Global Knowledge®

Expert Reference Series of White Papers

Cybersecurity Predictions for 2016

Cybersecurity Predictions for 2016

James Michael Stewart, CISSP, CEH, CHFI, ECSA, and Security+

Introduction

The many security breaches over the last year have taught us new lessons or clarified ones we should have already known. But history is doomed to repeat itself. By failing to learn from the mistakes or misfortunes of others, our digital world remains vulnerable. The onslaught of new, developing threats coupled with already well-known persisting ones will continue to bombard our information infrastructure with potentially disastrous results. In this white paper, I discuss my 10 security predictions for 2016.

1. Digital Extortion Will Become Fully Automated

Since 2013, there has been an increase in a new form of malware, called ransomware which takes over a computer system, often using encryption to hold files hostage, then demands payment in order to release the data back to the user. Ransomware is just one example of a "modern" malicious code. Other forms include fake or rogue anti-virus programs, law enforcement Trojans, and elaborate phishing scams aimed at taking over an account or stealing an identity.

Doxing is another growing trend in malicious activity. The general concept of doxing is researching someone to learn embarrassing secrets, discover illegal activities, or simply reveal private or sensitive information about that person to the public. Doxing is often performed to discredit or devalue someone. It can be devastating to the victim's personal and professional life.

Unfortunately, I foresee these two malicious activities combining into a new form of attack called digital extortion. Rather than simply taking a system hostage, such malware could gather documents, images, etc., from a system, then transfer them to a botnet cloud, then present the victim with some form of ransom demand, blackmail request, or other form of extortion. The victim may be given a period of time during which the hackers promise to keep the victim's secrets secured. But hackers could return in a few months to make yet another demand and threaten to release the data. By failing to meet the demands of the hackers, the victim's stolen information could be posted across the Internet on social networks, discussion forums, and file servers.

This type of extortion has always occurred, even before the Internet existed, but in a manual form against targeted victims. However, I anticipate that an automated form of this contemptuous activity will be discovered in 2016, fully automating the process to be used against anyone unlucky enough to encounter the infection vector.

2. A Digital Payment System Will Be Compromised

Digital payment systems have been springing up like weeds. With the popularity of near field communication (NFC) and radio frequency identification (RFID) payment systems, such as Apple Pay and Android Pay, many other groups have attempted to roll out their own systems. Banks, credit card groups, specialty vendors, mobile device manufacturers, retail conglomerates, and others have announced their own digital payment system hoping to catch some of the tidal wave of potential future profits.

While the world might be shifting to a mobile device–based payment solution eventually, the idea is still not widely adopted. Few retailers support one, much less all, of the available payment systems. Most consumers do not have a device that supports mobile payments. Generally, when a retailer supports a payment system that a

Copyright ©2016 Global Knowledge Training LLC. All rights reserved.

consumer has the ability to use, the equipment is often malfunctioning or the cashier is unfamiliar with how to accept the payment. I personally have yet to have a single successful digital payment with my mobile device. Each time, I've had to take out my wallet to complete the transaction.

However, the inability to use mobile payment systems everywhere is not my prediction. I actually think the systems will become more widely available and more consumers will prefer to use a mobile device for transactions in the next few years. My 2016 prediction is that one of these mobile payment systems will be breached. It seems that too many groups are attempting to craft their own mobile payment solutions, while racing to beat other competitors in winning over the marketplace. This creates a fertile environment for multiple groups to fail to address security properly. Thus, it is highly likely that hackers will uncover a serious flaw that will be exploited to the detriment of the payment system and the corresponding banks and merchants, as well as the consumers themselves. A mobile payment system breach would cause significant loss of revenue, loss of privacy, unauthorized charges or money extractions, identity theft, and other related casualties.

3. More Data Leaks Containing Personal Information, Possibly Related to Wearables, Will Occur

In 2015, we witnessed dozens of large organizations experiencing data breaches that led to leaked information about customers and employees. We have also seen the new category of computing and tracking devices—wearables—emerge and grow in popularity. The term wearable is loosely employed to refer to any device that is attached to your clothing or worn on your person, similar to a piece of jewelry, clothing, or accessory. This includes clip-on devices, bands, watches, necklaces, in-shoe devices, belts, purses, rings, earrings, glasses, hats/helmets, and just about every form of clothing (i.e., smart apparel). These devices often perform a wide range of data metric–gathering functions, including GPS location, activity level, intensity level, heart rate, stress level, shock, movement, altitude, speed, and more. Wearables are usually configured to link up to an online account in order to provide analysis of the recorded metrics and track events across time. Many wearables compare and contrast your metrics with those of others, either specific friends for competition or amalgamated groups for comparison.

The wearable devices and the cloud services behind them concern me. Many of the manufacturers in this new arena of the IT industry often seek market share over any other concern. Thus, security and data protection are frequently secondary considerations, if at all. In 2016, it's very likely that a significant data leak from a wearable or its related online service will occur. A leak of wearable-related data could result in identity theft or spear phishing (i.e. targeted attack e-mails) and could be used for a wide range of malicious social engineering attacks. On a related note, I also see a shake-up coming in the wearable industry. All too often the companies behind devices that collect data about users assume or classify that data as company property rather than being owned by the individual. Thus, while consumers are given access to view their data, they might not have any real control over it. If someone wishes to switch devices and back-end services, they are usually unable to extract their data from one company and import it into another. Additionally, if users decide to stop using a device and want to terminate their service, they may be able to "cancel" their account, but the wearable company might retain the data it has collected. It is likely that in 2016, users will discover they lack any real control and ownership of their personal data. This revelation will cause a movement to force wearable companies to change their data tactics. Users should be able to export their collected metrics and choose to delete all of their data from any wearable service.

4. Smart Home Devices Will Fail

Smart home devices are everywhere. Just about every product manufacturer involved in residential products and services seems to be developing or already selling smart home or other connected devices. Generally a smart, connected device is any typical household product that has been enhanced through the addition of digital

Copyright ©2016 Global Knowledge Training LLC. All rights reserved.

capabilities. These capabilities could include monitoring, metric recording, remote management, remote activity triggering, and automation. Some of these smart devices offer little more than remote digital triggers, such as being able to turn on a light from a smart phone app. While others cross over into the embedded devices arena when they are fully automated and digitally managed through computer equipment, such as smart HVAC controls and thermostats.

We have been promised the connected home for decades—the ability for our homes to adjust and react to us, the occupants, either on a fixed schedule based on triggers (such as motion detection), or through voice or fingertip commands For most of us, the technology is either too expensive or too challenging to implement. This is further compounded by each major group or individual manufacturer wanting to be your sole proprietor of smart home devices. There are dozens of standards, protocols, and application programming interfaces (APIs) that are not interoperable or compatible with other vendors' products. Until interoperability is consistent and reliable, smart home technology is not likely to see widespread adoption.

However, many enthusiasts are willing to buy into a limited ecosystem of devices and controllers. There are many examples of high-end homes that have been "fully automated," but often at significant expense and high levels of custom hardware and coding. That is not to say that you can't get be part of the smart home revolution on a limited budget and without advanced programming skills. You can walk into any home center or big-box store and find several options of smart devices to implement right now. These include light bulbs, lamps / light fixtures, thermostats, A/C plug controls, security systems, IP cameras, and more.

As with many of my other predictions in this paper, this one is again based on the long standing bad practices of many in the IT industry to fail to pay attention to security. In 2016, it is likely that a well-known and fairly well-implemented smart device (or device ecosystem) will be compromised by hackers. A smart device compromise could allow an attacker to gain access to the home network and remotely control and monitor devices. This could result in data breaches but could also include wasting of utilities and triggering high utility bills (such as wasting water, using more electricity, or burning more fuel). In some circumstances, these compromises could cause physical damage to property or people. For example, a smart refrigerator could be hacked to warm up and spoil food, or a smart oven/stove/range could be hacked to turn on to its maximum temperature in order to cause a fire.

5. Companies Will Continue to Underperform in Regards to Security

You may have noticed that many of these predictions rest on the continued lack of attention to security. It seems that even with all the examples of breaches and compromises caused by the lack of company security across the last two decades, organizations continue to move forward with a "same as it ever was" mentality. It is a travesty that most do not learn from the mistakes and adversities of others.

I predict that in 2016 we will continue to see organizations experience compromises that could have been prevented with common sense security solutions or by stress-testing their own implementations. Issues that continue to be a problem include the following:

- Failing to secure websites against injection attacks, such as Structured Query Language (SQL) injection. This is done by filtering input against length requirements, pattern matching against a known list of malicious signatures, and escaping metacharacters. Metacharacters are characters assigned a special meaning by a programming language or execution environment.
- Leaving default configurations, settings, or account credentials.
- Failing to update to current product versions and patches. Testing should always be performed to ensure productivity and functionality, but staying on older versions is usually less secure.

Copyright ©2016 Global Knowledge Training LLC. All rights reserved.

- Failing to log all activity and events, including system events, software activities, and user activities.
- Failing to encrypt stored user data and provide communication encryption.
- Failing to separate different categories of data into different storage containers. For example, a customer's billing data should be separate from their login credentials, which should also be separate from their profile settings, preferences, and activity history.
- Failing to separate OS files from data storage on distinct storage devices.

These and other standard security concepts are well established, but not as widely adopted as they should be. As new organizations come online, expand their Internet presence, or roll out new products, they often make the same security mistakes as many others did before them. As consumers, we have established the trend that we will purchase new products in spite of flaws and failures. Often the early adopters of a new product are more like beta testers than typical consumers, willing to live with and work around problems just for the sake of getting the new thing in their hands.

We need to take a stand and stop being willing beta testers. We should only purchase products and use services that have a proven track record of security and which can demonstrate successful security and quality assessments. Maybe organizations should publish their security standards, thus allowing us to review their practices and make informed decisions about who is doing the better job at protecting our information and our person. This idea is already established in the digital certificate marketplace through a certificate authority's publication of its certificate practices statements (CPS). A similar strategy or publishing security practices should be applied across most or all of IT-related industries. Perhaps if we, as consumers, request and demand this from our vendors, maybe 2016 is the year that we evoke change for better security.

6. Ad Blockers and Script Blockers Will Become Essential Internet Tools

The Internet is evolving and might always be doing so. What we think it is for today is different than what it was used for ten years ago. In other white papers, I have recommended some core security tools that every Internet-accessible computer should have, such as a firewall and anti-malware protection. In 2016, two more security tools will be essential as the Internet has changed again. A recent evolution of the Internet is the expansion of web capabilities that has given rise to amazing sites and services that have has unfortunately also provided new opportunities to push malicious code onto visitors.

Malicious advertisements have risen dramatically in 2015. So much so that we saw the implementation of the Do Not Track (DNT) and incognito/private browsing features of web browsers. These elements came out of the ever-more aggressive efforts of advertisers to push marketing materials to site visitors. This in turn resulted in new advances in mobile code and dynamic web content. While advertisers have used these advances to their benefit, these advances have also caused frustration and annoyance for users, who see ads everywhere online. It is as if the main purpose of the Internet has been transformed into a vehicle for advertising, and the content we seek is just used as a teaser to attract us to a site in order to show us ads.

Advertising itself is not really the core problem. Most of us understand that advertising is how many sites and services make money, therefore allowing us to use the service without having to pay a fee. We are paying with our time and attention in relation to the advertisements. The problem is that malicious entities have taken advantage of the improvements in web technology in order to push malicious code to a visitor's system through the visitor's web browser. This in turn has caused a significant increase in wasted bandwidth (used to transfer the ever-growing volume of mobile content to support legitimate or illegitimate advertising) and introduced noticeable latency into load times and site response.

Copyright ©2016 Global Knowledge Training LLC. All rights reserved.

To combat these issues, users have begun to install ad blockers and script blockers. These tools are used to prevent the mobile code related to advertisement and mobile code to be transferred from the server to the web browser in the first place to save on bandwidth, or at least to stop the execution of the code if it is transferred anyway. Usually the goal of these tools is to increase site response, decrease load time, reduce bandwidth, and minimize annoyance caused by overly attention-demanding advertisements. So far, these web annoyance blockers are used only by a small percentage of the technically-inclined user base. However, in 2016 these tools will continue to become more end-user friendly and will be installed by a wider number of non-tech savvy users. This will be triggered by web browser vendors including these features into their software natively as well as a widening of the discussion of these tools in social networks and through how-to guides and sites.

I predict that based on the increase in use of blocking tools in web browsers, advertisers and site managers will revise their tactics. It is time for the pendulum to swing in the other direction. Instead of pushing more obnoxious and in-your-face ads, sites will move to advertisers that use more subtle approaches, employ in-context presentations, and focus on minimizing bandwidth consumption or latency. You can encourage this trend by using blocking tools, frequenting sites that are using balanced advertising approaches while avoiding those that don't, and taking the time to write the site owners to inform them of your opinion about their use of advertising and what your preferences are. If a site offers an ad-based version and a subscription version, consider putting your money on the line for the cause of less annoying advertising.

7. Increased Social Engineering Attacks on Employees Focused on Compromising Companies

I often trumpet the problem that many companies lack security. And while that is true, there are many companies that have adopted a solid and sensible security plan. For those organizations, traditional technical hacking tactics are often ineffective. Thus, hackers have adjusted their approach to include a wider range of attack vectors. These include physical breaches as well as social engineering.

I anticipate a noticeable increase in social engineering attacks across the board in 2016, including phishing scams, misleading websites, false security programs, social network hoaxes, and attack phone/ VoIP calls. However, I think the largest increase in attacks will focus on compromising employee credentials in order to gain access to otherwise highly-secured physical and/or digital resources.

At this point in time, security experts have a good understanding of how to lock down an organization from physical and technical exploits. Such implementations are often expensive and require constant management and updates. However, the one area that remains the most difficult to address is that of the weakest link in the system, the human component.

Humans are inherently vulnerable to social engineering attacks through many means, including coercion, trickery, bribery, blackmail, threats, competition, social validation, impersonation, and scarcity. Using these and other tricks, hackers will often seek to compromise an employee, and with that initial success reach further into an organization, either working up the chain of personnel or gaining access to a vulnerable system through a compromised individual.

This social engineering attack scenario has been used in the past, but I think this will be most common in 2016. This increase will likely be attributed to the overall improvement in logical and technical security, causing attackers to focus on the softer targets of employees, as many organizations continue to overlook the weaknesses exploited by social engineering.

Copyright ©2016 Global Knowledge Training LLC. All rights reserved.

8. Cloud-Computing Security Will Be Challenged

Cloud computing is a hot trending technology and will continue to expand for the foreseeable future. I think it is important to realize that the term "cloud computing" is a great industry buzzword that does wonders to hide or mask exactly what cloud computing is. Cloud computing is effectively remote virtualization. That's it. An organization hosts a hypervisor system on their equipment, sets up either software, operating systems, or networking to offer to others as a service, and then sells that product (or uses advertising for revenue) to customers as a cloud service. I don't mean to imply that the technology is bad or that it should not exist. It is a wonderful development that has pushed the boundaries of what it means to perform computing. Cloud computing offers numerous benefits that simply cannot be implemented in any other way.

However, cloud computing is not all rainbows and sunshine. Because your data is being stored and processed on computers sitting in someone else's building, it is at a higher level of risk than if it was sequestered inside your own building. The moment data leaves your premises, it is exposed to numerous additional potential violations. This is true of the transfer, storage, and processing of your data in relation to a cloud service.
I expect that in 2016 a significant breach of a cloud service provider will occur. This compromise is likely to affect dozens to hundreds of its customers in a very public and visible manner. Many of the larger cloud service providers have customers which are large and popular online sites and services, such as retail stores, discussion forums, social networks, file repositories, smart home device backend, and wearable services. If one cloud company is breached, many of the most widely used sites and services could be affected, meaning just about everyone with a digital lifestyle will be impacted by the breach.

9. A Drone Will Be Involved in a Serious Security Breach

Drones, or unmanned aerial vehicles (UAVs), have become a popular hobbyist activity as well as used in many professional capacities. UAVs are useful in survey work, videography, sensor readings, journalism, law enforcement, search-and-rescue, research, military, delivery, and farm management. However, they are not without contention, as they can and have been used to violate privacy, damage property, violate laws and regulations (such as airspace around airports or into restricted areas, such as military bases or the White House lawn), are quite noisy, and can be used as weapons. Drones have long been used themselves as weapons by the military. However, consumer or commercial drones have only recently been known to have been armed with explosives, handguns, or flame throwers.

In 2016, we will likely see the usage of a consumer-grade drone to implement a serious security breach of a secure business or military location. The drone could be used to gain access to a wireless network, to breach physical security, or possibly to plant a listening or monitoring device. The breach will be more serious than taking aerial video of a private or confidential area and will result in granting the attacker(s) physical or logical access into the target. This security violation will trigger additional highly onerous laws and regulations to be implemented against the entire UAV community, possibly even expanding into model airplanes, helicopters, and rockets.

10. Cyber-Warfare with Consequences to Civilians Will Increase

It should be no surprise to anyone that governments and militaries across the world, including the United States, are using hacking as a cyber-warfare offensive weapon. There has been some public acknowledgement of this in the press, but mostly due to leaks and data breaches that revealed the attacks. Cyber-warfare has been used to spy on foreign officials, track down malicious agents, or compromise systems associated with enemies of the State.

Copyright ©2016 Global Knowledge Training LLC. All rights reserved.

Generally, the cyber-warfare attacks against other nations have not caused any significant harm to individual non-combative citizens, but that trend is not a guarantee into the future. I predict that in 2016, evidence will be revealed of a nation/state-level cyber-warfare attack that will have serious consequences for otherwise innocent citizens. The harm to individuals will be known and real, but the cause of the harm will not be initially revealed.

After journalistic research or a security leak, details of the cyber-warfare event will be disclosed detailing which country attacked and how its attack caused a violation of the safety and security of the victim country's citizenry. This event is likely to cause outrage amongst the populations of both the victim country and the aggressor nation. There may be justifiable reasons why war of one type or another must be waged, but when innocents are affected by those warfare actions, most agree this is an appalling consequence that should be avoided. The outrage of this event may cause international response encouraging the adoption of a treaty limiting the type of attacks used in cyber-warfare to harming only the government and military entities of a nation, and avoiding any intentional harm to businesses and citizens. However, this type of resolution is unlikely to have any significant effect on how cyber-warfare is waged in the future.

Conclusion

2016 is ripe for a wide range of disastrous consequences to occur. My listing of these 10 predictions is not meant to encourage these violations, but instead a call to response to work toward avoiding these unwanted events, minimizing their effect, or preventing their materialization altogether. We each have a responsibility to pay attention to our own personal safety and security both in the real world and in our newly acquired digital world. Our responsibilities are not limited to ourselves; we are also accountable for overseeing the safety and security of our friends, family, and neighbors. It is our duty as citizens of this planet to help everyone achieve a higher level of sanctuary against the malicious actors and events of this world. Pay attention. Be proactive. Stay secure.

Learn More

Learn more about how you can improve productivity, enhance efficiency, and sharpen your competitive edge through training.

- CISSP Certification Prep Course
- Certified Ethical Hacker (CEH) v9
- Security+ Prep Course
- Cybersecurity Foundations

Visit **www.globalknowledge.com** or call **1-800-COURSES (1-800-268-7737)** to speak with a Global Knowledge training advisor.

About the Author

James Michael Stewart has been working with computers and technology for over thirty years. His work focuses on security, certification, and various operating systems. Michael has teaches job skill and certification courses, such as CISSP, ethical hacking/penetration testing, computer forensics, and Security+. He is the primary author of CISSP Study Guide, 7th Edition and CompTIA Security+ Review Guide: SY0-401.

Michael has also contributed to many other security focused materials including exam preparation guides, practice exams, DVD video instruction, and courseware. In addition, Michael has authored or co-authored over 80

Copyright ©2016 Global Knowledge Training LLC. All rights reserved.

books on a range of security, certification, networking, and administration topics. He has developed certification courseware and training materials as well as presented these materials in the classroom.

Michael holds a variety of certifications, including: CISSP, CEH, CHFI, ECSA, and Security+. Michael graduated in 1992 from the University of Texas at Austin with a bachelor's degree in philosophy. Despite his degree, his computer knowledge is self-acquired, based on seat-of-the-pants hands-on "street smarts" experience. You can reach Michael by email at michael@impactonline.com.

Copyright ©2016 Global Knowledge Training LLC. All rights reserved.