Volume 27, Issue 1 – January 2018

DRIE Digest

Disaster Recovery Information Exchange

157 Adelaide St. West, PO Box 247, Toronto, ON M5H 4E7 | Website: www.drie.org

IN THIS ISSUE

CYBER 2018

Cyber security and technology trends for 2018

By Kenrick Bagnall, **Cybercrime Investigator @ Toronto Police Service**
@KenrickBagnall

2017 will go down in history as a year filled with news headline making events. Regardless of your personal or professional areas of interest, there were high profile events in the news on a weekly basis in politics, finance, food, fashion, culture and of course information technology and cyber security.

When considering cyber security and cybercrime, the 2017 reported data breaches of Equifax and Uber demonstrate a new trend. Cybercrime is more sophisticated, organized and the targeted cyber attacks are on larger more high profile organizations. The companies have what would have been considered at the time, sound technology and information security infrastructure, yet still they were breached.

2018 will see continued resource investment in breach planning and prevention, but there will also be a mindset and best practice shift as organizations trend towards cyber incident mitigation and incident response. Targeted attacks have time and time again proven to be successful. After hearing the message of cyber risk mitigation and incident response planning repeated throughout 2017, organizations are beginning to take cyber threats more seriously and take a more holistic approach to incident response planning.

That said, I'd like to share my thoughts on some selected areas of interest in technology and provide my insights on how I see them impacting cyber security and cybercrime through 2018.

IoT

Let's face it folks, IoT (Internet of Things) is there to stay. IoT is the technology category that describes third party (various manufacturers) Internet connected consumer grade devices aimed at home/office automation and come with some kind of control panel, web or mobile device user interface for configuration and interaction.

Factors including but not limited to price reduction, availability, variety, consumer appetite, and exponential increase in the use of IPv6 will cause IoT to explode in 2018. Many households will double or triple the number of IP enabled devices currently in use in their home. The growing market for home automation and commonplace use of devices like home voice assistance will add fuel to this explosive growth.

The fundamental security problems of IoT devices persist. Weak out of the box security and an inherent inability to seamlessly enable security path updates have been and will continue to be problematic. Many of these IoT devices will become "zombie" devices in massive Botnets. To that end, I see an increase in the number of DDOS (Distributed Denial of Service) attacks against high profile targets in 2018. Be smart, plan ahead and take steps to mitigate and respond to these types of attacks in 2018.

RANSOMWARE

If history teaches us anything, it's safe to say that there have already been a number of successful Ransomware attacks that we will not hear about until some time later in 2018.

When the hacking group The Shadow Brokers compromised the NSA (National Security Agency, USA) and distributed several hacking tools on the Dark Web we noticed an increase in the frequency and sophistication of cyber attacks. With plans to release more tools and roll out a SaaS (Software as a Service) model for the hacking tools, we can only expect more attacks to come.

The common motivators remain the same in terms of monetary gain, political advantage and simple bragging rights. However with a SaaS model for hacking tools, we can expect a large increase in copy cat style cyber attacks.

The best defense against Ransomware attacks remains to have good backups that can be quickly implemented and a staff/team that is well trained in cyber security and social engineering awareness.

The mainstream law enforcement position is to not pay the Ransomware demands. There is never a guarantee that paying will restore your data, or prevent a repeated attack. This is a law enforcement perspective. However payment or nonpayment is a business decision that should be considered and decided long before victimization occurs.

CYBER EXTORTION

Cyber extortion is a targeted cybercrime. Its success is generally based on victim vulnerability and their overwhelming desire to avoid exposure. The subject is selected and some reconnaissance using open source techniques is done to gather as much information as possible. Once enough information is obtained on the subject the contact is most often made via an email or social media connect where the vulnerability is identified and the demand is made.

2016 saw a high volume of these types of incidences with some leveling off during 2017. I'm predicting that we will see this category of cybercrime on the rise in 2018. More people are gravitating towards social media, very few know how to secure their accounts and far too many are posting information and personal details that make them an easy target.

I have three recommendations here that may assist you. First, privatize your personal social media accounts and take the time to read the provider's terms of use agreement. If you use social media to promote yourself or your business the former may not be possible but the latter is a must. Second, go through your personal social media and purge all unknown and unnecessary contacts. Sometimes the size of the contacts or friends list can become a bit of a bragging point, but it's not worth it if some unknown contact is really just there to socially engineer you then

extort you. Last but very important, report the cybercrime to law enforcement. Make it a matter of record and allow the police to investigate and hopefully identify a suspect. If a suspect is not identified in your particular case, the reported occurrence allows law enforcement to identify patterns and trends, work with other agencies both foreign and domestic by sharing intelligence about this type of offence. As occurrences build up this also assists law enforcement to better allocate resources going forward which ultimately helps the communities we serve.

CLOUD SECURITY

In 2010 I wrote a Blog entitled "Is your head in the clouds?". At the time I suggested that if as a business organization or a private citizen end-user you were not considering use of the cloud, you should be. In the past 7 years we've seen massive uptake in the use of cloud technology because of the benefits it can provide in terms of economies of scale, scalability, availability and flexibility.

Cloud security has evolved and it will continue to do so at an increased rate in 2018. I see a trend towards the increased use of private cloud. Organizations want to be able to quickly implement their existing security best practices in the cloud space. It gives them the benefit of being more agile and responsive as they grow or their business challenges change. They need to be able to leverage their technology tools to exploit the changing business landscape and the use of private cloud will help that.

The use of cloud architecture is not only about quickly spinning up servers or switches where needed. It's not only about the seamless deployment and support of the applications that make business run. It's about using cloud as the repository for sensitive and valuable customer data, employee data and corporate intellectual property. All of these things are susceptible to Ransomware attacks. The use of private cloud is simply a better way to mitigate the response and get your organization back up and running as quickly as possible.

NET NEUTRALITY

A lot has been said about the issue of Net Neutrality during 2017 and the dialog will continue well into 2018. My personal opinion on this matter is that it will become a self-correcting issue. As the conversation continues it will be the end users themselves whose voices will be heard. This will force regulators and policy makers to implement punitive measure of enough significance that the Internet Services Provides and other Internet bellwether organizations will fall in line to protect their bottom lines.

As the message of Net Neutrality gets out during 2018, the general consumer will become more informed and opinions will be formed along various lines including but not limited to content and provider preferences or even political persuasion. However there is another side to this that has not shown up yet, but will at some point in 2018.

There is a criminal element out there constantly looking for ways to take advantage of people's vulnerabilities. There are many concerned about increased Internet access fees and compromised Internet speeds to access their favorite sites.

I believe there will be a new Phishing scam that will take centre stage at least for a portion of 2018. Consumers will be targeted to pay a small fee to guarantee that their access portals and accounts do not suffer any adverse consequences. This will occur as the Net Neutrality issues are debated, distilled and dissolve into a regulatory framework that keepings all the major players in check and protects the user. Look for this phishing email in an inbox near you, and when you see it just remember to click delete.

CRYPTO CURRENCY

This is fascinating, volatile and now controversial subject matter. It is fascinating because of the subject matter and the technology that supports it. It is volatile because of trading volumes, price fluctuations and a massive north of 1200%

increase through 2017. It is now controversial because of the resulting environmental impact crypto currency mining and transaction validation is having because of the massive computing resource requirements.

So what will 2018 bring for crypto currency? Even more time and attention will be directed toward virtual currency. I believe the volatility will continue but will somewhat stabilize for BitCoin because of the underlying technology of the Block Chain. Block Chain technology will expand to other mainstream business applications and these will lend greater credence to the viability of BitCoin specifically.

The environmental impact issue will persist through 2018, however there is a game changer on the horizon and it's called Quantum Computing. If more renewable energy sources can be applied to powering BitCoin mining, combined with the processing power of quantum computing, BitCoin (and other crypto currencies) will soar in 2018 and beyond. Also, anything currency related has always been about regulation. So look for more involvement from the mainstream banking organizations and policy makers in 2018.

As for law enforcement, crypto currency is no different from any other asset and will be treated as such within the guidelines of the criminal code when it comes to investigations, search and seizure and asset forfeiture.

QUANTUM COMPUTING

With advances in AI (Artificial Intelligence) and machine learning we can expect to see the fruits of quantum computing being served up a lot sooner than most are expecting. One of the collateral issues associated with quantum computing going mainstream is the requirement to keep this technology cool (literally) as the hardware is performing computations.

I remember in the early 90s working with an IBM ES/9000 mainframe that was liquid cooled. From experience I can tell you that this is a logistical and technical problem that will be solved very quickly with a little time, ingenuity and cool innovation.

I see Quantum computing will have a huge impact on encryption and cyber security. There will be many issues that will surround this technology but the real issues are not technological; they revolve around policy, compliance and most importantly privacy.

There are many who believe that quantum computing will tilt the scales in favor of cyber criminals. I don't agree with this but it will put increased demand on law enforcement and other cyber security professionals to improve their knowledge and skills in an area where many private sector organizations and public sector agencies are already suffering from the effects of a depleted talent pool.

In short, 2018 will not see quantum computers for sale at your local Best Buy or Canada Computers but their slow and steady implementation will have a trickle down effect on all of our computing lives. For 2018, be quantum computing aware and continue to build strong passwords and more secure infrastructures.

CYBER SECURITY, MOVE TO MITIGATION AND INCIDENT RESPONSE.

Over the past decade or so a great deal of emphasis (and money) has been put into cyber security from a preventative perspective. In 2017 a definite shift was noted. Organizations and indeed individuals alike have been investing more resources into response and recovery and this will continue through 2018. It is an advisable strategy and here are my thoughts as to why.

It comes back to my earlier comments regarding random and targeted attacks. More and more organizations are being specifically targeted since the success rate of random attacks appears to be decreasing. A few things that have helped are increased awareness of potential cyber threats, staff training on social engineering awareness and better password management have all helped to stem the tide of mass email phishing scams, cyber fraud and broad brush Ransomware attacks.

In 2018 organizations will take greater advantage of available cyber related educational resources and training. Mandatory breach notification will become a reality in 2018. This will have significant impact on organizations in terms of the time, effort, and attention they put into their ability to make appropriate notification to authorities post breach environment. This factor speaks directly to incident response and brings me to my closing point.

LAW ENFORCEMENT ENGAGEMENT

Under all of the glitz and excitement that Hollywood and the media make cybercrime out to be, let us not lose site of the fact that when the facade is stripped away, what you are left with is a criminal offence.

Let's make 2018 the year of cyber incident reporting. Not just mandatory breach reporting to regulators, but also taking the steps that will provide the only punitive measure against cybercrime, reporting the offence to law enforcement.

This will allow police agencies to work with you and their global law enforcement partners to conduct thorough investigations, identify suspects and put credible cases with a strong likelihood of conviction before the courts.

Cyber security and the prevention of cyber crime is a shared responsibility, together we win.

Have a great 2018.

KENRICK BAGNALL

Prior to joining the Toronto Police Service Kenrick spent twenty years working in the Information Technology industry primarily in the financial services sector. During this time Kenrick spent twelve and one half years working in Bermuda where he was a Senior Network Analyst for the Bank of Butterfield, then an IT Manager for Flag Telecom and then as Senior Vice President of Information Technology for CAPITAL G Bank (Now Clarien Bank) before returning to Canada in 2005.

Kenrick has been a member of the Toronto Police Service since April of 2006 and holds the rank of Detective Constable. He has worked in several areas of policing including Primary Response, Community Response, The TAVIS Neighbourhood Imitative Program, General Criminal Investigations, and Divisional Fraud Investigations.

In February of 2015 Kenrick joined the Computer Cyber Crime (C3) section of Intelligence Services where he currently works as a Cybercrime Investigator, and also instructs at the Toronto Police College on the Internet Felicitated Investigations course.

Kenrick is a contributor to Canadian Security Magazine where he was written several columns on Cybersecurity including cyber bullying and threats to critical infrastructure. Kenrick has been a keynote speaker and presenter on Cybersecurity at the Converged Security Summit (Atlanta, GA), The Fraud & Breach Prevention Summit (Toronto, ON), The Niagara Counterfeit and Fraud Workshop (Niagara Falls, ON), The Axis Communications USA Partner Summit (Tucson, AZ) and several other public sector and private industry symposiums.

Kenrick's background in Information Technology combined with his Law Enforcement experience has uniquely positioned him as an investigator, instructor and presenter on technology, information security and cyber investigations. ■

Letter From The Editor

January 2018

It's a new year filled with limitless possibilities. We aren't the only ones thinking this way. Cyber criminals and cyber security professionals are thinking the exact same thing.

According to the State of Cybercrime 2017 report the cyber security industry is going to explode over the next 5 years based on a few very significant statistics.

The cyber security community is forecasting that cyber crime damages will cost the world $6 trillion annually by 2021, up from $3 trillion just a year ago. This represents the greatest transfer of economic wealth in history.

Global spending on cyber security products and services are predicted to exceed $1 trillion from 2017-2021.Cyber crime will more than triple the number of unfilled cyber security jobs, which is predicted to reach 3.5 million by 2021.

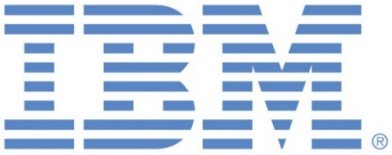
As the world goes digital, humans have moved ahead of machines as the top target for cyber criminals. There are 3.8 billion internet users in 2017. The hackers smell blood now, not silicon.

In this issue, Kenrick Bagnall a local expert on cyber security provides us with his keen insights into what the trends will be for cyber crime and cyber security in 2018. He also outlines how we can best prepare to defend and mitigate against these trends.

Vickie

NATIONAL SPONSOR

GOLD SPONSORS



SILVER SPONSORS

BRONZE SPONSORS

AD FOR UPCOMING CONFERENCE

CONGRATULATIONS

Graeme Jannaway Hon FBCI

The Digest would like to celebrate the welcome addition to the ranks of Canadian Fellows of the Business Continuity Institute one of the legends of business continuity in Canada – Graeme Jannaway. Well known to the DRIE community as a long-time member and past President, for his involvement in DRI Canada and through his international standing as an expert in BCM standards, Graeme was awarded the Honorary FBCI designation in recognition of his significant contributions to the profession for over 30 years. He accepted his award in person in London at the BCI World Gala Dinner on November 7th. Congratulations Graeme!