Symantec Enterprise Security

0

0 Votes

Symantec Official Blog

Symantec Predictions for 2016 -- Looking Ahead

By: **Symantec APJ** SYMANTEC EMPLOYEE

Created 01 Dec 2015

Co-Authored By: **Nick Savvides**

0

Translations: 简体中文, 繁體中文, 日本語, 한국어

Share

Today's cybercriminals are skilled enough and sufficiently resourced to have the persistence and patience to carry out highly successful attacks on consumers, businesses and governments around the world. Their efforts have turned cybercrime into big business with private information being stolen on an epic scale.

In 2015, we saw how much consumer confidence was rocked by the number of mega breaches that exposed the identities of millions of people. The ability for some organizations to recover from a data breach was paralyzing as we saw in the Ashley Maddison data breach.

There is no magic-bullet technology that will guarantee immunity from Internet crime or determined, targeted attacks, but being prepared for the worst can prevent some attacks. So, what lies ahead for 2016? **What will be the biggest threats that will target consumers and businesses**? How will some of the newest technology trends impact privacy and regulation? And how will businesses respond to data breaches when it is no longer a matter of if, but when you will be breached?

As the year draws to a close, Symantec's security intelligence team has put together the top security predictions for the year ahead and beyond. Here are our top picks for 2016 -

1. **The Need for Improved Security on IoT Devices Will Become More Pressing**

As consumers buy more smart watches, activity trackers, holographic headsets, and other Internet of Things (IoT) devices, the need for improved security on these devices will become more pressing.

According to a Gartner report titled *Agenda Overview for the Internet of Things*, by 2020 close to 30 billion connected things will be in use across a wide range of industries and the IoT will touch every role across the enterprise. There's no doubt the market for Internet of Things–ready devices is growing but it is still very fragmented, with a rich diversity in low-cost hardware platforms and operating systems. As market leaders emerge and certain ecosystems grow, the attacks against these devices will undoubtedly escalate, as we've already seen happen with the attacks on the Android platform. The good news is that OS makers, in particularly Apple, are making good strides in enforcing security in the eco-systems they support, such as HomeKit.

In addition, the evolving concept of "care is everywhere" may see medical device security become a mainstream topic in 2016. It's widely known that life-sustaining devices like pacemakers or insulin pumps can be hacked. Fortunately, to-date, no such case has been reported outside proof-of-concept security research; however, the potential impact remains high. Under the evolving umbrella of mobile health, or mHealth, new care delivery models will move devices into the patient's home. This will place medical devices on public networks, provide medical apps through consumer devices such as smartphones, and interlace personal data with clinical information.

With these changes happening so rapidly, regulation may be forced to catch up with technology in 2016. We may find that some countries or industries will begin to develop guidelines that address the new risks of information use, data ownership, and consent presented by IoT devices.

2. **Opportunities For Cybercriminals To Compromise Apple Devices Will Grow**
   Apple devices have experienced a surge in popularity in recent years. According to IDC, the company now accounts for 13.5 percent of global smartphone shipments and 7.5 percent of global PC shipments. This increase in usage has not gone unnoticed by attackers. A rising number of threat actors have begun developing specific malware designed to infect devices running Mac OS X or iOS.

   Although the number of threats targeting Apple operating systems remains quite low when compared to the company's main competitors (Windows in the desktop space and Android in mobile), the amount uncovered has grown steadily in recent years. In tandem with this, the level of Apple-related malware infections has spiked, particularly in the past 18 months.

Security researchers have also given a greater focus on vulnerabilities in Apple software, with a number of high-profile flaws uncovered in the past year. Zero-day brokers have begun offering bounties for Apple vulnerabilities, with US$1 million paid recently for a jailbreak of iOS 9.1.

Should Apple's popularity continue to grow, it seems likely that these trends will continue in 2016. Apple users should not be complacent about security and change their perception that Apple devices are "free from malware"- this perception opens up opportunities for cybercriminals to take advantage of these users. They need to take precautions in order to prevent their devices from being compromised.

3. **The Battle Between Ransomware Gangs and Malware Distribution Networks Will Heat-Up**
   From early beginnings in Russian speaking counties, ransomware has evolved and spread into Western Europe, the United States, Canada, Australia, Europe and Asia. It is likely that some of the gangs responsible for the original ransomware are part of this expansion, but other established criminal gangs are also becoming involved. Clearly, the fraud is profitable for criminals and is likely to increase.

   It is also possible that ransomware gangs will come into conflict with more traditional malware distributors in 2016. Ransomware infections are overt and obvious, while most other malware infections are covert and discreet. The presence of ransomware on a computer will usually prompt the computer owner to clean the machine thoroughly, removing any malware from it. As the ransomware may have been installed by a separate piece of malware, that other malware will also be removed, cutting into the malware operator's business model.

   In 2016, more malware distribution networks may soon refuse to distribute such obvious malware, forcing the ransomware gangs to develop their own distribution methods (like Trojan.Ransomlock.G and Trojan.Ransomlock.P have already done).

   As awareness of these scams increases, the attackers and their malware are likely to evolve and use more sophisticated techniques to evade detection and prevent removal. The "ransom letter" will likely also evolve and the attackers will use different hooks to defraud innocent users.

4. **Cyber Attacks and Data Breaches Will Drive the Need for Cyber Insurance**
   When we look at the rapid adoption of cyber insurance, there are two key factors that attribute to this growth: new regulations which obligate companies to respond to information breaches; and the increase of cyber criminals using stolen information for

payment fraud, identity theft, and other crimes.

Cyber attacks and data breaches cause reputational harm and business interruptions, but most of all—they are expensive. Relying on IT defenses alone can create a false sense of security; however, no organization is immune from risk. In 2016 many companies will turn to cyber insurance as another layer of protection, particularly as cyber attacks start mirroring physical world attacks.

Cyber insurance offers organizations protection to limit their risk, but companies should consider all coverage options carefully. It's not about checking off a box; it's about finding a policy that protects an organization's brand, reputation, and operations if faced with a breach.

Cyber insurance is evolving as fast as technology. What is considered core coverage today was not available as little as three years ago, and enhancements to coverage will continue to be negotiated in the marketplace every day as data breaches and cyber risks evolve.

5. **Risk of Serious Attacks to Critical Infrastructure Will Increase**
   We have already seen attacks on infrastructure and in 2016 we can expect this to continue to increase. Motivations for critical infrastructure attacks are both political and criminal, with nations and political organizations operating cyber-warfare campaigns, and criminals attacking for profit or ransom. The industrial IoT is becoming more connected due to requirements and demand for reporting and improved functionality through connectivity with additional services. These changes introduce bigger attack surfaces into the more traditionally hard to secure environments.

6. **The Need for Encryption Escalates**
   Encrypt everywhere is quickly becoming the mantra of the technology industry. With so much communication and interaction between people and systems happening over insecure and vulnerable networks like the Internet, strong encryption for this data in transit has been well recognized for some time and it is generally implemented.

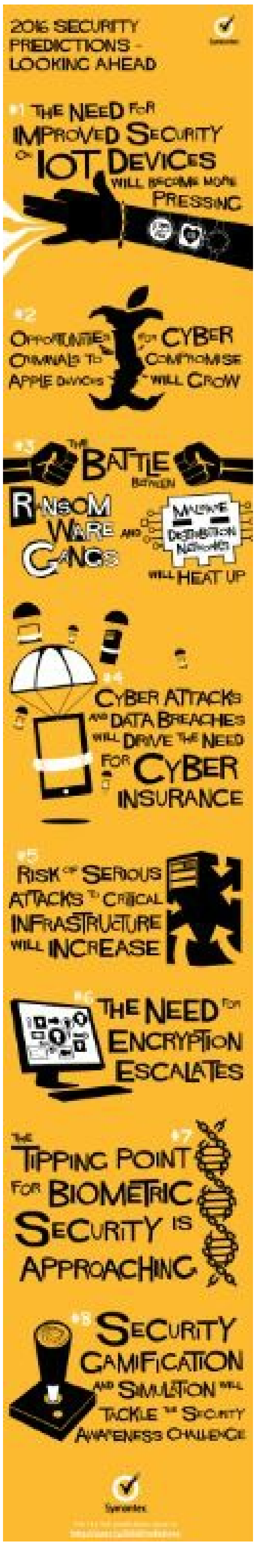
   Unfortunately many new devices and applications have had poor implementations, leading to vulnerabilities that allow focused attackers to gain access to communications. For example, the mobile device has become center of most peoples' lives for communications, data storage and general technology interaction. This presents a high value target for cybercriminals, who are looking to exploit this. Mobile OS makers continue to make improvements to the encryption of their products to fill in the gaps from the application and service makers. While this trend of encrypting more is good for protecting user data from cybercriminals, it has also raised the ire of governments who believe this be a hurdle for law enforcement. It seems that the crypto-wars of the 90’s may be repeated in the next two years.

7. **The Tipping Point for Biometric Security Is Approaching**
   The last two years have seen a significant rise in the use of biometrics. This is expected to grow significantly with major industry players implementing new capabilities both with new sensors in devices and with adoption of biometric authentication frameworks like FIDO and TouchID. This facilitates secure on device storage of biometric information (like fingerprints) as well as interoperability between apps and systems. What this means is that biometrics can finally answer the "what’s in it for me” question that consumers have been asking, while replacing passwords with strong traditional PKI authentication protected by the biometric sensor. The consumer gets better security with significantly increased convenience for device unlocking, purchasing and payments. This also is leading to enterprise adoption of biometrics that may start to see a reduction on the dependence on passwords.

8. **Security Gamification and Simulation Will Tackle the Security Awareness Challenge**
   Internet security relies on the human element as much as it does on technology. If people were more skillful, they could help reduce the risks they faced. This is as true of consumers avoiding scams as it is of government employees avoiding the social engineering in targeted attacks.

   In this context, security gamification will be used to turn “the desires of the moment” into lasting changes of behavior by using the psychological rewards and instant gratification of simple computer games. Security Gamification could be used, for example, to train consumers to be wary of phishing emails or to generate, remember, and use strong passwords. Symantec sees a big market opportunity and a great need for this kind of training in 2016.

   Companies will also invest more in preparing for security breaches and understanding their defenses better by using simulations and security “war games.” By extending conventional penetration testing into a simulated response and remediation phase, companies can train their employees and improve their readiness. This message is not lost on governments. In January 2015, UK Prime Minister David Cameron and U.S. President Barack Obama agreed to carry out “war game” cyber attacks on each other. Companies could follow their example in 2016.


2016 SECURITY PREDICTIONS - LOOKING AHEAD
#1 THE NEED FOR IMPROVED SECURITY ON IOT DEVICES WILL BECOME MORE PRESSING
#2 OPPORTUNITIES FOR CYBER CRIMINALS TO COMPROMISE APPLE DEVICES WILL GROW
#3 THE BATTLE BETWEEN RANSOMWARE GANGS AND MALWARE DISTRIBUTION NETWORKS WILL HEAT UP
#4 CYBER ATTACKS AND DATA BREACHES WILL DRIVE THE NEED FOR CYBER INSURANCE
#5 RISK OF SERIOUS ATTACKS TO CRITICAL INFRASTRUCTURE WILL INCREASE
#6 THE NEED FOR ENCRYPTION ESCALATES
#7 THE TIPPING POINT FOR BIOMETRIC SECURITY IS APPROACHING
#8 SECURITY GAMIFICATION AND SIMULATION WILL TACKLE THE SECURITY AWARENESS CHALLENGE
Symantec

File Attachments:

- SYMANTEC_2016 SECURITY PREDICTIONS.PDF

Tags: Security, Symantec Enterprise Security, Security Community Blog, Symantec Enterprise Security

Subscriptions (0)

Symantec APJ

👤 View Profile

Login or **Register** to post comments.

Recent Posts

- The Gift that Keeps on Giving: 12 Ways Everyone Can Help IT This Holiday Season
- Symantec Predictions for 2016 -- Looking Ahead
- Driving Towards the SOC of 2020
- What is the Norton Cybersecurity Insights Report?
- Monitoring Shadow IT

Community Stats

Total Posts	Members
1,418,866	437,629