPR) - will add to the complexity of critical asset management.

Regulation adds complexity, and the sweeping European Union General Data Protection Regulation (GDPR) will come online in early 2018, adding another layer of complexity to critical asset management. "There probably isn't a conversation that I have with anybody, anywhere in the world in which GDPR isn't touched on," Durbin says. "It isn't just about compliance. It's about making sure you have the ability across your enterprise and supply chain at any point in time to be able to point to personal data and understand how it's being managed and protected. You have to be able to demonstrate that at any point in time, not just by regulators, but by the individual."

(5) Unmet board expectations - will be exposed by major incidents.

Misalignment between the board's expectations and the reality of the information security function's ability to deliver results will pose a threat in 2018, according to the ISF. … The ISF says boards will expect that their approval of increased information security budgets in past years will have enabled the CISO and information security function to produce immediate results. But a fully secure organization is an unattainable goal. And even if they understand that, many boards don't understand that making substantial improvements to information security takes time - even when the organization has the correct skills and capabilities in place. This misalignment means that when a major incident does occur, it won't just be the organization that feels the effects; it's likely to reflect badly on the reputations of board members, both individually and collectively. Because of this, the CISO role must evolve, Durbin says. "The role of the CISO these days is to anticipate, not to make sure the firewall stays up," he says. "You have to anticipate how the challenges coming down the road will affect the business and articulate that to the board. A good CISO needs to be a salesman and a consultant. You can't not have both. I can be the best consultant in the world, but if I can't sell my ideas to you, it's not going to go anywhere in the board room."

3 Cybersecurity Predictions for 2018

https://www.hackread.com/3-cybersecurity-predictions-2018/

[By Carolina at HackRead] The rise of new forms of technology is creating new threats to our privacy, financial information, and personal possessions. And hackers are ready and willing to exploit any gap they can find in any way possible. Here are three cybersecurity predictions for 2018 and beyond. Note that none of these proposals are science fiction because the technology, methodologies, and problems are already seen in various forms in the real world today.

(1) Ransomware Infecting New Targets.

Technology has enabled new forms of control over one’s vehicle. Alcoholics may have breathalyzers connected to the ignition so that they cannot drive if they are not sober. At least one auto lender has tied the ability to start one’s car to making payments so that you lose the ability to drive if your car payment is late. If you start seeing self-driving vehicles, expect to see ransomware target your mobility by demanding payment so your car can take you to work.

(2) Your Data Used Against You.

You could see hackers stealing your online financial information by going not for the Amazon account with its credit card number, but putting up fake “skills” so that when you think you’re ordering pizza, you’re sending money to someone who will never send you food. Hackers could target your financial information in other ways by asking you to verify your account information out loud when you place an order verbally, and many people would share personally identifiable information because they don’t know the system shouldn’t do that.

(3) New Versions of Old Schemes.

We’re seeing new variations of old schemes arising because weak points in the IT infrastructure are being secured. For example, big businesses are better at securing their clients’ financial data, Equifax excepted. Hackers haven’t quit trying to steal financial information from websites but have shifted to small business and non-profit websites that don’t have the same level of security. Those earning an online Masters of Software Development degree will find that it is these small businesses and organizations who are desperate for interactive content but often cannot afford the help they need. Given the rise of intrusion detection software and automated IT security, internal threats and leaks have come back to the fore as a major source of security breaches.

Our Top 7 Cyber Security Predictions for 2018

https://www.csoonline.com/article/3242866/security/our-top-7-cyber-security-predictions-for-2018.html

[From V Michael Nadeau Senior Editor, CSO] Given what’s happened in 2017 - the Equifax breach, state-sponsored attacks, Russian manipulation of social media, WannaCry, and more phishing scams than we can count - you might not be looking forward to 2018. Breaches will be bigger, hackers will be smarter, and security teams and budgets won’t seem to keep pace. There is reason to be optimistic, though. Yes, some things will get worse before they get better, but we expect real progress in a few areas. Here’s what we think will happen next year.

(1) Many, if not most, U.S. companies will not meet GDPR compliance by deadline.

Surveys show that U.S. companies subject to the European Union’s (EU) General Data Protection Regulation (GDPR) are far behind where they need to be to make the May 25 compliance deadline. For some, it might not matter. Regulators will not audit for GDPR compliance, so companies are vulnerable to fines only if there is a breach or EU citizens file complaints. Even if a company experiences a breach or complaint, regulators will likely treat it leniently if the company can document good-faith efforts to comply. Organizations that don’t take GDPR seriously and experience an event that triggers an investigation by regulators are at real risk of a heavy fine. That leads us to our next prediction.

(2) GDPR regulators will quickly make an example of an organization.

There are two schools of thought about whom regulators will target first. Some say they will set a precedent first with an EU company because they are perceived to be less likely to fight a fine. Others believe that regulators will not only go after a U.S. company early, but they have specific companies in mind. It’s not hard to guess which companies they might be. Google, Apple, Amazon, and Facebook have all had contentious relationships with the European Commission on privacy and antitrust issues. If any of these four show signs of non-compliance with GDPR, EU regulators might well seize the opportunity to make a statement. Other companies are not likely to be early targets unless an especially egregious event occurs that could have been prevented or minimized had GDPR rules been followed. The safe plan is to make your best effort to be in compliance by May 25.

(3) The decline of password-only authentication will accelerate.

The Equifax and Anthem breaches were wake-up calls for many consumers, who are now asking questions about the safety of their online accounts. Most still have no idea about password alternatives or enhancements like multi-factor authentication (MFA) or risk-based authentication, but they are more aware that passwords alone no longer are enough. In fact, research done by Bitdefender shows that U.S. citizens are more concerned about stolen identities (79 percent) than email hacking (70 percent) or home break-ins (63 percent). This is important, because companies often cite a lack of demand for stronger authentication as a reason for not offering it. They are reluctant to do so, in part, because they don’t want more complicated authentication degrading the user experience.

That worry will be eased by risk-based authentication tools that are becoming widely available. These tools work in the background to assess behavior and other data to determine the likelihood that the person attempting access is actually authorized. Coupled with MFA, risk-based authentication puts up a strong barrier to unauthorized access. Risk-based authentication is often bundled with identity and access management (IAM) tools. According to Stratistics MRC, the IAM market is projected to grow at a compound annual growth rate of 14.8 percent in 2018, which is another indicator that password-only authentication is headed to extinction.

(4) State-sponsored attacks will increase.

The usual suspects for state-sponsored attacks - North Korea, Iran, and Russia - don’t have much to lose by continuing their attempts to extort, steal, spy and disrupt by infiltrating information systems. All are already heavily sanctioned, and the consequences - at least those we know about - in response to state-sponsored attacks have been minimal. This makes the risk of escalating those attacks seem low. Expect state-sponsored attackers to keep pushing the envelope in terms of scale and impact of their assaults. An area of particular concern is critical infrastructure like power and communications grids. “The progression of cyber attacks driven by nation-states will undoubtedly place critical infrastructure in the crosshairs, potentially leading to widespread outages or exposed personal information that could impact millions of innocent consumers,” stated Experian’s 2017 Data Breach Industry Forecast.

Affected nations and the international community will respond with more pressure on the bad actors. More sanctions and indictments of foreign nationals deemed responsible are likely. “Unfortunately, until there is a clear international agreement regarding rules of engagement in cyberspace, these attacks are likely only going to increase and escalate,” the Experian report stated. State-sponsored attacks might also spur countries to form alliances to fight them. “Increased attacks on critical infrastructure will drive countries to begin discussing cybersecurity alliances. Establishing these alliances will provide mutual defense for all countries involved and it will allow for the sharing of intelligence in the face of attributed nation-state attacks, not to mention agreements to not attack each other,” says Eddie Habibi, CEO of PAS Global. Until effective deterrents are in place, offending nations will escalate their attacks until the cost is too high. That cost might come in the form of in-kind counter-attacks or even some kind of physical strike. Let’s hope we don’t end up with the kind of brinkmanship that kept the world on edge during the Cold War.

(5) Attacks via compromised IoT devices will get worse.

Millions of connected devices have little or no defense against hackers who want to gain control of them. In fact, it’s getting easier for hackers to take over scores of internet of things (IoT) devices. All they have to do is purchase a botnet kit from the dark web and they are in business. The top three botnet kits - Andromeda, Gamarue and Wauchos - are estimated to be responsible for compromising more than a million devices a month. The Reaper botnet has infected more than a million devices. The problem is that we haven’t yet seen what the hackers who control the botnets intend to do with them. Will it be to launch distributed denial of service (DDoS) attacks? Send massive amounts of spam? Or will they do something we haven’t seen before? We’ll find out in 2018. It takes time to build, secure, and set up the command infrastructure for a botnet at a Reaper-like scale. A hacker would not likely invest that kind of effort without expecting a large return. Botnet attacks in 2018 could be very interesting, and not in a good way.

That’s the bad botnet news. The good news is that efforts against botnets are improving. In December, three people pleaded guilty to charges related to their creating and using the Mirai botnet to launch a DDoS attack on DNS service company Dyn. Also in December, ESET and Microsoft announced that they had cooperated to take down 464 botnets and more than 1,200 command and control domains. Also encouraging, an individual believed to be associated with the botnets was arrested in Belarus. International cooperation will be necessary to stop botnets. The Belarus arrest along with the arrest of Peter Levashov, the hacker behind the Waledac and Kelihos spam botnets, in Spain last spring give hope that hackers will have fewer safe havens next year.

IoT device makers are slowly making progress on securing their devices as well. That won’t help the scores of devices already deployed that are difficult or impossible to patch, however. “Manufacturers will start to address these security faults or risk losing to the companies that bake-in security from the start,” says Ken Spinner, VP of field engineering at Varonis. “GDPR may save the day in the long run, forcing businesses to reconsider personal data collection via IoT, but we won’t see this effect until at least 2019."

(6) Automation of some threat-detection tasks will increase.

Security teams wade through massive volumes of alerts and data every day to determine what is or isn’t a likely threat. That volume will increase, driven by more attacks and more attack vectors. Filtering the alert data is repetitive, tedious work, which makes it a perfect candidate to automate using software.

Organizations are already taking advantage of machine-learning-based tools to help filter alerts to lighten the load of over-burdened security staff. We expect this trend to accelerate in 2018 as the volume of threat indicators increase and the security talent pool remains constrained. And why not? Studies have shown that, properly deployed, automation tools are highly effective at identifying which alerts a person needs to look at.

The automation trials that organizations are doing now will give them confidence in the technology and help them understand where it can and can't help. That will encourage security teams to expand the use of automation where it makes sense. Automation will not be a panacea or replace staff, but it will boost threat detection effectiveness and free staff for other important tasks. With the increased use of machine-learning-based automation will come a greater awareness of what it can't do. For example, machine learning is only as good as its model and the data available to analyze. It will likely miss any new type of attack. This better understanding of machine learning and automation will allow security teams to deploy the technology more effectively.

(7) Trust will be a casualty of the war on cyber crime.

Who can blame anyone for mistrusting everything when it comes to cyber security? No one's personally identifiable information (PII) is safe. Companies can't count on the integrity of their suppliers' and partners' security capabilities. The U.S. government is even throwing shade on a leading provider of security software because it's based in Russia. This lack of trust is starting to have a real effect on business that will continue into 2018. Uber did not help matters when it was revealed that the company hid a large breach for a year. It will be harder to engage consumers when they are reluctant to trust companies with their PII. As explained above, this will drive companies to provide stronger authentication.

Expect more companies to demand security audits of their partners, suppliers, and service providers. Third-party breaches are becoming more common, and it shows that any organization's security is only as good as its extended network. It can't assure its customers and employees that their data is safe if they don't know the risk presented by other organizations with which it does business. The U.S. government has banned the use of Kaspersky software in government agencies because it believes the risk of Russian influence to compromise the software too high. Similar actions by other countries are likely in 2018. **"**Other countries have shown similar nationalistic tendencies such as China and its recently passed, far-reaching cybersecurity law that requires access to vendor source code. We predict that the U.S. Executive Branch will show similar tendencies and direct government agencies to exercise procurement preference for vendors with development and manufacturing in the U.S. or allied countries," says PAS Global's Habibi. The environment of mistrust will present opportunities for companies that can show genuine concern for protecting data and that they have proper security infrastructure in place. In other words, earned trust becomes an asset when consumers and other organizations are willing to do business with you because they feel secure doing so.

Forrester's Top 6 Cybersecurity Predictions for 2018

https://www.techrepublic.com/article/forresters-top-6-cybersecurity-predictions-for-2018/

[By Alison DeNisco Rayome at Tech Republic] Last year, Forrester predicted that 2017 would see a cybersecurity crisis for the Trump administration in its first 100 days, that healthcare breaches would become as large and common as retail breaches, that more than 500,000 IoT devices would fall victim to a cyberattack, and that security professionals would increase spending on security services and automation to fill the tech talent gap. All of those predictions came true over the course of the year.

Here are Forrester's six cybersecurity predictions for 2018, and actions that your organization can take to mitigate the risks.

(1) Governments will no longer be the sole providers of reliable, verified identities.

The Equifax breach demonstrated that no single entity - including any government - can safeguard identity data and provide trusted and reliable identity verification for a large number of consumers, especially as customers increasingly engage with businesses through digital channels. Forrester predicts that in 2018, we will see an expansion of identity verification services to large banks such as Bank of America, Capital One, Citi, and Wells Fargo. Researchers also said that customers will be able to use bank-issued credentials to log into government services. Blockchain will also likely emerge to help verify identities based on federated, consortium-based transaction data. **Action:** Evaluate an identity verification service provider as soon as possible. When selecting a solution, Forrester recommends prioritizing support, coverage, compliance, security of data handling, and reputation of the provider.

(2) More IoT attacks will be motivated by financial gain than chaos.
The Mirai botnet that hit in late 2016 demonstrated how hackers can use a botnet army of compromised IoT devices to launch a massive DDoS attack. IoT-based attacks will likely continue to grow in 2018, including those on both devices and cloud backplanes, as hackers try to compromise systems for ransom or to steal sensitive information. Instead of being motivated solely by political, social, or military reasons, cybercriminals will likely be motivated by financial gain moving forward, the report noted. We've seen that these hackers are already exploring the potential for ransomware that targets vehicles, operational technologies, and medical equipment. **Action:** Assess IoT attack vectors, compliance risk, and organizational readiness. Ensure security in existing IoT deployments by conducting assessments of endpoint devices for gaps such as default passwords, weak encryption implementations, and inadequate patching or remediation capabilities.

(3) Cybercriminals will use ransomware to shut down point of sale systems.
Many merchants have updated their payment systems to use end-to-end encryption and prevent criminals from obtaining credit card data from point of sale (POS) systems. This has led criminals to turn to ransomware as a means of monetizing an attack, as opposed to stealing and selling data. Often, victims of ransomware choose to pay the ransom, because they have no other means by which to restore their systems and data. **Action:** Don't pay the ransom. Create strong plans for system and data recovery as soon as possible, including backing up all systems daily.

(4) Cybercriminals will attempt to undermine the integrity of US 2018 midterm elections.
The US has not addressed the systemic vulnerabilities that can be found in its voting systems, which depend on software to cast votes, count them, verify them, and report them, the report stated. "A hacker doesn't need the voting machine to alter results; he could modify the spreadsheet or database that tabulates precinct voting totals, or use compromised Windows machines to adjust the voting tabulation results in web-accessible software," the report stated. Data stolen in the recent breaches of Equifax, the Republican National Committee (RNC), and various state agencies can potentially help criminals commit voter fraud in contested districts, Forrester researchers wrote. **Action:** Volunteer your time to assist precincts, counties, and states with securing a voting system.

(5) Blockchain will overtake AI in VC funding and security vendor roadmaps.
Blockchain offers strong security and encryption, leading security teams to explore ways it can enhance the security of their on-premises and cloud workloads through capabilities like distributed integrity guarantees, tamper detection of policy changes, and transactional integrity. "Forrester predicts blockchain will become a foundational technology for: (1) certificate issuance and authentication; (2) IDV; (3) malware and ransomware protection via binary reputation checks; and (4) document authenticity and integrity verification," the report stated. "Those are just the immediate use cases." Blockchain is now similar to artificial intelligence (AI) in 2016, in that it will soon be the functionality every security vendor is going to seek out. "We predict that 2018 will be the start of an avalanche of new startups offering blockchain-related security solutions and that incumbents will scramble to update vision, strategy, and road maps so they don't lag behind," according to the report. **Action:** Begin asking all security vendors about their blockchain road maps.

(6) Firms too aggressively hunting insider threats will face lawsuits and GDPR fines.
It's become easier for firms to monitor employees and their activities as a means to thwart malicious insiders, employees making mistakes, or an attacker with compromised employee credentials. However, employees may find this to be an invasion of privacy. In September, the European Court of Human Rights ruled that companies must inform employees in advance if their work email accounts are going to be monitored. Further, such monitoring must not infringe upon workers' privacy, the court ruled. The EU GDPR also applies to employee privacy and data handling, and includes large fines for noncompliance. "Conventional wisdom dictates that mishandling of customer data will draw the ire of regulators, but employee data is personal data, and Forrester predicts that regulators will be just as likely to focus on employee privacy violations as they are customer violations," according to the report. **Action:** Create privacy rules of engagement for employee monitoring.

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! Stay Safe and Secure – Protect your information, your family's, your employer's, your clients', and all the folks in your cyber circle.

The Security News Digest (SND) is a collection of articles published by others that have been compiled by the Information Security Branch (ISB) from various sources. The intention of the SND is simply to make its recipients aware of recent articles pertaining to information security in order to increase their knowledge of information security issues. The views and opinions displayed in these articles are strictly those of the articles' writers and editors and are not intended to reflect the views or opinions of the ISB. Readers are expected to conduct their own assessment on the validity and objectivity of each article and to apply their own judgment when using or referring to this information. The ISB is not responsible for the manner in which the information presented is used or interpreted by its recipients.

For previous issues of Security News Digest, visit the current month archive page at:
http://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/security-news-digest

To learn more about information security issues and best practices, visit us at:
Information Security Awareness Team - Information Security Branch
Office of the Chief Information Officer
Ministry of Citizens' Services
4000 Seymour Place, Victoria, BC   V8X 4S8
http://gov.bc.ca/informationsecurity
OCIOSecurity@gov.bc.ca

The information presented or referred to in SND is owned by third parties and protected by copyright law, as well as any terms of use associated with the sites on which the information is provided. The recipient is responsible for making itself aware of and abiding by all applicable laws, policies and agreements associated with this information.

We attempt to provide accurate Internet links to the information sources referenced. We are not responsible for broken or inaccurate Internet links to sites owned or operated by third parties, nor for the content, accuracy, performance or availability of any such third-party sites or any information contained on them.

****