



Best Practices

September/October 2008

Top Ten Security Concepts Managers Need to Know

Whether they know it or not, business managers are responsible for information systems, functions, and data within their span of responsibility. In order to effectively manage these assets, business managers need to be familiar with several concepts. Familiarity with these concepts will help business managers better understand the implications of their decisions regarding their employers' assets.

Defense in depth

This concept specifies that two or more controls, ideally of different types, work in combination to protect assets. Each control provides some type of protection by itself, and together they offer greater protection. Examples of defense in depth include:

- **Castle.** The ancients understood defense in depth and got it right. A loot of treasure or a beautiful princess are hidden in the innermost chambers of a castle that is protected by a moat, a moat monster (or possibly just a deterrent control in the form of a "Beware of moat monster" sign), a drawbridge, turrets for archers, high walls that are difficult to climb, inner courtyards with more gates, turrets, hostile terrain and so forth.
- **E-commerce data.** An online merchant protects its valuable transaction data with firewalls, routers with ACLs, intrusion detection systems, system-level access controls, database-level access controls, acceptable use policies, audit logging, and encryption. Notice that some of these controls are preventive, while others are detective, deterrent, and administrative.

Least privilege

This concept states that personnel are to have *only* the permissions and authority that they *require* in order to perform their stated functions, and no more.

Least privilege applies equally to systems: programs, processes, and other objects should have access to only the data and other systems required. For example, applications should never be run as *root* or *Administrator*.

Fail open / Fail closed

Sometimes these mechanisms can fail, and when they do, they fail in one of two ways, which are:

- **Fail open.** When a control fails open, this means that all events (authorized as well as unauthorized) are permitted. An example of a fail-open situation is the failure of a key-card or biometric-controlled door buzzer, resulting in a door that opens just by pushing on it. A fail open situation puts protected assets at risk because they can be accessed by any party.

- **Fail closed.** In a fail closed situation, all events are blocked, including those that should be allowed. An example of a fail-closed situation is a failure of a key-card or biometric reader that prevents everyone from going through a protected doorway. A fail-closed situation disrupts business operations by preventing subjects from being able to access business assets or information needed to complete tasks.

Role based access control

In complex systems with many users, it can be tedious and time consuming to administer the access levels and privileges that individual users need. Many complex applications support the use of *roles* - abstract definitions or templates of predefined roles for common job descriptions. It works like this: an organization defines permissions for each role, and then assigns personnel to a role based upon their job title.

When changing business conditions require that people in a certain role have different privileges, only the *role* is changed, which results in the permissions for everyone assigned to the role being changed likewise. This is a far more scalable solution than administering permissions for each user.

Spoofing

Spoofing, in its most basic form, is the act of pretending to be something you're not. There are many forms of spoofing, including:

- **Phishing.** Those e-mails that pretend to originate from a financial institution or other organization that advises the recipient to "log in" to reset their credentials.
- **Spam.** Often the vector for spreading malware (viruses, worms, and Trojan horses), spam messages often claim to be something they're not.
- **Caller-ID spoofing.** Several caller-id spoofing services provide a service that allows a caller to change their originating caller-ID number to any legitimate number.

CIA

At the most basic level, biometric systems need to be protected in three ways: confidentiality, integrity, and availability. Security professionals use the term CIA to denote these terms. Let's look at these concepts more closely:

- **Confidentiality.** Information must be protected from viewing by unauthorized parties and systems. While in many cases the biometric system is serving as part of the means to protect information in the organization, the biometric-related information itself must be protected from onlookers.
- **Integrity.** The integrity of biometric-related devices, systems, and information must be maintained. All of the components in a biometric system must be protected from unauthorized tampering. This includes the biometric devices themselves, as well as the systems and software that make it all work. Any unauthorized modifications to a biometric system may render it ineffective.
- **Availability.** The biometric system must be available for use at all times. If some condition or event makes the biometric system unavailable, then the assets that the biometric system protects may themselves be unavailable when they are needed. This could result in disruptions to business operations.

Social engineering

Clever and resourceful intruders know that the easiest way to reach a target is by the path of least resistance. If an intruder is unable to successfully penetrate the technical defenses of a system or

facility, he may instead rely on some unwitting employee to help the intruder gain access. Some examples of social engineering include:

- **Tailgating.** If an intruder is unable to enter a facility on his own, he can pretend to be an employee who has lost his key card (or index finger or eye) and follow an employee through a secured door. It's especially effective if the intruder is carrying some heavy object like a computer monitor or box of books – an employee is more apt to help the intruder into the building.
- **Remote access.** A clever intruder can make a series of phone calls to various people inside of an organization to get all of the pieces necessary to successfully log on to the corporate network. He can get the VPN URL from one employee, a user name from another, and get a password reset from the helpdesk if they do not sufficiently validate the identity of the “user”.
- **Loading Dock Entry.** Many reasonably secure facilities will have a blind-spot when it comes to the loading dock. A good social engineer in a brown shirt and pants can often just walk in the back door with nothing but a clipboard.
- **Road Apple.** The attacker leaves removable media lying around somewhere that it will get picked up, say near the door to the lobby. A curious employee picks up the media, takes it inside and plugs it in, whereupon it autoexecutes a Trojan or virus, granting the attacker access. This is especially effective if the media is of some value like a USB stick or an SD card.
- **Dumpster diving.** Intruders can go through an organization's trash in the hopes of finding discarded printouts, memos, and documents that contain enough information to con their way into a system or facility.

Change management

The number one cause of business interruptions, outages, and downtime is not technology, but people - people who make changes without fully understanding the implications of the change. Change management is the formal process of vetting every proposed change in a system prior to making the change. The steps in a change management process typically are:

1. **Proposed change.** Someone requests a change be made to a system. This change could be something as simple as a configuration change or as complicated as a software or operating system upgrade. The requested change should include: a) Description of the change; b) Business or operational justification for the change; c) Who will perform the change; d) When the change will be made; e) Impact of not doing the change; f) Risks associated with making the change; g) Backout plan in case the change is unsuccessful; h) Anticipated user impact (e.g. downtime while the change is made); i) Other systems affected by the change; j) Test results (hopefully the change was tested on a test environment).
2. **Change review.** The proposed change is circulated for review among all of the formal participants in the change management process.
3. **Change approval.** Participants in the process discuss the proposed changes in order to identify any other risks or impacts. Then they can decide whether the change can take place as-planned.
4. **Change wrap-up.** After the change is made, final recordkeeping can be filed, to record the successful implementation of the change.

Access management

Organizations with information systems and information assets accomplish tasks and meet business objectives through people. People access these information systems and assets to directly or indirectly manage or perform these tasks. People require access to the right functions and systems in order to accomplish this.

One of the leading causes of security breaches is the “inside job” - where someone with access to a system causes deliberate harm. Often this is done by persons who have left the organization but whose access rights are still active.

Access management is a formal discipline and process where all access requests to systems are managed. The process of requesting and granting access should follow these steps:

1. **Formal request.** An employee’s manager should make a formal access request that states explicitly what systems, functions, or information the employee should be able to access and perform.
2. **Review.** The system or information owner should review the request.
3. **Approval.** The system or information owner should approve the request if it is determined that the employee does require this access in order to perform his or her duties.
4. **Fulfillment.** The access administrator (who is a different person than the requestor, the manager, the approver, or the user) fulfills the access request.
5. **Recordkeeping.** The request, review, approval, and fulfillment are all recorded in an official log.
6. **Audit.** Periodically (every month to every six months), the access rights of all information systems must be reviewed to make sure that all persons who have access are still authorized to do so.
7. **Termination.** Whenever an employee leaves the organization, all access rights must be terminated within 24 hours - or sooner for highly sensitive applications and data.

Article from *Securitas Operandi™*; <http://peterhgregory.wordpress.com/>. Some material excerpted from *Biometrics For Dummies* by Peter Gregory and Mike Simon.



Trends

September/October 2008

Top IT Security threats of 2008

The SysAdmin, Audit, Networking and Security (SANS) Institute has released its list of the top 10 cyber security threats for 2008. The list includes:

- new developments of evergreen security risks,
- new exploitations of browser vulnerabilities,
- worms with advanced peer-to-peer technologies,
- insider attacks by rogue employees, consultants or contractors, and
- mobile phone technologies and voice over internet protocols (VoIP).

As a manager, you should be asking what are the greatest security threats facing your company's business network? And, what can be done to keep it secure?

Social Threats

Does your company use a standard instant messaging or IM client to keep in touch desk-to-desk such as AOL Instant Messenger, Yahoo or Internet Relay Chat? Do employees access social networking sites at work like MySpace.com or Facebook? Do you use Google Talk, Skype or other voice-over-Internet technologies to connect with customers? What was once considered to be relatively secure technologies on personal computers, can pose significant security risks to a secure business network.

In 2007, more than 1,000 malware attacks were reported coming from IM and chat clients alone, according to FaceTime Communications Inc., an IM security and compliance firm. Social networking sites were besieged by social engineering which tricked visitors into clicking links that activated malicious code spreading viruses such as the Skype worm and advancing phishing and identity theft. The introduction of Apple's new iPhone has been labeled as a "security nightmare" for the potential to expose business data to outsiders.

Espionage

In January 2008, the US Central Intelligence Agency admitted that cyber attacks had caused multicity blackouts and the loss of critical national data. Such attacks were traced back to IP addresses in China, where the People's Liberation Army has created an "elite Chinese unit" trained for "information warfare" and capable of carrying out "sophisticated attacks on high-risk targets." Not surprisingly, the threat of cyber espionage ranks as number three on the SANS Institute's list.

How Secure Do You Feel Now?

View the complete SANS Institute list of security threats that follows and share it with your IT department to gain an understanding of your company's risk exposure.

1. Sophisticated Web Site Attacks That Exploit Browser Vulnerabilities - Especially On Trusted Web Sites

Website attacks on browsers are increasingly targeting components, such as Flash and QuickTime, that are not automatically patched when the browser is patched. Website attacks have migrated from simple, based on one or two exploits posted on a website, to sophisticated, based on scripts that cycle through multiple exploits or packaged modules that effectively disguise their payloads. One of the latest such modules – mpack – claims a 10-25% success rate in exploiting browsers that visit infected sites.

2. Increasing Sophistication and Effectiveness In Botnets

The Storm worm started spreading in January 2007, with an email saying, "230 dead as storm batters Europe". Within a week, it accounted for one out of every twelve infections on the Internet, installing rootkits and making each infected system a member of a new type of botnet. Previous botnets used centralized command and control; the Storm worm used peer-to-peer control, so there was no central controller to take down. Additional variants have used messages with different subjects and improved the capabilities of rootkits. In 2008, additional variants and increased sophistication will keep this worm and others near the top of the list of security threats.

3. Cyber Espionage Efforts by Well Resourced Organizations Looking to Extract Large Amounts of Data - Particularly Using Targeted Phishing

One of the biggest security stories of 2007 was disclosure in Congressional hearings and by senior US Department of Defense officials of massive penetration of federal agencies and defense contractors and theft of terabytes of data by the Chinese and other nation states. Despite intense scrutiny, these nation-state attacks will expand; more targets and increased sophistication will mean many successes for attackers. Economic espionage will be increasingly common as nation-states use cyber theft of data to gain economic advantage in multi-national deals. The attack of choice involves targeted spear phishing with attachments. It uses social engineering to make victims believe an attachment comes from a trusted source, and then takes advantage of Microsoft Office vulnerabilities and hiding techniques to circumvent virus checking.

4. Mobile Phone Threats, Especially Against iPhones and Androids Plus VoIP

Mobile phones are general purpose computers, so worms, viruses, and other malware increasingly target them. Google's announcement of "android" and the formation of the "open handset alliance" is a watershed moment for the mobile phone industry. A truly open mobile platform will usher in unforeseen security nightmares. Developer toolkits provide easy access for hackers who are taking note. Attacks on VoIP systems are on the horizon as VoIP phones and IP PBXs have numerous published vulnerabilities. Attack tools exploiting these vulnerabilities are currently available on the Internet.

5. Insider Attacks

Insider attacks are initiated by an organization's rogue employees, consultants and/or contractors. Insider risk has long been exacerbated by the fact that insiders usually have some degree of access to systems, databases, and networks. Recently, however, there are cases where security has broken down, allowing insiders to attack from both inside and outside an organization's network boundaries. One defense against this type of risk is limiting employee access to IT systems based on job requirements.

6. Advanced Identity Theft from Persistent Bots

A new generation of identity theft is being powered by bots that stay on computers for three to five months collecting passwords, bank account information, surfing history, frequently used email addresses, and more. They gather enough data to pass basic security checks, enabling extortion and identify theft.

7. Increasingly Malicious Spyware

Attackers continue to refine the capabilities of malicious code, expanding on flux techniques to obscure their infrastructure and making it harder to locate their servers. Additionally, the ability of attackers to detect investigator activity and respond with an attack will become more mainstream and powerful. Tools will increasingly target and dodge anti-virus, anti-spyware, and anti-rootkit software to preserve the attacker's control of a computer for as long as possible. In short, malware will become stickier on target machines and more difficult to shut down.

8. Web Application Security Exploits

Large percentages of web sites have cross site scripting, SQL injection, and other vulnerabilities resulting from programming errors which can be exploited by criminals looking for financial gain. Web 2.0 applications are vulnerable because user-supplied data cannot be trusted; the script running in the users' browser still constitutes "user supplied data." In 2008, web 2.0 vulnerabilities will be added to more traditional programming flaws and web application attacks will grow substantially.

9. Increasingly Sophisticated Social Engineering Including Blending Phishing with VoIP and Event Phishing

Blended approaches will amplify the impact of more common attacks. For example, the success of phishing is being radically increased by stealing IDs of users of other technologies. Salesforce.com users were targeted for an "FTC complaint" phishing email. Monster.com users were targeted for a job offer phishing email. Even if it is non-targeted, event phishing is gaining in sophistication. Tax filing and US presidential election scams will be widely used in 2008, and many of them will succeed. An email with the subject "Obama drops out of presidential race" could generate huge new botnets of people who are interested in politics, but may not have patched their systems fully. Add to those opportunities potential bogus fund raising sites and political dirty tricks going digital, and you'll have an explosive junction of hacking and politics.

A second area of blended phishing combines email and VoIP. An inbound email being sent by a credit card company asks recipients to "re-authorize" their credit cards by calling a 1-800 number. The number leads them (via VoIP) to an automated system in a foreign country that convincingly asks the caller to key in their credit card number and expiration date.

10. Supply Chain Attacks Infecting Consumer Devices (USB Thumb Drives, GPS Systems, Photo Frames, etc.) Distributed by Trusted Organizations

Retail outlets are increasingly becoming unwitting distributors of malware. Devices with USB connections and CDs packaged with those devices sometimes contain malware that infect computers and connect them to botnets. This has been seen among conference attendees who are given USB thumb drives and CDs that supposedly contain conference papers, but also contain malicious software.

Excerpts by Jim Higdon, January 23, 2008, [IT Security](#) and [The SANS Institute website](#).



Productivity

September/October 2008

To Block or Not to Block? Social Networking Sites in the Workplace

There's no doubt that social networking sites are a relevant part of the everyday lives of people at home as well as in the workplace. People are realizing these sites have impact not only in terms of personal growth and relationships, but also as tools for staying connected in business.

The recording industry recently demonstrated the growing importance of social network sites when BusinessWeek reported that Warner, Sony BMG and Universal launched an endeavor with MySpace in which the social networking giant will allow users to listen to and watch music content and purchase related merchandise and tickets on its site. Certainly, there are business reasons to employ these sites.

But like all worthwhile technology tools, this one, too, comes with pitfalls. The increasing use of social networking sites in the workplace can have serious security and productivity implications for companies, which is why more and more companies are choosing to block or limit the use of these sites.

Scammers are coming up with new ways to steal information and corrupt computers through sites such as LinkedIn, Plaxo, MySpace and Facebook. One such method is the Nigerian 419 advance fee fraud scams, which experts say has popped up recently on these sites.

According to Paul Wood, senior security analyst at MessageLabs, "We've seen one example of Nigerian 419 recently where the fraudster had created a fairly convincing-looking page on LinkedIn to give credibility to their background in the business they were trying to promote." In these cases, scammers may use e-mail correspondence to prompt unsuspecting users to visit their profiles and learn about their fake personas. The aim is to provide a false sense of trust so users will be convinced to do business with them — and ultimately give them money.

In some cases, a scammer will claim to be someone you know, "pretending to be that person in order to gain access to your profile, your friends list, or other information you might be willing to give them," explained Wood.

Another trick is the use of fake embedded videos on otherwise legitimate-looking websites. "You might see [what looks like] a link to a YouTube video with the YouTube logo, but in fact it's just a spoof. When you attempt to view the video, you are asked to download a codec that supports the video's format. In most cases, what you downloading is malware.

In order to protect yourself, Wood suggests verifying the identity of people who claim to be someone you know and also being skeptical of videos and links that may appear to be legitimate.

“If somebody says, ‘I’m so-and-so that you used to work with several years ago,’ do you have another means of contacting that person?” Wood said. “Don’t take it at face value; [on the computer, people] tend to be more trusting than if [they] were face to face meeting somebody for the first time. [On the Internet], there are so many other factors that you miss out on, like body language.”

These sites also can cause a lag in productivity. “If someone’s spending too much time online or addicted to playing Scrabble with somebody on Facebook, then they might not be doing their jobs,” said Wood. This is another reason why companies need to adopt policies regarding acceptable Internet use on the job.

Some companies choose to completely block social networking and blogging sites, and others allow some use of these sites at specific hours, such as lunchtime. Excessive blabbing on social sites can generate unwanted gossip about a company and its plans, while unscrupulous competitors can social-engineer employees into revealing intellectual property. An employee’s mere presence on a social network also sends a signal: job titles, experience, friends and family, and contact information can all be combined to where competitors can draw reasonably accurate organizational charts of a company, its suppliers, partners and clients.

What’s important, said Wood, is accounting for the “three prongs” of web policies. “You have to look at the policies appropriate to your business: the user training and awareness side of it as well as the educational aspects internally, to make sure employees understand the potential risks — the social engineering threats — that they may come into contact with. “The third part is having the tools and technology in place to protect employees so they don’t visit a site that may harbor malicious content,” he concluded.

Minimizing Social Network Risk

Realizing that perceived security gaps could lead individuals and companies to shun their sites, big names like Facebook and LinkedIn allow users to adjust how much information — posts, photos, online status and other factors — others may access.

Facebook’s [privacy site](#) describes several such controls. Users can reduce what appears in their profile and what information about their online activities is public, such as their use of specific Facebook applications. Users can also block specific users from seeing more than a limited profile or from finding a user via search.

Facebook also limits the ability of search-site Web crawlers to harvest user information, saying in its privacy policy, “Facebook limits access to site information by third party search engine ‘crawlers’ (e.g. Google, Yahoo, MSN, Ask). Facebook takes action to block access by these engines to personal information beyond a user’s name, profile picture, and limited aggregated data about the users profile (e.g. number of wall postings).” LinkedIn is the most business oriented social network, and its users seem generally aware of the need to behave professionally. The site provides a wide range of tools for customizing views, such as the ability to change whether people you’re connected to can see just those you both have connections with, or your entire connections list.

These types of features increase social networks’ corporate usability. However, at the end of the day, specific company policies that limit what employees may share online might create the biggest payoffs, like resistance to social engineering, preservation of the company’s and employees’ reputations, and preservation of trade secrets and internal company structure.

Excerpts from two articles: Certification Magazine, May 12, 2008, by Meagan Polakowski. www.certmag.com/articles and IT Security Magazine, Social Network Security Hazards, July 25, 2007 by Paul D. Kretkowski; www.itsecurity.com



Professional Development

September/October 2008

The Essential Guide to Email Security

What you need to know about protecting incoming and outgoing email.

Over the past couple of decades, email has become one of the world's leading communication mediums, perhaps even outpacing the telephone and traditional mail service.

Unfortunately, over this same time span, email has proven itself to be highly vulnerable to outside influences, including individuals and organizations that seek to cause some form of technological damage or hope to make money in an illegal fashion. As a result, security has become an increasingly important issue for email users.

Email Threats

Although email security is often viewed as a single issue, it is actually a conglomeration of several different threats that work to damage computers and defraud recipients, as well as to undermine the effectiveness, reliability and trust of email systems. Email threats can be divided into several distinct categories:

Viruses, Worms and Trojan Horses: Delivered as email attachments, destructive code can devastate a host system's data, turn computers into remote control slaves known as [botnets](#) and cause recipients to lose serious money. [Trojan horse](#) key loggers, for example, can surreptitiously record system activities, giving unauthorized external parties access to corporate bank accounts, internal business websites and other private resources.

Phishing: According to the Anti-Phishing Working Group — a trade organization that consists of financial organizations, software publishers and other concerned parties — [phishing](#) attacks utilize social engineering to steal consumers' personal and financial data. The attacks rely on "spoofed" emails that direct recipients to bogus websites that are designed to trick them into revealing confidential financial data such as credit-card numbers, usernames, passwords and social security numbers. Phishing perpetrators typically operate by hiding under phony identities that they have stolen from banks, online merchants and credit-card companies.

Spam: Although not an overt threat like a virus-infected attachment, junk email can quickly overwhelm an inbox, making it difficult to view legitimate messages. The [spam](#) problem has gotten so bad that it is commonplace for users to abandon email accounts that are overrun with spam rather than try to fight the problem. Spam is also the delivery medium of choice for both phishers and virus attackers. So just how bad is the problem in terms of numbers? Tens of billions of spam messages are sent every day.

Email Safeguards

Protecting email users and their systems from attackers is a 24/7 job that requires the use of multiple security tools. Some of these include:

Client Security: Virtually all major email clients offer security settings, anti-spam tools, phishing filters and other features that are designed to snare and isolate dangerous messages before they can inflict harm. Email users should investigate these features and use them as their first line of defense.

Firewall: A [firewall](#) can bolster email security by filtering out malware-laden attachments and other types of unwanted material that don't meet pre-configured rules.

Encryption: Rendering messages indecipherable to unauthorized recipients is a popular way of protecting outbound emails. [Encryption](#) software isn't perfect, however, since even the best products consume both processor speed and storage space. Users can also lose or forget passwords. Encryption can be handled by firewalls or additional software.

Anti-Virus Tools: Leading [anti-virus products](#) and services generally do a good job of spotting and removing viruses, worms and Trojan horses from incoming email messages.

Spam Filters: A good spam filter can differentiate between legitimate email and spam, freeing a user's inbox from mounds of digital debris. A drawback to this technology is that a poor spam filter, or one that has not been properly tuned, will remove a certain number of legitimate emails from a user's view while letting some spam pass through untouched. Improved spam-recognition technologies are making spam filters more accurate. Most vendors now promise 99 percent-plus accuracy rates — but even the best spam filter will incorrectly categorize some emails.

Education: One primary email-defense tool is education. Users who are aware of email threats are less likely to open potentially virus-infected attachments, click phishing links or perform other risky actions.

Email threats will continue to exist for as long as there are people and organizations that thrive on the misery they inflict upon others. Therefore, the practices and tools that constitute email security are likely to exist for as long as email itself.

Article from IT Security by John Edwards; September 19, 2008, <http://www.itsecurity.com/>