

AUTHOR PROFILE:

KEVIN PRINCE,
CHIEF TECHNOLOGY OFFICER

Named Chief Technology Officer of Perimeter in 2009, Kevin Prince spearheads the company's technology strategy and leads the technical team in working closely with its customers to manage all of the complexity and compliance requirements of securing information across the enterprise.

With more than 19 years of expertise in Information Technology and 11 years focused on Internet security, Mr. Prince is an evangelist on Internet security topics, including network security threats, fraud, identity theft, cyber terrorism and data breaches. Through regular speaking engagements, webinars, whitepapers and blog postings, Mr. Prince is dedicated to educating organizations on how to manage information complexity, meet increasingly stringent compliance and security requirements, and mitigate risk. Mr. Prince has trained federal examiners for several years.

TOP 10 INFORMATION SECURITY THREATS OF 2010

2010 is upon us. I am amazed that it has been a decade since all the fear and speculation of Y2K. Take a moment to review your personal technological transformation in the last 10 years. Were you using a mobile phone 10 years ago? Could you live without it today? How about how far the Internet has come and your reliance upon it? Did you ever imagine you would use technologies like Facebook and Twitter as often as you do? Did you ever imagine that cyber security would be such a huge issue that you have to deal with it personally, every day?

2009 IN REVIEW

Some big predictions were made last year. Lets start by seeing how we did.

The volume and severity of attacks from international sources did increase substantially. Many of these attacks were targeted towards the government and military. There were many stories and articles on this topic in 2009 that confirm the predictions made last year. We also saw a strong increase in targeted attacks towards utilities and other critical infrastructure systems. It wasn't just the U.S. either; this was widespread across many nations.

As predicted, botnets did not pose a significant threat, especially to small and medium sized businesses. While botnets such as those based on "Conficker" were feared and there were even some days when some in the industry braced for something big, nothing much happened that caused a large scale impact.

Another prediction was an increase in the exploit of buffer overflows. Some have reported that close to 90% of exploits in 2009 targeted Microsoft buffer overflow vulnerabilities. (see [Microsoft Security Bulletin MS08-067](#))

One big shift last year was predictions tied to the downturn in the economy and the impact that has on information security. Malicious insiders were listed as the #1 threat for 2009 and were listed as a rising threat. According to a survey released in October of 2009 by Actimize and reported by DarkReading, nearly 80% of financial institutions worldwide say the insider threat problem has increased in the wake of the economic downturn. 70% of financial institutions reported incidents of insider fraud in the last 10 months. Nearly half of the banks in the Actimize survey say they are losing 1 to 4 percent of their total revenues to insider fraud.

2010

Now we look into the future. What do we have to worry about in 2010 from an information security perspective?

TOP 10 INFORMATION SECURITY THREATS FOR 2010

#1 - MALWARE (RISING THREAT)

In 2009, Malware was listed as a “steady threat” and the 2nd highest ranked threat to organizations. I underestimated the dramatic increase in malware in 2009. Due to that increase and the number of organizations that are affected each day by malware, I have elevated it to the #1 position. This is a bit controversial since most security experts would list insiders as the top threat, but I believe in 2010 more organizations will be negatively affected by malware than by malicious insiders.

There are so many methods employed today to get malware installed on systems. One primary method is through the use of client-side software vulnerabilities. These are usually 3rd party applications that are exploited such as Adobe Acrobat, Quicktime, Flash¹, and even Microsoft Office. Client-side applications are not patched nearly as frequently as operating system vulnerabilities. Browsers remain a top target for vulnerabilities that criminals want to exploit as well. Browser flaws and subsequent patches were common news in 2009 and will likely be in 2010.²

Malware is most often getting installed on systems when the user is lured through any number of methods to malicious or compromised websites that can exploit one of these client-side vulnerabilities. Once the malicious software is installed, it acts as a Trojan horse software program performing any number of malevolent acts including information stealing keyloggers, fast flux botnets, relays, and remote control agents. In 2009, the Zeus Trojan began spreading via drive-by downloads³ (malware sites that automatically infect systems that simply browse the webpage) and was capable of spreading, capturing financial data, and a variety of other things. IBM reported that during the first half of 2009, malicious links on websites increased by 508%.⁴

Much of the malware distribution is performed by organized cybercrime networks. In 2009, the FBI reported that for the first time ever, revenue from cybercrime had exceeded drug trafficking as the most lucrative illegal global business, estimated at taking in more than \$1 billion annually in profits.⁵ Individual hackers and groups loosely tie themselves together into an organized criminal hierarchy where common goals are achieved through a reward system.

Malware is used in all the major cases you hear about in the news. Heartland, TJMaxx, Hannaford, and many other companies have seen the effects of malware installed on their systems. Many organizations go months and sometimes years before the malware is discovered. According to a study released by the Verizon Business Risk Management group, malware contributes to about one third of data breaches.

1. <http://www.scmagazineus.com/researcher-finds-frighteningly-bad-adobe-flash-flaw/article/157734/>

2. <http://blogs.zdnet.com/security/?p=4990>

3. <http://www.scmagazineus.com/zeus-spreading-through-drive-by-download/article/158691/>

4. <http://www.h-online.com/security/news/item/IBM-Report-Phishing-is-going-out-of-style-743159.html>

5. <http://www.technewsworld.com/story/47559.html>

TOP 10 INFORMATION SECURITY THREATS FOR 2010

#2 - MALICIOUS INSIDERS (RISING THREAT)

Malicious insiders were listed as the top threat for 2009 but have fallen to the #2 spot for 2010. With the downturn in the economy, it was no surprise that many desperate and disgruntled employees attempted to exploit the companies they currently or previously work for. Here are just a few of the 2009 stories:

- The Fannie May former engineer who planted a logic bomb that (had it not been discovered) would have shut down the company for at least a week by decimating all of their 4,000 servers. It would have cost the company millions in lost productivity and damages.
- Luis Robert Altamirano accessed a system a year after he was no longer an employee at United Way. He deleted files and disabled the voicemail system.⁶
- The University Medical Center in Las Vegas learned that an employee allegedly leaked confidential patient data including Social Security numbers, billing data, and full descriptions of injuries and it has been reported that the information was sold.⁷
- A T-Mobile employee stole customer records and sold them to a data broker who in turn sold the data to T-Mobile competitors. It included millions of records that contained valuable information such as account expiration date so competitors could target those customers at the time they may look for a new provider.⁸
- After a series of disputes with executives and investors, the former YouSendIt co-founder and CEO left the company and later launched a denial-of-service attack against YouSendIt systems.⁹
- Former Bank of New York Mellon employee Adeniyi Adeyemi was indicted on identity theft charges. He was charged with grand larceny, identity theft, and money laundering after stealing and using New York Mellon employee information. He opened phony bank and brokerage accounts where he deposited stolen money.¹⁰
- A former DuPont research scientist is facing federal criminal charges for allegedly trying to steal trade secrets.¹¹
- A hospital security guard at a Dallas, Texas hospital had been planning an attack to be launched July 4. He had been installing malware on several systems at the hospital including the environmental control system and many systems that contain sensitive data.
- A former bank employee attempted to steal 1.9 million after their successful theft of more than 1.1 million in April 2005 and May 2006. Ansir Khan used his position at the bank to extract customer information and shared it with accomplices who performed the theft.

#3 - EXPLOITED VULNERABILITIES (STEADY THREAT)

Some might wonder why exploited vulnerabilities are listed in the malware section, but then also have a section of their own. Well, malware often relies upon exploited vulnerabilities to be installed properly. At the same time, user behavior can do it as well through social engineering techniques. Vulnerability exploit is at the heart of hacking and data breaches. Worms, viruses,

6. <http://miami.fbi.gov/dojpressrel/pressrel09/mm112409.htm>

7. <http://www.lasvegassun.com/news/2009/nov/21/fbi-looking-umc-records-leak/>

8. http://www.darkreading.com/database_security/security/privacy/showArticle.jhtml?articleID=221900209

9. <http://news.zdnet.co.uk/security/0,1000000189,39852055,00.htm>

10. <http://www.scmagazineus.com/NY-bank-computer-technician-charged-with-ID-theft/article/156711/>

11. http://www.computerworld.com/s/article/9139014/Former_DuPont_researcher_hit_with_federal_data_theft_charges?taxonomyId=17

TOP 10 INFORMATION SECURITY THREATS FOR 2010

malware, and a host of other attack types often rely on vulnerability exploit to infect, spread, and perform the actions cyber criminals want. According to a Microsoft Security Intelligence Report¹², Conficker was the top threat to enterprise computers during the first half of 2009. Worm infections have doubled between the second half of 2008 and the first half of 2009.

With organizations still not doing what they need to for patch management, vulnerability exploit remains a major problem. According to a Verizon study, the vast majority of data security breaches where vulnerability exploit was used relied upon vulnerabilities that had patches available for more than 6 months. There are several reasons this remains an issue. First, it only takes one unpatched system for your entire organization to be compromised. One system not up-to-date is all a hacker needs. Second, there are many applications loaded onto each and every system, many of which have weaknesses that can be exploited. Often these 3rd party applications are not patched. Few application vendors automatically update their software so this is a manual process if you don't use a commercial patch management package. For many enterprises, SMBs, and especially home users, this simply doesn't happen.

Last year I listed this vulnerability as a decreasing threat. In fact, that is still true for operating system vulnerabilities. But hackers have moved up the stack and are more often exploiting client side vulnerabilities and other vulnerabilities associated with 3rd party applications. As a result, this threat is being changed to "steady", which means we will likely see many more vulnerability exploits in 2010.

#4 - CARELESS EMPLOYEES (STEADY THREAT)

Careless and untrained employees will continue to be a very serious threat to organizations in 2010. Remember that insiders can be broken down into 3 categories: careless & untrained employees, employees that are duped or fall prey to social engineering type attacks, and malicious employees. The reason I think it is important to understand these categories of insiders is because protecting your network and critical/sensitive data is done very differently for each type. In a recent research report released by RSA¹³, accidental disclosure of sensitive information occurs far more frequently than deliberate incidents.

In the annual Perimeter E-Security data breach study¹⁴ released last year, it is noted that for data breaches between 2000 and 2008, more incidents happen by careless and untrained employees than any other type of insider incident. Careless insiders can be devastating to an organization. What is worse, this category of threat is one of the most controllable. Policies, procedures, training and a little technology can make a world of difference in reducing an organization's risk to careless insiders.

Take the employee of Rocky Mountain Bank¹⁵ for example. The employee was asked to send a loan statement to a customer. Not only did the employee send the information to the wrong email account, a file was attached that contained confidential information on 1,325 individual and business customers including their names, addresses, tax identification or social security numbers and loan information. The bank then sued Google to identify the recipient. Google refused. Google was then ordered to deactivate the recipient's account. Google determined that the email

12. <http://www.microsoft.com/downloads/details.aspx?FamilyID=037f3771-330e-4457-a52c-5b085dc0a4cd&displaylang=en>

13. http://www.theregister.co.uk/2009/08/25/rsa_accidental_security_breach_survey/

14. <http://www.perimeterusa.com/wp/Financial-Data-Breach-Study-2008.pdf>

15. <http://www.wired.com/threatlevel/2009/09/bank-sues-google/>

TOP 10 INFORMATION SECURITY THREATS FOR 2010

had never been opened and they deleted it. This is a case where the bank knew what devastating consequences disclosing the data breach would bring and went to great extremes to avoid that path.

Sometimes simply allowing employees to access their personal email can cause major problems. Scott Graham from Ohio sent his girlfriend (who he thought was cheating on him) an email laced with spyware. He was hoping the spyware would be installed on her home system, but she accessed the email from Akron Children's Hospital where she worked and it infected her computer. The spyware captured and sent a lot of sensitive information which constituted a data breach.

#5 - MOBILE DEVICES (RISING THREAT)

Mobile devices have become a plague for information security professionals. They are an easy way for a malicious employee to remove data from the corporate network. There are worms and other malware that specifically target these devices, such as the iPhone worm that would steal banking data and enlist these devices in a botnet.¹⁶ There was also the iPhone game maker that designed his game to harvest user information.¹⁷

USB thumb drives are also a problem. In the case of the Virginia Department of Education, an unencrypted flash drive containing personally identifiable information of more than 103,000 former students (including social security numbers) went missing. Many times it isn't the data that leaves on these little devices, but rather what they bring in. For example, the infected USB key that shut down a town council for four days.¹⁸ The USB drive was infected with Conficker and spread to many systems inside the network, wreaking havoc and costing them just under \$1,000,000.

Theft is still a major cause of data breaches. Mobile devices, especially laptops, are the main culprits. Tens of thousands of laptops are stolen each year. Often these have sensitive data that require public disclosure as a data breach. Blue Cross Blue Shield is being investigated after a laptop computer containing 800,000 healthcare providers' personally identifiable information was stolen in Chicago.¹⁹ In this case, the attorney general Richard Blumenthal said that one year of credit monitoring for the victims is "inadequate and unacceptable", while the cost of that alone would be tens of millions of dollars. We could have chosen any of the hundreds of stories in 2009 like this.

#6 - SOCIAL NETWORKING (RISING THREAT)

Social networking sites such as Facebook, MySpace, Twitter, and many others have literally changed the way many people communicate with one another. Due to many publicly disclosed breaches and compromises, we saw that these sites can be very real and serious threats to organizations. There are many Trojans, worms, phishing and other attacks targeted specifically at the users of these sites. One main problem is the inherent trust component these sites carry, much like email did many years ago. Furthermore, people that utilize these sites for entertainment purposes, such as online games, are rewarded for accepting friend requests even from people they don't know. This is very fertile ground for identity thieves. Some might say that

16. http://www.msnbc.msn.com/id/34115776/ns/technology_and_science-security/

17. http://www.theregister.co.uk/2009/11/06/iphone_games_storm8_lawsuit/

18. <http://www.scmagazineuk.com/ealing-council-facing-501000-fine-after-its-network-was-hit-by-a-virus-that-crippled-it-for-weeks/article/148144/>

19. <http://www.informationweek.com/news/healthcare/security-privacy/showArticle.jhtml?articleID=221601331>

TOP 10 INFORMATION SECURITY THREATS FOR 2010

there isn't enough information on their account to do any identity theft, but criminals are very resourceful. Just a little bit of information correlated with other sources of available information on the Internet can give someone all they need to steal your identity.

There is also a personal safety issue here as well. Social networking sites are a stalkers dream come true. With some people posting multiple times each day, you can know exactly what someone is doing all of the time. In a well publicized article,²⁰ the wife to the Chief of the UK International Spy Agency had information released on social network sites including the location of their home, where their children went to school and played, etc. Imagine the manipulation tactics, blackmail, kidnapping, and other things that could result by knowing this information, especially for influential people. Even friends and family can cause problems. Posts like "see you when you get back from vacation" can give others the vital information they need to commit crimes.

Employers are using these sites for a variety of reasons as well. They can use them to filter through applicants. One employee lost her long term sick leave benefits when the company she worked for found her "having fun" in pictures on Facebook.

Social networking sites are breeding grounds for SPAM, scams, scareware, and a host of other attacks. In June a scareware scam was spreading on Twitter with a message that simply read "Best Video" and contained a link to malware with a similar outcome to what was mentioned above.²¹ Social networking threats will undoubtedly continue to increase into 2010.

#7 - SOCIAL ENGINEERING (STEADY THREAT)

Social engineering is always a popular tool used by cyber criminals. Often, the more difficult it is to exploit vulnerabilities natively, the more they rely on social engineering to make up the difference. I mean really, why would you go to all the effort to exploit a vulnerability when a user will simply give you their username and password? Phishing is still a popular method for doing just that. But this is where the classifications blur a bit. Phishing in email is a social engineering threat, but is a phishing email on Facebook a social engineering threat? Or is it a social media threat?

Despite the mediums these tactics rely upon, tricking users into performing actions they wouldn't normally perform will remain very popular into 2010. In fact, these new venues make social engineering even more effective. For example, people are very skeptical when they get a phishing email, but are far less skeptical when they get a message on Facebook, MySpace, LinkedIn, Twitter, instant messaging and so forth. Most people are ten times more likely to click on a link or follow instructions from social networking messages than from regular email.

A method that found a tremendous amount of success in 2009 is scareware. The two most effect methods I saw were the "Blue Screen of Death" scareware and Fake Anti-Virus scareware. In the blue screen of death case, users would see what looks like a Microsoft blue screen of death and then be prompted to fix the issue by downloading and installing software. The phony program was called SystemSecurity and collects money from the user to remove the 'blue screen'. In an even more successful campaign, cyber thieves would have pop-up messages appear on the desktop of the user telling them they were infected with a virus. They would be prompted to buy, download

20. <http://www.cnn.com/2009/WORLD/europe/07/05/uk.spy.chief.facebook/index.html>

21. <http://www.eweek.com/c/a/Security/Twitter-Hit-With-Fake-Security-Software-Scam-663998/>

TOP 10 INFORMATION SECURITY THREATS FOR 2010

there and install a program to remove the infection. These programs were so insidious that they would actually disable the anti-virus software you already have loaded. Until resolved, the computer is nearly unusable. Cyber criminals are earning tens of thousands of dollars from these scams.

According to a report by IBM²², phishing attacks are on the decline. This is measured by taking the percentage of SPAM messages that are phishing emails and comparing 2008 to 2009. There was either a significant drop in phishing or a radical increase in SPAM. I believe one of the reasons for this is the myriad of ways criminals can send phishing messages outside of traditional SMTP email, like social networking mediums.

While generic phishing attacks seem to be declining, targeted phishing attacks are still an effective method for cyber criminals. Take the Aetna data breach this past year as an example. Hackers were able to extract 65,000 current and former employee information as well as 450,000 individuals who had applied to Aetna over the years. The criminal sent a targeted email that asked the individuals to go to a website (link provided) to fill out some more specific information to continue the process of their employment application. The information was then used to commit fraud. At Downeast Energy and Building Supply, in Maine, an employee received a spear phishing message that appeared to come from the company's bank. After clicking on the provided link, the employee entered the company's account access credentials, which the attackers then used to steal \$150,000.

2010 will have an added measure of complexity when it comes to social engineering attacks. Beginning sometime mid-2010, domain names will be expanded to include Japanese, Arabic, Hindi and even Greek characters. For years, people have analyzed the domain name to determine legitimacy of the site. With all these characters being available for domain names, no longer will looking at a domain help you determine if it is legitimate or not.

#8 - ZERO-DAY EXPLOITS (STEADY THREAT)

Zero-day exploits are when an attacker can compromise a system based on a known vulnerability but no patch or fix exists. Even a couple of years ago, zero-day exploits were pretty rare. They have become a very serious threat to information security. Many of these zero-day flaws reside in browsers and popular 3rd party applications. In November 2009 alone, Microsoft announced zero-day flaws in IE 6 and 7²³ and a Windows 7 zero-day vulnerability²⁴. Zero day vulnerabilities are being discovered in traditionally very secure protocols such as SSL and TLS as well.²⁵

The zero-day vulnerability may not even be in your systems, it could be in your providers. For example, web hosting provider Vaserv had an attack against 100,000 of their websites based on a zero-day exploit.²⁶ The HyperVM software they were using to run many virtual websites was compromised. In this attack, the perpetrators destroyed the sites. Some companies did not have backups of website data and files.

22. http://voices.washingtonpost.com/securityfix/2009/08/phishing_attacks_on_the_wane.html

23. http://www.computerworld.com/s/article/9141363/Microsoft_confirms_IE6_IE7_zero_day_bug?

24. <http://www.washingtonpost.com/wp-dyn/content/article/2009/11/16/AR2009111602221.html>

25. http://www.computerworld.com/s/article/9140362/Scramble_on_to_fix_flaw_in_SSL_security_protocol?

26. http://www.theregister.co.uk/2009/06/08/webhost_attack/

TOP 10 INFORMATION SECURITY THREATS FOR 2010

#9 - CLOUD COMPUTING SECURITY THREATS (RISING THREAT)

Cloud computing is a concept that is becoming very popular. While it still means a lot of things to a lot of people, using cloud based (i.e. Internet based) applications may not be as secure as you might hope. There were many stories in 2009 regarding cloud based security. Many are calling for forced encryption to access many of these services. While it seems ludicrous that this isn't done by default, you can't simply assume cloud apps are secure.

Some cloud computing security threats come in the form of vulnerabilities such as the October 2009 story that attackers exploited a web application flaw to hijack Yahoo Mail accounts.²⁷ This was a brute force attack where the hackers use software to systematically guess the passwords. Someone even went so far as to post the passwords, where there were many common ones such as "password" and "123456". Poor password policies and software that doesn't limit this type of attack will always lead to compromise.

As cloud computing becomes more popular in the next few years, we will see the issue of cloud security become a very big issue. There will be no shortage of cloud based security issues in 2010.

#10 - CYBER ESPIONAGE (RISING THREAT)

A threat that we hear about more and more all the time is Cyber Espionage. There has been a flood of stories in 2009 on this subject. Most of them of course surround governments and therefore have not been a huge threat to most individual organizations. A few of the incidents include:

- According to the US-China Economic and Security Review Commission's annual report to Congress, US Defense Department computer systems have been the target of cyber incidents 43,785 times in the first half of 2009, which if it continues at that pace will be a 60% increase over 2008.²⁸
- For one-third of US government agencies, security incidents are a daily occurrence.²⁹
- A National Journal article³⁰ talks about America's use of cyber terrorism tactics.
- 60 minutes reported on US cyber security in November 2009. While there was quite a bit of sensationalism, the piece spoke about verified incidents of cyber espionage including those targeting and compromising the countries power grid, military computer systems, and much more.³¹
- An attack on an alleged Syrian nuclear facility was aided by a compromised laptop.³²
- Evidence of North Korean involvement in July cyber attacks.³³
- The U.S. government opens a new cyber security operation center designed to help the government coordinate cyber attack responses.³⁴

27. <http://www.scmagazineus.com/rampant-brute-force-attack-against-yahoo-mail/article/149373/>

28. http://www.msnbc.msn.com/id/34108078/ns/technology_and_science-security/

29. http://www.govinfosecurity.com/articles.php?art_id=1931

30. http://www.nationaljournal.com/njmagazine/cs_20091114_3145.php

31. <http://www.cbsnews.com/stories/2009/11/06/60minutes/main5555565.shtml>

32. http://www.theregister.co.uk/2009/11/06/mossad_syria_trojan_hack/

33. http://www.msnbc.msn.com/id/33550486/ns/technology_and_science-security/

34. http://www.msnbc.msn.com/id/33557123/ns/technology_and_science-security/

TOP 10 INFORMATION SECURITY THREATS FOR 2010

- The US-China Economic and security review commission released a report entitled "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploration." According to the report, domination of an adversary's information flow is critical to Chinese military strategy. The report also states that China will likely conduct "a long term, sophisticated computer network exploration campaign."³⁵
- There is an interesting article entitled "Cybercriminals have penetrated the U.S. electrical grid". It is an interesting article showing the use of malware to map the entire network and grid.³⁶

BLENDING THREATS

Over the years it has gotten more and more difficult to classify threats because so many of them are blended. For example, a social engineering technique will be used to get someone to click on a link that infects their system with malware that is based on a zero-day exploit. Very few attacks utilize a single method.

You could take the top 10 threats and look at them another way. The threats from insiders (for the most part) include malicious insiders, careless and untrained insiders, social engineering attacks, mobile devices and social networking. Vulnerability exploit includes malware, exploited vulnerabilities, zero-day exploits and even some cloud computing and cyber espionage threats. But these broad based threat categories don't help create mitigation strategies. Obviously you will have different tactics to deal with careless employees as opposed to malicious employees. The solutions you employ to deal with the threats from social networking will be different than those from social engineering.

FALLING FROM THE TOP 10

Reduced Budgets

This threat was certainly a major player in 2009. Due to the downturn in the economy, this jumped into the top 10 for the first time in 2009. While 71 percent of SMBs believe a data security breach could put them out of business, three quarters froze or cut security spending according to a McAfee survey.³⁷ While this will likely continue to negatively affect organizations in 2010, it is not listed in the top 10. This is primarily due to so many other threats increasing so dramatically.

Remote Workers

Remote workers still represent a threat to organizations, however, this threat used to focus on an infected laptop being connected to the network. Today the greatest threat is not just remote workers, but all the various forms of mobile media they use. So in reality, this threat has morphed into the "mobile media" threat listed above.

Unstable 3rd Party Providers

Again, due to the downturn in the economy that hit so hard in 2009, it was projected that many vendors would reduce service quality or go out of business. While this happened, there is only anecdotal evidence of reduced service quality. All-in-all most companies fared better than expected.

35. <http://www.scmagazineus.com/Security-report-finds-Chinese-cyberspying-threat-growing/article/156013/>

36. http://www.computerworld.com/s/article/9131275/Report_Cybercriminals_have_penetrated_U.S._electrical_grid

37. http://www.mcafee.com/us/research/security_paradox/index.html

TOP 10 INFORMATION SECURITY THREATS FOR 2010

Downloaded Software

This was a problem in 2009. For example, areas of the US government banned the use of peer-to-peer software which enables the download of software that could be infected with Trojans, spyware, or other malware. A bill was even introduced in the US House of Representatives that would prohibit the use of P2P file-sharing technology in government computers.³⁸ This is in response to a flurry of problems with sensitive data being leaked via P2P as well as malicious downloads.

While downloaded software still poses a threat to organizations, it simply cannot be put in the top 10 for 2010.

QUICKLY CLIMBING TO THE TOP 10

Macking (Media Hacking)

Macking is a term coined in the up-and-coming book "Security 2020" to be released second quarter 2010. The book illustrates how over the next several years there will be high value placed in manipulating the media in conjunction with computer information systems to commit fraud and other crimes. We have already begun to see this type of behavior. Take a few stories in 2009 as examples:

- An Internet based "pump and dump" stock scheme netted 2.7 million.³⁹
- Climate research documents stolen and posted to the Internet just before the international climate summit. The documents supposedly show that researchers are not disclosing research that isn't in support of climate change.⁴⁰
- Several high profile celebrities passed away during 2009. Inevitably what followed were false media reports, compromised Twitter accounts sending false information, and Facebook and other social media outlets exploited over the news.
- Some celebrities didn't even have to pass away to become fodder for this type of behavior. Britney Spears, Jeff Goldblum and others were victims of Macking.

While this is still in its infancy stage, manipulating the media through online means will become an effective tool in criminal arsenals.

CONCLUSION

Information security is an ever evolving discipline that requires tremendous expertise, time, and money to effectively manage. Each of the top 10 threats for 2010 could be broken out into a separate whitepaper with mitigation strategies, tactics, and solutions. Every organization should take stock of what they are doing today, how well their current solutions mitigate the risk of the top 10 threats, and make adjustments where necessary. In some cases, new technology should be implemented. Other technology may be of little value and can be discarded. Other threats will only be able to be addressed through policies, procedures, training and enforcement. Proper information security is fluid and dynamic. Be sure your organization is properly preparing itself for what cyber criminals, thieves, spammers, phishers, hackers, and all manner of society's underbellies are planning to do to exploit you in 2010.

38. <http://www.washingtonpost.com/wp-dyn/content/article/2009/11/17/AR2009111703841.html>

39. <http://www.justice.gov/opa/pr/2009/November/09-crm-1275.html>

40. <http://news.bbc.co.uk/2/hi/science/nature/8370282.stm>