

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 BREACHES & BLUNDERS OF 2009

2009 was a banner year for information security news. Rarely did a day go by where a data breach of some sort wasn't announced. What would once have been headline news for at least a week now barely makes the ticker on the bottom of CNN. That being said, as we enter 2010 we are seeing more and more regulatory control, fines being levied, lawsuits being filed, and much more. Data security breaches are nasty business and should be avoided at all costs.

Let's take a look at the top 10 biggest information security breaches and blunders from 2009.

#10 - NETWORK SOLUTIONS INCIDENT

You would think that a company like Network Solutions would be the least likely to be compromised. I mean, they register the domain names and host the web sites and email accounts. If anyone is good at Internet security, it should be them. Well, hackers broke into web servers owned by the domain registrar and hosting provider and planted rogue malware that resulted in the compromise of more than 573,000 debit and credit card accounts. The hackers successfully kept this malicious code in place for over 3 months. This "extended stay" of malicious code on systems is a trend we saw progress in 2009 and will show up again in this list.

#9 - STRONGWEBMAIL BLUNDER

The company StrongWebmail made the mistake that most mature security companies do not. They offered a \$10,000 prize to anyone who could hack into their CEO's mailbox. StrongWebmail uses an authentication method that involves sending a one time pin code to your mobile phone. StrongWebmail was so confident in their authentication process, they even gave the user name and password out to help people try to break in. Well, a team of guys was able to break in, effectively bypassing the 2nd factor authentication using a cross site scripting vulnerability. Essentially, they just found a workaround. StrongWebmail was a little embarrassed but paid the \$10,000. That being said, the biggest problem here is you just don't do that. Good security professionals know that if a talented hacker wants to get into something, it is only a matter of time. That is why layers of defense are necessary. The more difficult you make it, the more likely they will go after other low hanging fruit...that is unless you are offering 10k cash.

#8 - THE JEALOUS BOYFRIEND

An Ohio man (Scott Graham) sent an email to his girlfriend which contained spyware (sounds like he thought she might be communicating with someone else and cheating on him). Unfortunately for Mr. Graham, his girlfriend opened the email on her work computer, resulting in an installation of the spyware on her work system rather than her home system. Mr. Graham began to receive information in his email box which included sensitive medical information. This constituted a data security breach on the part of Akron Children's Hospital. While he will spend up to 5 years in

TOP 10 INFORMATION SECURITY BREACHES & BLUNDERS OF 2009

prison and has to pay \$33,000 in damages to the hospital, it makes me think of what the hospital could have done to eliminate this threat. While the spyware would have likely ended up on some system, it didn't have to be the hospital's system. Many organizations still allow employees to access their own personal email from work. While using a web content filtering solution would likely help a situation like this, it wouldn't completely eliminate it. Other organizations are also implementing desktop controls that prevent end users from installing any software. That right is reserved for the IT administrator. This would have really helped out the hospital. However, I am still amazed just how apathetic some healthcare organizations can be towards information security.

#7 - MACKING

This has been quite a year with several celebrities that have passed away including Ed McMahon, Farrah Fawcett, and of course Michael Jackson (wait, that was just one week). As a result, there were a flurry of scams that attempted to get people to click on links, open attachments, and do an assortment of other things. In addition to this, we are seeing people taking advantage of the media and how quickly bad information can be spread in our "instant information" society. Stars that in fact are alive and well had "passed away" according to Internet blogs, web posts, Twitter, Facebook, and even some television stations. A hacker even broke into Britney Spears Twitter account and posted a message to all her followers that "Britney has passed today. It is a sad day for everyone. More news to come".

Manipulating media, in other words Media Hacking or "Macking" (as we have decided to call it), is becoming quite popular. There are, of course, many ways this can be facilitated. Macking can be very profitable for cyber criminals, and in this day in age when search engines can be manipulated, botnets can send billions of email messages, and social networking sites have worms and viruses that can spread messages, it is easy to see why they do this.

In my opinion, Macking is the lowest of the low hanging fruit. It is practically the fruit that falls off the tree and rolls to your feet.

#6 - INSIDERS EVERYWHERE

What a year 2009 has been for insider breaches! The scary thing is, I am sure there is a large percentage of these types of cases that get swept under the carpet, are yet to be announced, or continue to go undiscovered. I'll outline a few breaches caused by malicious or careless insiders.

Symantec had an International office employee steal customers credit card numbers. They only made the announcement about the breach once the BBC reported that they had purchased the credit card numbers from a Delhi-based man. Most of the compromised customers were in the U.S.

A temporary employee from AT&T was arrested on charges that she stole personal information on 2,100 coworkers and then pocketed more than \$70,000 by taking out short-term payday loans in the names of 130 of them.

What did my mom say about curiosity? Kaiser Permanente hospital in Bellflower, CA, was assessed a \$250,000 fine for failing to prevent unauthorized access to confidential patient information. A second fine of \$187,500 was slapped on them for the same infringement.

TOP 10 INFORMATION SECURITY BREACHES & BLUNDERS OF 2009

Then there is the case of the laptop stolen with information on 800,000 doctors in its database. That's practically every doctor in the United States. The culprit in this case is allegedly an employee of the Chicago-based Blue Cross and Blue Shield Association who downloaded the information on his personal computer.

Insiders, whether malicious, untrained, or simply careless, are a rising threat for 2010 and beyond.

#5 - UNIVERSITY OF CALIFORNIA BERKELEY LAPSE

Come on in. Take your shoes off. Kick up your feet. Stay a while. This is what most hackers are doing (as I mentioned in #10). In the University of California (Berkeley) case, personal information of 160,000 current and former students and alumni may have been compromised. It included Social Security numbers, health insurance information, and other medical information all the way back to 1999. While the breach was discovered April 21, 2009, the database had been illegally accessed by hackers beginning on October 9, 2008, over six months prior. TJX and Heartland were both 18 months prior to discovery. There are many other cases where they don't even know how long they were in there prior to discovery. In the case of Hannaford Brothers, they didn't know they were compromised until the FBI knocked on their door and told them there were 1800 fraud cases all linked to them. How confident are you that a hacker hasn't setup shop on one or more of your systems?

#4 - VIRGINIA DEPARTMENT OF HEALTH BLACKMAIL

Modern hackers are bold and fearless. The FBI and Virginia State Police have been hunting down hackers who demanded that the state pay \$10 million dollars ransom for the return of millions of personal pharmaceutical records claimed to have been deleted and stolen from the Prescription Monitoring Program web site, the state's prescription drug database. The hacked database contained records of more than 35 million prescriptions dispensed since 2006. By the time of this paper's publishing, the state of Virginia has not paid the ransom and there is no evidence that the records have been sold by the hackers. The alleged "deleted data" was backed up and secured within days of the ransom demand. The state has mailed notifications to 530,000 people whose prescription records may have contained Social Security numbers.

#3 - GOOGLE

In 2009, Google had its fair share of data breaches as well. In all fairness, Google means so many things. Are we talking about Google Apps being breached? Are we talking about Google AdWords being breached? Are we talking about Google Docs being Breached? Are we talking about hackers causing outages? Are we talking about Gmail? Are we talking about SEO poisoning? To all of these, the answer is YES!

#2 - SOCIAL NETWORKING SITES

While so many data breaches are specific cases, others on our list can't be so specific. Why? Twitter was hacked so many times in 2009 we could have a top 10 Twitter breach article by itself. Whether it is individual accounts being compromised like Britney Spears, Twitter employees, or Twitter 3rd parties, Twitter has equal opportunity exploitability.



TOP 10 INFORMATION SECURITY BREACHES & BLUNDERS OF 2009

Facebook and MySpace aren't any better. There have been profiles hacked, applications hacked, account exposure, and the list goes on and on. There are even YouTube training video's on how to hack a MySpace account. Social networking sites have had a tough 2009 as far as data breaches and blunders are concerned, and it doesn't look like it's getting much better in the near term.

#1 - HEARTLAND PAYMENT SYSTEMS

2009 has been a year full of data breaches, compromises, exposures, loss, theft, wrongdoing, and all around cyber-criminality. Demanding first place is of course the new poster child of data security breaches, Heartland Payment Systems. An "A for effort" should be given to Heartland announcing the breach during the inauguration of President Obama in the hopes it would go under the radar...it didn't. While the official court proceedings report 130 million records (by far the largest data breach announced), I am not sure how they came to that number. Heartland told us a few things: 1) The compromised system processes over 100 million records a month. 2) The hackers had access to the system for about 18 months without detection. I am not great at math, but the recorded number doesn't sound right. Perhaps that is the number of unique records compromised. So when my sister goes shopping and swipes her card 20 times that day, it may only count as 1 of the 130 million rather than 20. Who knows...

Heartland processes credit cards for over a quarter of a million merchants nationwide. They have had 31 separate lawsuits filed against them as a result of the breach. Somewhere around 700 banks announced losses as a result of the Heartland breach. The good news is that we caught the bad guys! Albert "Segvec" Gonzalez has been indicted by a federal grand jury in New Jersey along with two unnamed Russian conspirators. It appears these same guys are responsible for more than Heartland, including Hannaford Brothers, 7-Eleven, and TJX.

CONCLUSION

When analyzing the top 10 breaches and blunders of 2009, the common thread between all of them is how they were all avoidable. Whether a security solution should have been implemented, an employee trained, a system locked down, a filter set, a monitor enabled, or an account disabled, it is amazing how little it would have taken for these highly publicized breaches and blunders to be avoided. Of course it is easy to say that with 20/20 hindsight, but basic security standards that are followed and a culture of security are not too much to ask. The thing is, most organizations know exactly where they lack security. They know where their gaps and exposures are. But knowing this, they still "play with fire" and hope that when they don't spend a few dollars this year, they will not get burned. Unfortunately in this day in age, getting burned does not mean 1st degree burns, it means incineration.

KEVIN PRINCE
CHIEF ARCHITECT
PERIMETER E-SECURITY