GreenPoint Financial
www.greenpoint.financial

REGULATORY PERSPECTIVES
June 27th, 2017
Volume - 8
Series - 1

PREPARE FOR GROWING THREATS OF MOBILE SECURITY

By **Kirsten Bay – President & CEO, Cyber adAPT**

Although no one has a crystal ball, it does not necessarily take one to follow trends. To best discuss predictions in the realm of information security for 2017, a review of 2016 events can inform how the landscape has changed.

2016 Year in Review

Ransomware

Ransomware was the single most frustrating and visible of issue throughout 2016. Although not the costliest or the most technically sophisticated, it wreaked havoc on a good deal of small and medium sized businesses and universities.

As PC World put it: "*The number of ransomware attacks targeting companies increased threefold from January to September (2016), affecting one in every five businesses worldwide.*"

Among the most successful ransomware programs in 2016 was *CTB-Locker*, which reportedly accounted for approximately 25% of all affected users, with *Locky* and *TeslaCrypt* following at a distant 7% and 6.5%, respectively.

Ransomware affected a wide range of organizations including hospitals, retail, financial institutions, and many government agencies with varying degrees of severity. Many of these victims actually paid their attackers, which the FBI highly recommends against.

The Tesco Bank Hack was another 'highlight' of 2016. My thoughts on Tesco Bank were recently highlighted by FTSE Global Markets:

> *"The recent Tesco Bank hack has left the retail banking world reeling, searching for answers and more effective ways to secure networks against future attacks. It has revealed weaknesses in how the bank's mobile applications left the door open for cybercriminals to brute force their way in and take more than £2.5m of customers' money. Worse still, the bank had been warned by several security experts of this weakness prior to the attack. Is the Tesco Bank hack the wakeup call needed to make mobile security a priority?"*
>
> **www.ftseglobalmarkets.com/news/lessons-from-the-tesco-bank-hack.html*

Let's be honest – all banks (among other institutions) are under daily attack in one form or another with only a handful of these attacks making the news. The main difference for the Tesco hack, which I would argue is a more pervasive problem within organizations, is that Tesco Bank was **warned** of these issues prior to this event. These warnings were either ignored or were not resolved in time. Sadly, we continue to see this happen on a regular basis, within all sizes and types of organizations.

What about the half billion Yahoo! users who had their personal information stolen? One could argue that Yahoo! is even more culpable than Tesco because Yahoo! failed to disclose this massive attack for two years. The full nature of the compromise was only reported when the attackers struck again late 2016, but not before the SEC had already opened a formal probe into the initial hack.

The list goes on and on – but let's close the discussion of 2016 with how the year ended, the hacking of the DNC. Recently we learned that Russian army malware, dubbed "X-Agent," was reportedly linked to the DNC hack.

More malicious than past malware, the one known as "X-Agent" is an implant. It's designed to supplement phishing campaigns, such as the one that ensnared the ranking leadership of the DNC. It's dropped in by infected sites, designed to look legitimate, and, once installed, logs keystrokes, filtrates data, and executes commands remotely. These DNC attacks, and the crafty use of WikiLeaks, were an attempt to influence the US Presidential election. They were well planned, strategic and stealthy. They could compromise a user and had a sophisticated plan for disseminating the information.

We were left with the overarching question of who and what we can trust online or otherwise.

On that bright note . . .

2017 Predictions

After many years of securing data, we've learned that there are no shortcuts. Hard work from both a research and technology perspective are essential, while always keeping a watchful eye on the big picture. Unknowns and volatility make it very hard to mitigate cyber risk.

Cyber Insurance

Although not a new market, 2017 will prove to be either groundbreaking or more challenging than ever, depending on how one can value the cyber insurance market.

> *The current market size is around $3 billion, according to various estimates. According to PwC the global cyber insurance market, dominated by North America, is expected to generate $14 billion in gross premiums by 2022, growing at a compound annual growth rate of nearly 28%.*

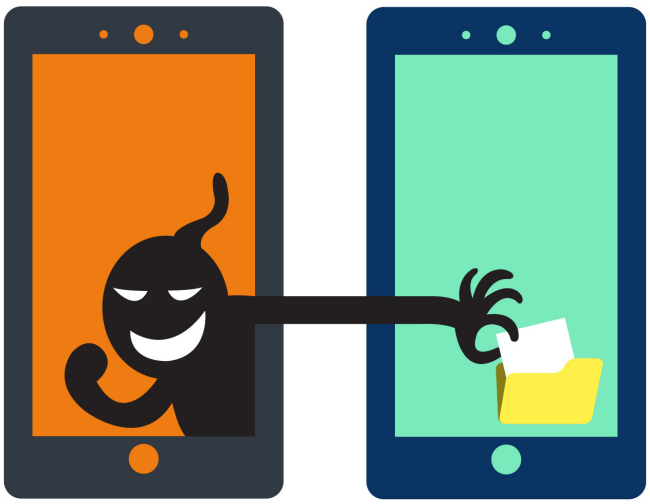
Carriers have been valuing policies with a keen eye on the cost of recovery, however a lack of incident data combined with high potential severity lead to the potential for asymmetric payoffs. How does this asymmetry get priced into the insurance equation? The challenge for cyber insurance underwriters is having enough data to calculate risk of loss in an area with several complex variables and potentially large payoffs.

Ransomware

Throughout 2017, you are going to see *target of opportunity vs target of convenience* as an ongoing theme. Understanding this distinction can help not only remediate, but also prevent, many cyber-related attacks.

We saw an a tremendous amount of ransomware activity in 2016 – many felt that 2016 was 'The Year of Ransomware' – but we predict this year will only be worse. We'll see a marked increase in both the sophistication of the encryption used to lock organizations out of their systems as well as a more rapid spread of such attacks across vertical markets, with a targeted *increase* of both state and federal government agencies.

2017 opens as organizations worldwide are rapidly moving IT infrastructures to cloud providers such as Amazon Web Services (AWS), Microsoft Azure, Google, and others. We predict ransomware will quickly escalate along with this transition as we see instances of individual organizations successfully attacked and brought to their knees. This will be similar to last year when fixed network infrastructures were attacked. The difference in the cloud will be that the same attack can be used on many more organizations because the attack profile will be simple to replicate.



The Internet of Things (IoT) will be a new and growing vector for ransomware attacks. This will increase quickly given how little security exists in IoT products. As reported by Wired Magazine:

> *An Austrian hotel lost control of its door locks, keeping new guests stranded in the lobby. A police department in Cockrell Hill, Texas abandoned years of video evidence and digital documentation. In Washington, DC, the police couldn't access its CCTV footage storage system days before Donald Trump's inauguration. All of this news came out in the last week, stemming from a rapid escalation of how ransomware is deployed. And it's only going to get worse.*

Mobile

As we saw last year with Tesco Bank, mobile devices will only become a more prominent point of entry into organizations' networks. Criminal and state sponsored activists will increasingly harness methods to automate mobile infiltration.

Phishing tactics from social engineering, bad apps, and drive-by malware websites will be magnified by the infiltration of hardware, including your new phone, with pre-installed malware compromised due to poor third party supply chain security. We see *these targets of convenience* will continue to grow exponentially.

With a $150 tool and a YouTube video, a hacker can hang out in an airport, hotel, coffee shop, or even your neighborhood, and intercept your mobile communications. While decryption of content may be difficult, stealing your username and password to your banking app, your iCloud account, your company exchange email account, etc. is simple. An attacker can sit in your company parking lot of your local branch to do this – **that** is a target of opportunity.

Scary?

Now turn it into a target of convenience. That same $150 tool can scrape, learn, and store in memory every Wi-Fi access point it touches. Users will connect to what they think is their secured Wi-Fi (Home, Delta Lounge, Company Wi-Fi, etc.) when their traffic is being intercepted and pwned (an industry term for owned or hacked).

Did I mention this tool, called the *Wi-Fi Pineapple Nano*, can fit in your pocket and be powered by one of those little phone charging juice packs?

People are demanding more and more out of mobile. Demands on banks and other businesses for mobile is increasingly "anywhere, anytime and anyhow." With seamless connectivity comes a boundless enterprise, and with a boundless enterprise comes risk. *The more access, the more risk.* Although it is easy to understand why employees want to be able to do everything from mobile devices, it should be even easier to see how of the lack of security on those devices can create the ultimate target of both convenience and opportunity.

Further Predictions and Actions

2017 will be the year that a cyber-related incident based on one or multiple of the characteristics stated above will bring down a financial institution and/or another enterprise in a much-publicized event. This will more than likely be either state sponsored or hacktivist related.

2017 has also already brought much discussion about how the new administration and government aims to improve security to further protect data. For example, private organizations often break their own industry regulations, such as SarBox and HIPAA, simply in the way they provide key data sets to the federal government for compliance. This is because those federal systems do not meet the private sector standards.

This leads me to the role of government protection and some thoughts shared by the majority leader of the US House of Representatives:

> *"Cybersecurity: Americans are rightfully worried about becoming the victims for the next major data breach and Congress must insist that Americans' personal*

financial data is protected. Data breaches subject consumers to uncertainty and confusion and increase consumers' vulnerability to identity theft, leading to further inconvenience and possible financial loss. As technology advances and personal data becomes its own currency, consumers face an escalating risk of identity theft and financial fraud from criminals, many of them operating overseas, seeking to access their personally identifying data. The increasing frequency and sophistication of cyberattacks demands heightened vigilance and enhanced efforts by industry participants to safeguard consumers' financial data.

Task Force Solution: House Republicans are developing legislation to ensure stronger protections for consumers against identity theft and fraud as well as legislation to ensure that sensitive information that is submitted to the government is fully protected from cyberattack. H.R. 3738, Rep. Ed Royce's legislation, requires the Office of Financial Research (OFR) to provide a detailed strategic plan regarding its priorities and to develop and implement a cybersecurity plan to protect the data that it collects."[2]

If you believe that, I have a bridge to sell you. Your organization *cannot* rely on the government at the state or federal level to protect your company's data. Instead, it is up to your organization to use technology, in tandem with policy and strong governance, to protect customers, employees, and all other company data. This includes the sharing of that data with government agencies. The legal, regulatory and reputational risks are large.

---

1. PC World
2. From www.abetterway.speaker.gov/_assets/pdf/abetterway-economy-policypaper.pdf