Trends to watch out for in 2016:

The cyber insurance market will dramatically disrupt businesses in the next 12 months. Insurance companies will refuse to pay out for the increasing breaches that are caused by ineffective security practices, while premiums and payouts will become more aligned with the actual cost of a breach. The requirements for cyber insurance will become as significant as regulatory requirements, impacting existing businesses security programs.

2015 was a tough year for businesses, and the trend for 2016 looks to be no better. Against this backdrop is the gradual realization within corporations that the value of their company's data is a large part of corporate assets, and a huge potential cost during a cyberattack event. Such losses comprise not only that data related to customers, but also to employees.

Prediction: Risk model is a fast moving, impossible to predict, and a difficult to understand model. With DTP (Data Theft Prevention) adoption dramatically increasing in mainstream companies.

A November 2015 Wells Fargo survey of U.S. companies with $100 million or more in annual revenue found that 85 percent have purchased cyber or data privacy insurance, primarily to protect the business against financial loss. Of those with policies, 44 percent have filed a claim as a result of a breach.

Not all companies are created equally and not all companies pose equal risk for an insurer. Different sectors face different encounter rates for threats, with the Healthcare sector leading the list of more likely than others to encounter specific threats, including dropper files, lures, redirects and advanced malware. As for retail, it stands still at the 4th most likely to be attacked. Showing how the industry and company culture may influence the likelihood of threats and risk.

The takeaway from this, is as cyber insurance is becoming more mainstream, the impact of verifiable security risk exposure, including continuous monitoring of corporate networks for risky user behavior, and regularly training employees to be smart with email attachments and browsing behavior will be increasingly tied to the bottom line. Ultimately, cyber insurance will drive companies to adopt security postures to handle threats, leading to minimising data theft and strengthening prevention methods.

Because data has value to criminals, they began to spread their attacks to steal data much more widely than ever before. From retail, pharmacy, healthcare and insurance industries; to university systems and financial service companies; and even to attacks against prominent security companies; data is money to attackers, and in 2015, they made a lot of money from stolen data.

Prediction: Mobile wallets and new payment technologies will introduce additional opportunities for credit card theft and fraud

As criminals look to shift their game plans, there are three distinct areas we see attackers migrating to: newly introduced infrastructure, new payment methodologies and mobile wallets. Mobile technology and retail innovation is rapidly morphing payments methodology. With security not being the first priority for those seeking to alleviate payment friction, convenience has often trumped security in these rollouts.
While it may seem that the act of swapping one payment terminal for another is without hazard, the introduction of this new hardware will inevitably lead to security gaps exploited by attackers. This is further complicated by the fact that it can be more difficult to dispute fraudulent charges made using these new "safer" cards. Integrating new technology and processes securely is a painstaking process. While many will take every measure to do so, the massive scale of change will present significant chances for criminals to attack poorly configured devices, or their network connections.

NEW PAYMENT METHODOLOGIES

While this shift is occurring, there is an increasing push for retailers to take advantage of new technologies to streamline the payment process. The increase in nontraditional payment methods via beacons (a system to allow retailers to detect a mobile app user's presence in the store), online, and smart shopping carts is opening up the doors for a new wave of attacks. Less rigorous security oriented implementations of these systems will leave them vulnerable.

As adoption and the types of transactions capable on mobile phones increases, malware authors will also increase their efforts to steal from a digital wallet. Mobile malware will evolve to use these payment methods to commit fraud, with ransomware on mobile coming as a result of the increased significance of the mobile device in commerce. Some banks are already taking action to diminish their responsibility for attacks associated with third-party payment applications that link to accounts at the financial institution.

With the wake of the BYOD (Bring your own device) phenomena years ago, more corporations are seeing the results and indirect cost of allowing BYOD into the business paradigm. Taking advantage of their residency on the infected device, attackers have a head start to compromise the business network, with plenty more money to be had. Emails, contacts, authentication measures and apps that access the corporate network from the phone can become a phenomenal source of intellectual property, insider information and other confidential business materials becomes easily obtainable and can net an attacker sizable treasure.
The takeaway from this, is that the enterprise must acknowledge that the technological push by attackers against the mobile platform to commit fraud will also enable others who wish to breach the enterprise, not just retailers. As new mobile and payment technologies stretch and extend the traditional notion of a network, organizations must look to prioritize the protection of data by monitoring industry best practice and implementing security protections prioritizing data protection.

Prediction: New opportunity for Social Engineering using gTLD (generic top level domains)

The Internet community has seen a major change in the domain name registration system, with the increased adoption of new generic top level domains, as a result, criminals who populate the new top level domains win a much larger proportional presence than in existing, more common top level domains (TLD). This is a demonstrated behavior with all new technologies when introduced, it is often the fringe elements of the Internet that first moves into them.

The old Internet of .com, .edu, .gov, .net, .org, and .info; is about to get a lot more generic with the implementation of expanded (gTLD) by the Internet Corporation for Assigned Names and Numbers (ICANN) means that you are now beginning to see many more URLs ending in .club, .xyz and .guru.

Will consumers shopping for a computer steer towards shop.apple, apple.macintosh or apple.computer? While there has been a tremendous effort by ICANN to ensure that brands have an opportunity to control the TLD of their names, this hasn't prevented controversy and contesting for specific terms. This potential confusion is a golden opportunity for criminals and nation-state attackers to create highly effective social engineering lures to steer unsuspecting users toward malware and data loss.

New gTLDs will definitively be used in active spam and other malicious campaigns. With attackers well entrenched within the new domains, before legitimate users, consumers will eventually hesitate before casual navigation. These gTLDs will also make it significantly harder for businesses to protect as many. This will prompt IT leaders to demand being involved earlier in the process with how to approach new technologies on the Internet.

We clearly see where 2016 is heading towards, and having educated business employees is a must in today's world of technology and Internet dependent life. As early as we start the year, a new threat the "Ransom32" malware is released into the wild, with the ability to infect Windows, Mac and Linux.

Ransomware, as known by a lot of people, are nasty pieces of software that encrypt files on a Windows system, and then threaten users that their data will be lost forever, unless they pay up. Many have surfaced in the past year, like a program that scrambles your computer's file names, and another that even offers a 'referral program,' turning victims into perpetrators. And more recently, such programs have evolved, now targeting a wider range of computers. Enter Ransom32, one of the newest ransomware for the New Year. The program is written in Javascript and can infect systems running on the Windows platform and also have the capability of targeting Mac OS X or Linux computers.

The program will be distributed via the usual methods of spam emails. It can be received as a packaged ZIP/RAR file, the archive has the capability to extract all by itself, utilizing the scripting language in order to make the malicious program always launch at startup, and execute the files inside it, successfully locking up a victim's computer using a 128-bit AES encryption. The usual behavior of Ransom32 is targeting data on a computer with file extensions such as .jpeg, .mp3, .mov, .mp4, .docx, .csv, .xlsx, .xml, .dat, and .pptx, among many others.

It's always an advantage if users are aware of how their behavior and approach to technology impacts the corporate IT environment and the business. Cooperating with IT to ensure that files are properly backed up, before such incidents take place is critical to the users data at an early stage, and before being infected as using methods to remove this software after it has encrypted the files can result in their permanent damage, and most of all, users must be cautious when opening email attachments that look suspicious.