Security Outlook:
Look Out! What to watch for in 2015

Presented by:
W. Jackson Schultz
Security Consultant – Information Security Practice
GraVoc Associates, Inc.

GRAVOC
ASSOCIATES
“Our Business is Your Success!”

81 Main Street
Peabody, MA 01960
www.gravoc.com

As we come upon the New Year, most security professionals will instinctively be thinking about what threats exist to their organization throughout the holiday season and what will be introduced next year. Holiday consumers are shopping very uneasy considering all the breach related news from this and previous years. It is crucial to identify past cyber security threats, remain diligent in the moment, and prepare for whatever the future will bring.

In previous years, we have seen a mass of increasingly new advances of cyber security attacks throughout different industries, like financial services, education, and healthcare. These occurrences have resulted in identity theft and financial fraud, and have also led to hefty fines for different corporations and businesses. These attackers are hacktivists, state sponsored attackers, terrorists, or just criminals trying to make a quick dollar. The only thing for sure that will come of 2015 is that information protection responsibilities will no longer be owned solely by security professionals but rather will encompass an organization as a whole, from chief executive to entry level employees.

- **2012:** Distributed denial of service (DDoS) attacks – these DDoS attacks hit various financial institutions, including banking giants such as Bank of America, PNC, and SunTrust, and took them offline for several hours.
- **2013:** Social engineering and internal threats – the buzzword "social engineering" was reintroduced as an industry staple, rather than a term previously tied to Kevin Mitnick and Frank Abagnale. Cyber security experts noted a major increase of internal threats; researchers found that those with intention to harm an organization for which they work typically succeed in their efforts, and can go undetected for a long period of time, up to three years in some cases.
- **2014:** Holes within encryption previously deemed secure – The openSSL Heartbleed bug and the Shellshock (bash) bug both proved a major vulnerability from encryption to a hole within every UNIX based operating system developed. This includes Linux servers and Apple's OS X.

In 2015, immerging threats will be Corporate Account Takeovers (CATO), social engineering, exploitable holes within security measures previously thought safe, especially in older open-source software that has since become an industry standard, an increase in ransom-ware, and exploits of the Cloud.

CATO is currently a popular buzzword, and will maintain its title as we head into the New Year. As big of a threat as CATO is, there are many ways to help prevent these takeovers. It is key to maintain strong password controls, enabling complexity, ensuring an inactivity lock as employees leave their desks, installing a strong anti-virus, using encryption, among others. Employees also should be regularly trained on red flags to identify phishing emails by performing social engineering tests. It is not uncommon for employees to even open emails that are flagged as a threat and enter their personal credentials.

Social engineering is another term that is becoming a staple of the information security industry. Fraudsters who practice social engineering try to exploit others' good nature to convince them to share sensitive information, including social security numbers, bank account numbers, login credentials, names and addresses. These criminals can pretend to be a consumer, a member of a different department, a vendor, or a supervisor. Conducting social engineering exercises, specifically pretext calling tests, and training employees on best practices to identify threats is the only way to combat these kinds of attacks.

Open source applications are a blessing and a curse. On one end, they are very customizable, and can be used within a business in a variety of ways. At the same time, this means that the source code is accessible to everyone. Hackers will commonly try and find vulnerabilities within the code or make tweaks to create exploits. It is important to patch systems, install updates as often as they come, and regularly test the application for potential breaches.

Ransom-ware is another growing threat. Ransom-ware is a form of malware that is downloaded on a business' or consumer's machine because of poor practices, such as clicking on a malicious link, and encrypts all the information on the hard drive. This information cannot be backed up or copied and is inaccessible until the amount is paid to the hacker (hence the name). In most cases if the data is not paid within 96 hours, all of the information of the machine is wiped. The price of the information is never extremely high, and is definitely a 'small price' to pay for the data that could potentially be lost.

Cloud hacks and exploits are also seem to be on the rise. There is much complication surrounding this because an organization like a bank storing personally identifying customer information or a hospital storing electronic health records (EHR) has no option but to trust their service provider. If the provider has an unqualified SOC 2 report done by a reputable CPA firm, this should, in theory, be all that is needed to put a customer at ease. Unfortunately, that is not the case. It is important to maintain diligence and continue to make sure no data has been altered or stolen by monitoring change logs within the system and reviewing audit reports. Cloud providers will notify a user if their data was breached. Alternatively, if a customer notices the breach, it is their duty to notify the provider.

Fortunately, as these threats develop, industry professionals are not tasked with finding new prevention methods but are instead focusing on detection and incident response techniques. The federal government and law enforcement agencies have recognized the importance of an efficient response, information sharing is continuing to improve, and the media has made an effort to report any breach or hack to the public to maintain awareness. Regulators in each industry are also cracking down to ensure best practices are being followed from password controls to specific policies and procedures contained in an information security program.

Over time, it is easy to see emerging trends, patterns in security and how hackers are trying to break into systems. Repairing security holes that we know exist and taking preemptive action to ensure no vulnerabilities that have previously been exploited tends to be simpler than combating those that industry professionals are unaware of. As a group, cyber security experts are tasked with one specific job: to prevent attackers from exploiting security flaws that we do not even know exist.

The question then remains, how is an organization supposed to combat the bad guys when they are using breach methods previously untested? While there is no clear-cut answer, there are industry best practices that can be adapted related to mitigation techniques. True layered security is a defense that can used which combines an array of security controls in order to best protect sensitive information. Examples of this would be to amalgamate single sign-on (SSO) with multifactor authentication (MFA) and network folder encryption. It should also be noted that the fluctuation of new threat prioritization within the security industry will ideally result in an annual reassessment of budgets related to mitigation and prevention. When this reallocation of funds is in process, remember to make sure that the object your organization is paying to protect is truly worth the measure of security you're surrounding it with. In other words, do not spend more on security than the object or data is worth.

There are groups such as the Federal Financial Institutions Examination Council (FFIEC) who develop strict guidelines that should be followed meticulously. There are trade associations such as BITS, the technology policy division of the Financial Services Roundtable, who host Member Company working groups, compose whitepapers, and are some of the leading experts into financial services technology, security, and fraud prevention. Financial Institution technology professionals' continued education maintains to be of growing importance.

The Financial Services industry has set the standard for threat mitigation and prevention, compliances rules, and security policies. Regulators of other industries such as healthcare, retail, organizations who handle credit card transactions, among others are moving towards stricter legislation and seem to be modeling themselves after financial services regulators. Some also use NIST as a guideline to compose their compliance standards, because NIST seems to be relevant from a security standpoint.

The question then becomes, why wait for these guidelines to be published? Security professionals know there is potential for a breach, regardless of industry. We also know some industry best practices that are effective, and some that aren't. Wouldn't knowing that financial institutions have stricter guidelines to follow mean that less regulated and more exploitable organizations who hold personally identifying sensitive data should anticipate being attacked? Absolutely.

There is a common misconception that compliant is synonymous with secure, and interchanging those terms can lead to a false sense of security which is almost as dangerous as not having any controls in place at all. Security is an industry that leaves professionals room to be creative and the ability to not need to follow every guideline to the lowest level, but rather just apply the required standards and improvise the rest.

The United States is seeing breaches to law firms, healthcare businesses, accounting firms, colleges and universities, manufacturing companies, and even some sports franchises. At some level industry professionals must recognize that history repeats itself. Flaws that existed within financial institutions that have since been prevented could still exploitable in other industries that have not taken legitimate precautions and adapted best practices.

The only true solution to maintaining vigilance and security, regardless of industry, is to stay educated on emerging trends, working with outside firms and vendors, and to continue information sharing. We live in an age where data is so easily accessible, meaning that there is no excuse to remain in the dark related to anything that could harm your organization.