

Top 10 Security Risks for 2008

It is becoming apparent that 2008 is going to be a challenging year for business. Although the market conditions may prompt you to look for ways to cut corners and decrease costs, that doesn't mean you need to compromise on information security.

Below is a list of the Top 10 risks that could compromise your bank operations, data and ultimately your customers' trust. To keep the list short, I have omitted many of the well-known threats (e.g., un-patched servers, application vulnerabilities and phishing). Please note that this omission does not diminish their importance.

1. Identity black market – There is a thriving and sophisticated market for buying and selling confidential information, including account information and identities. The price of a stolen identity is currently estimated to be \$14-\$18. Not very compelling for a single identity, but a significant motive for stealing a database of 10,000, 100,000 or 1 million records.

2. Cyber-extortion – What would you do if you received a call threatening to bring down your computer system unless you paid a \$10,000 ransom? It may sound far-fetched, but it is very real. Recently, a CIA official confirmed that there have been “cyber intrusions into utilities, followed by extortion demands.” In at least one case, the disruption caused a power outage affecting multiple cities.

3. Transportable data (USB, laptops, backup tapes) – It seems like every day there is a report of data loss because of a stolen laptop or “lost or misplaced” data backup tapes. Plus, USB devices that fit on a keychain and hold 64 gigabytes of data are now available, making it very easy to covertly transport massive amounts of data.

4. “Zombie” networks – Commonly referred to as “botnets,” these are networks of computers that have been compromised by a virus or worm and are now under the control of a centralized command, without the knowledge of the computer owner. The botnet originator can control the group remotely to forward transmissions for nefarious purposes, including denial of service attacks, spam or viruses. This is particularly nasty because it is almost impossible to detect with anti-virus software, since the program lies dormant until awakened.

5. Exploits in new technology – Technologies such as VoIP, server virtualization and even the iPhone have significant advantages, but also introduce new risks. Professional hackers and malware authors are now finding ways to exploit vulnerabilities that are inherent to new technology. One example of this is the exploit of IP telephone systems to perform a “vishing” campaign. Similar to phishing, a vishing campaign makes calls out from a compromised phone system that appears to be a trusted source, to entice individuals to enter confidential information such as PINs and account numbers.

6. Outsourcing – Most companies—large and small—have embraced outsourcing services as a cost-saving strategy. Outsourcing not only reduces overhead, it also can improve quality to provide a competitive advantage. However, because of this trend, an unprecedented amount of sensitive data, including customer and employee personal information, is being shared with outside vendors. It is imperative that you require vendors that have access to sensitive customer information to have adequate safeguards to protect your information.

Remember, you can delegate authority, but not ultimate responsibility for the security and protection of sensitive information.

7. Business interruption – Natural disasters are rare, but we saw plenty of weather anomalies in 2007. From the tornado in Brooklyn, NY to the flooding in southeastern Minnesota, businesses nationwide were reminded of the importance of preparation. These are the high-visibility events. More common are the routine problems, such as power outage and equipment failure. Unfortunately, many businesses are still woefully unprepared to respond and recover from business interruption in an acceptable time. And that lack of preparedness could result in devastating consequences.

8. “Minnesota nice” – We all want to be pleasant and helpful to our customers and guests. We may feel uncomfortable asking someone for credentials, verifying the identity of a caller or stopping someone from freely walking around the office. But it needs to be done to safeguard your assets and information. You can have all the latest technology to secure your Internet perimeter, but if your employees are not trained on how to follow and enforce your security policies, you may not be prepared to stop the “hacker” from walking in the front door to get access to your data.

9. Low barrier to entry for criminals – To be a hacker today, you don’t need to know how to write technical code. You can buy it. According to Symantec, 42 percent of phishing websites observed in 2007 were associated with just three phishing toolkits. The combination of motive (see #1) with the ease of entry for criminals, presents a scary outlook.

10. Focus on the wrong things – In school, you may have studied for your math test by memorizing the formulas that you knew would be on the test. Studying for the test instead of mastering the subject may have resulted in a passing grade, but the value of the lesson probably was not retained. The same is true for information security. If your primary focus is on passing your compliance exam, you may overlook major vulnerabilities.

Consider the well-chronicled TJX data security breach, for example: Thieves stole 45 million customer credit and debit card numbers, which cost TJX \$256 million. TJX’s federal court hearing revealed that Visa provided the retailer a compliance “pass” to 2009 in spite of known security issues found in a 2005 audit.

Good security programs lead to compliance...good compliance does not necessarily lead to security.

While this list may appear daunting, there are counter-measures businesses can and should take. Key steps in successful and sustainable information security programs include:

- Document security policies and expectations
- Assess safeguards (technical, physical and administrative controls)
- Implement tools and procedures to monitor and enforce compliance with policies
- Build information security into the culture through employee training and awareness
- Ensure senior management governance, support and oversight
- Repeat

By: Jeff Olejnik, President
Assurity River Group, Inc.
4500 Park Glen Road, Ste. 120
Minneapolis, MN 55416
952-230-6488
jolejnik@assurityriver.com
www.assurityriver.com