

Information Security Awareness (part1 of 3)

By
Rick J. Scarfino, CPA, CITP, CISA
&
Josh A Ayers, CPA, CITP, CISA

DECEMBER 2010

STONE  CARLIE

Going Beyond The Numbers®
101 South Hanley Road
Suite 800
St. Louis, MO 63105
(314) 889-1100
www.stonecarlie.com

Information Security Awareness: What You Need to Know About Information Security to Protect You and Your Business

Not a day goes by without hearing some reference to cybercrime in the news. Whether it's news about spam, email scams, the latest virus threat, or stories about hackers obtaining confidential data the threats seem overwhelming. These threats are ever present in our daily lives from our home to our work computer and everywhere in between on our cell phones and laptops. So, how do we protect ourselves and our businesses from a seemingly never ending list of threats?

In a three part series, we will give you the information you will need to protect yourself from cybercrime. With a little awareness and a common sense approach to information security we will help you significantly reduce the risk of becoming the next cybercrime story in the news. Part one of our series will focus on the emerging cyber security threats and the risks they present to you and your business. Part two will give you tips on countermeasures you can implement and communicate to your employees to guard against the emerging cyber security threats. Part three will give you our top ten list of things to do to secure your workforce.

Cyber Threats Affecting You and Your Business

Let's first start by giving a general definition of some key terms for you to use as reference throughout this series of articles:

Spam- the use of electronic messaging systems to send unsolicited bulk messages indiscriminately.

Malware – short for “malicious software” and is software designed to infiltrate or damage a computer system without the user's knowledge. Can be hidden in zip files or transmitted during instant message (IM) chat sessions.

Phishing – the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card detail by masquerading as a trustworthy entity in an electronic communication.

Virus – a computer program (malware) that can copy itself and infect a computer. Viruses can increase their chances of spreading to other computers by infecting files on a network file system that is accessed by another computer.

Worm – a self-replicating malware computer program. It uses a computer network to send copies of itself to other nodes (computers on the network) and it may do so without any user intervention.

Trojan Horse – malware that appears to perform a desirable function (like a game) for the user to run or install but instead facilitates unauthorized access of the user's computer system. Users are typically tricked into loading and executing it on their systems. A Trojan Horse may allow a hacker remote access to a target computer system. Once a Trojan horse has been installed on a target computer system, a hacker may have access to the computer remotely and perform various operations.

Keystroke logging – (often called key logging) is the action of tracking (or logging) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that their actions are being monitored.

Website spoofing – the act of creating a website, as a hoax, with the intention of misleading readers that the website has been created by a different person or organization. By using domain forwarding, or inserting control characters, the URL can appear to be genuine while concealing the address of the actual website.

Zombie – a computer that has been infected by a piece of malicious software such as a Trojan horse, virus or another type of malware. Once infected, the zombie's sole purpose is to perform a malicious task on behalf of the attacker. Zombies can be used to bring down corporate networks, websites and send mass amounts of spam to individual users.

Bot – an automated computer program or robot. In context of “botnets”, bots refer to computers that are able to be controlled by one, or many, outside sources. An attacker usually gains control by infecting the computers with a virus or other malicious code that gives the attacker access. A computer may be a part of a botnet even though it appears to be operating normally.

Botnet (Robot Network) – a large number of compromised computers that are used to create and send spam or viruses or flood a network with messages as a denial of service attack. Also known as a Zombie Army.

Now that we are more familiar with some of the common terms used in the world of cybercrime, let's take a look at how these threats are affecting the world we live in.

Symantec released a report this year titled the Symantec Internet Security Threat Report: Trends for 2009. Some interesting facts obtained from the results of Symantec's report are summarized below:

- 60% of identity exposures were compromised by hacking attack.
- 130 million credit card numbers were compromised by a single successful hacking attack of credit card payment processor Heartland Payment Systems (you probably did not hear about it – it was conveniently announced on the day of President Obama's inauguration).
- 75% of enterprises surveyed experienced some form of cyber attack in 2009, providing evidence cyber crime is not limited to only a few large enterprises.
- The top Web-based attacks observed in 2009 primarily targeted vulnerabilities in Internet Explorer (18%) and applications that process PDF files (49%). Due to Internet Explorer and Adobe's large market share, it is likely that attackers are targeting them to compromise the largest number of computers possible.
- Equally as interesting – of the Web browsers analyzed by Symantec in 2009, Mozilla® Firefox® had the most reported vulnerabilities, with 169, while Internet Explorer had just 45, yet Internet Explorer was still the most attacked browser. This shows that attacks on software are not necessarily based on the number of vulnerabilities in a piece of software, but on its market share and the availability of exploit code.
- It is no surprise the United States and China are the number one and two countries in the world when it comes to originating cybercrime. However, what is surprising is the increase in activity in developing countries (Brazil, India and Russia). Clearly, as connectivity increases in those parts of the world, hackers are taking advantage of new access and availability to a large number of people.

Symantec Internet Security Threat Report: Trends for 2009

Overall Rank		Country	Percentage		2009 Activity Rank				
2009	2008		2009	2008	Malicious Code	Spam Zombies	Phishing Hosts	Attack Bots	Attack Origin
1	1	United States	19%	23%	1	6	1	1	1
2	2	China	8%	9%	3	8	6	2	2
3	5	Brazil	6%	4%	5	1	12	3	6
4	3	Germany	5%	6%	21	7	2	5	3
5	11	India	4%	3%	2	3	21	20	18
6	4	United Kingdom	3%	5%	4	19	7	14	4
7	12	Russia	3%	2%	12	2	5	19	10
8	10	Poland	3%	3%	23	4	8	8	17
9	7	Italy	3%	3%	16	9	18	6	8
10	6	Spain	3%	4%	14	11	11	7	9

Do you ever wonder where compromised data may go or how available it truly is? Symantec issued a separate study entitled Report on the Underground Economy. The study included Symantec’s research of the underground economy from July 2007 to June 2008 where they found the following:

- Value of all advertised goods > \$276 million.
- Credit Card Data and Financial Account Information is the most popular items bought and sold.
- \$0.10- \$25 per compromised credit card.
- \$10-\$1,000 per compromised financial account information.
- \$1-\$15 for full compromised identities (name, DOB, SSN, etc.).
- Certain passwords, user security question answers, mother’s maiden name and credit card info could sell for \$200+.

If you look at the price per compromised record and compare to the total amount of advertised goods (\$276 million), you can get an idea of the volume of compromised records.

Cybercriminals continue to make available and/or use crimeware kits or toolkits that allow people to customize a piece of malicious code designed to steal data and other personal information. For example, a crimeware kit called the “Zeus” kit can be purchased for \$700, but can also be found for free on some forums. Crimeware kits make it easier for unskilled attackers to compromise computers and steal information and allow anyone who buys them to customize them to their own needs. In 2009, Symantec observed nearly 90,000 unique variants of the basic Zeus toolkit.

Risks of Data Loss and Cyber Crime

Hopefully the statistics above show you how pervasive cybercrime has become and the risk it poses to your business. All business owners should understand that there is no doubt that data loss as a result of cyber crime is not only financially dangerous, but also potentially criminal.

Financially Dangerous ...

The Federal Trade Commission estimates that more than 10 million Americans have their personal information stolen or abused each year, costing consumers \$5 billion and businesses \$48 billion.

The Ponemon Institute issued its *2009 Annual Study: Cost of a Data Breach* that further discusses the direct financial impact of breach notification and the cost to implement preventive solutions and the indirect financial impact of customer turnover and diminished reputation as a result of a data breach. These results were not based on hypothetical responses, but represented cost estimates for activities from actual data losses. 45 organizations participated in the study and the breaches studied ranged from 5,000 records to more than 101,000 records covering 15 different industry sectors. The Ponemon 2009 Annual Study found the following:

- The average cost of a data breach was approximately \$204 per record. The average total cost per breach in the organizations studied was \$6.75 million. The least expensive breach was approximately \$750,000, while the most expensive was estimated at \$32 million.
- Of the \$204 per record average cost, \$144 pertains to indirect costs, which included abnormal turnover or churn of existing and future customers.
- Of the \$204 per record average cost, \$60 pertains to direct costs, which included detection, escalation, notification, and post-response costs.
- 42% of all cases involved third-party mistakes, which is particularly important given the increase in reliance we have placed on third-parties in the normal course of business. Contrary to what most would assume, organizations incurred a significant cost even in situations where a third-party vendor was at fault. This statistic highlights the importance of due diligence when selecting a third-party vendor. If any third-party vendor is handling your corporate data, it should be a requirement for that vendor to have a SAS 70 or similar independent assurance on their internal controls in order to have your business. Additionally, when data breaches didn't involve a third-party the average cost per stolen record decreased from \$204 to \$194 (a 10% difference).
- 24% of all cases involved malicious or criminal attacks and 36% of all cases involved lost/stolen laptop or mobile device.
- Non-malicious/non-criminal attacks had an average cost per record breached of \$154 and the average cost per record was \$166 when system glitches were the root of the incident.

Potentially Criminal...

There are many Federal laws governing data security and data disposal which include, but are not limited to, the Gramm-Leach-Bliley Act (GLBA), Health Insurance Portability and Accountability Act (HIPAA), and the Fair Credit Reporting Act (FCRA).

One of the more recent set of rules pertains to the Fair and Accurate Transactions Act (FACTA) Red Flag Rule (the Rule). The Rule is currently delayed through 12/31/10. Congress has directed the Federal Trade Commission and other agencies to develop regulations requiring “creditors” and “financial institutions” to address the risk of identity theft. All such entities that have “covered accounts” are required to develop and implement written identity theft prevention programs to help identify, detect, and respond to patterns, practices, or specific activities – known as “red flags” – that could indicate identity theft.

There are also state laws governing data security and data disposal. All states except Alabama, Kentucky, New Mexico and South Dakota have enacted some sort of legislation governing data security and/or data disposal, which are primarily driven by data breach notification laws. These breach notification requirements expose businesses to potentially significant losses arising from negative publicity, loss of reputation, regulatory fines and class action lawsuits.

Are you aware of the Missouri and Illinois breach notification requirements? They are summarized below:

Missouri Breach Notification Law

Application: Everybody that maintains Missouri (MO) resident personal information (PI)

Breach Definition: Unauthorized access to and unauthorized acquisition of PI

PI Definition: First name or first initial and last name in combination with one or more of the following: SSN, driver’s license or other unique ID, financial info in combination with other required info, other unique electronic ID with other required info, or medical or health insurance information

Notification: Specific notice requirements with minimum information and distribution

Penalties/Enforcement: Actual damages AND civil penalty not to exceed \$150,000 per breach

Note: If PI is encrypted, redacted (blacked out) or otherwise altered by any method or technology in such a manner that the name or data elements are unreadable or unusable, you may not be required to meet the notification requirements or be liable for the penalties and enforcement under the law.

Illinois Breach Notification Law

Application: Everybody that maintains Illinois resident PI

Breach Definition: Same as Missouri

PI Definition: First name or first initial and last name in combination with one or more of the following: SSN, driver's license or other unique ID, or financial info in combination with other required info

Notification: Specific notice requirements with minimum information and distribution

Penalties/Enforcement (under IL Consumer Fraud Act): A violation and actual damage allow a court, in its discretion, to award actual economic damages, injunctive relief, punitive damages, reasonable attorney fees, court costs, and "any other relief which it deems proper"

Note: If PI is encrypted, redacted or otherwise altered by any method or technology in such a manner that the name or data elements are unreadable or unusable, you may not be required to meet the notification requirements or be liable for the penalties and enforcement under the law.

Final Thoughts

As we have outlined above, the risks are many and the costs are significant if you do not take a proactive approach to information security. The Internet has provided criminals the two things they require most - anonymity and mobility - and that makes it extremely difficult to combat these criminals. Cybercriminals continue to take advantage of two very concerning trends in the current environment:

1. The cost of cybercrime tools is decreasing while the availability of these tools are increasing; and
2. The technical knowledge of cyber criminals is decreasing while the sophistication of their attacks is increasing.

The culmination of these factors makes it difficult to understand what risks to defend against and what solutions to implement. However, in parts two and three of this series, we will increase your security awareness and provide a common sense approach to significantly reducing the risks you and your business face in today's computer environment.

Rick Scarfino, CPA, CITP, CISA is a Senior Manager with Stone Carlie & Company, LLC. Rick can be reach at rscarfino@stonecarlie.com. Josh Ayers, CPA, CITP, CISA is a Manger with Stone Carlie & Company, LLC. Josh can be reached at jayers@stonecarlie.com. Stone Carlie & Company, LLC (www.stonecarlie.com) is a full service accounting firm that specializes in SAS70 engagements for TPAs and other entities within the insurance industry.



Joshua A Ayers, CPA, CITP, CISA

Manager Assurance Services



Responsibilities

Josh is a manager at Stone Carlie and helps oversee all activities and services performed at or on behalf of a client organization in the Firm's Assurance Services Department.

- Manage audit, internal audit, SAS 70, SysTrust and WebTrust services
- Plan, perform & review fieldwork, and provide technical support for audit, internal audit, SAS 70, SysTrust and WebTrust services
- Monitor services on an ongoing basis
- Provide technical support to clients on an ongoing basis
- Meet with client executives on a periodic basis

Qualifications

- Certified Public Accountant – Missouri
- Certified Information Technology Professional
- Certified Information Systems Auditor
- Member of Stone Carlie System Security and Process Assurance Group
- Possesses four years of professional experience in the assurance services field with commercial and not-for-profit entities, including audits, reviews, compilations, agreed-upon procedures, due diligence, and consulting engagements for industries such as manufacturing, construction, retailers, distribution, logistics, life sciences, financial institutions, application service providers, data storage companies, website hosting, development companies, web browsers, document imaging companies, health care, and large governmental agencies.
- Possesses almost two years of professional experience in financial reporting and compliance with a leading global life reinsurance company, which included identifying, researching, and documenting technical issues that ensured compliance with appropriate United States Generally Accepted Accounting Principles (US GAAP) and Securities and Exchange Commission (SEC) regulations. In addition to providing general US GAAP and SEC compliance support, served as primary accounting liaison to an investment department that managed over \$16 billion in invested assets that included traditional fixed maturity securities, mortgage loans, derivatives and other emerging investment vehicles. Accomplishments included the research, development and implementation of the Company's first hedge accounting policies as it related to a \$300 million net investment in a foreign operation and a fair value hedging strategy to convert \$50 million in fixed rate investments to floating rate investments.

Education and Selected Memberships

- Saint Louis University – St. Louis, MO B.S. – Business Administration with an emphasis in Accounting
- Member, American Institute of Certified Public Accountants (AICPA)
- Member, Missouri Society of Certified Public Accountants (MSCPA)
- Member, Information Systems Audit and Control Association (ISACA)
- Extensive continuing professional education

Richard J. Scarfino, CPA, CITP, CISA

*Senior Manager
Assurance Services*



Responsibilities

Richard will serve as the Audit Engagement In-Charge, coordinating audit services and staff support during fieldwork. He will plan, supervise and perform fieldwork as well as provide technical support on industry specific, accounting and tax related issues.

- Manage audit, internal audit, SAS 70, SysTrust and WebTrust services
- Plan, perform & review fieldwork, and provide technical support for audit, internal audit, SAS 70, SysTrust and WebTrust services
- Monitor services on an ongoing basis
- Provide technical support to clients on an ongoing basis
- Meet with client executives on a periodic basis

Qualifications

- Certified Public Accountant – Missouri
- Certified Information Technology Professional
- Certified Information Systems Auditor
- Member of the Stone Carlie System Security and Process Assurance Group
- Member of the Stone Carlie Manufacturing and Distribution Group
- Member of the Stone Carlie Not-for-Profit Services Group
- Possess nine years of audit and internal audit experience in a variety of industries including professional service, retail, distribution, manufacturing and not-for-profit
- Possess five years of experience providing SAS 70, SysTrust and WebTrust services

Education and Selected Memberships

- Saint Louis University, Business Administration – Accounting, Finance and Management Information Systems
- Member, American Institute of Certified Public Accountants
- Member, Missouri Society of Certified Public Accountants
- Member, Information Systems Audit and Control Association
- Extensive continuing professional education