

**Information Technology Article Release
Web & IT Security**

8/22/2002

Contact: Mike Ament
Ament Resource Group, LLC
Voice: 206-261-7477 - Fax: 206-938-9900
<http://www.amentrg.com>

IT Bandits Don't Always Wear Masks.

How to protect your company's information systems from a costly security breach.

By: Mark McBurney - Information Strategist, Ament Resource Group, LLC

In today's complex, competitive and information driven environment it is often difficult to tell who the bandits are. Your IT System is exposed daily to potential attacks from multiple sources both internally and externally. Your job as a key decision maker is to assess your company's risk tolerance while taking prompt, strategic and cost effective actions to safeguard these precious assets.

The source of these raids takes a variety of forms including; corporate espionage, internet portal or viral attacks, natural disasters, antiquated IT Systems, hardware failures, end-user errors and even as we have witnessed in today's corporate news, fraudulent embezzlement schemes. As you can see it is imperative to take precautions that prevent these bandits from targeting and sabotaging the fine efforts of your trusted employees and customers who rely upon your organization. Much hard work and profit have been undone by few keystrokes from a crafty Bandit.

The first step in securing your information system is to conduct a risk assessment and **security audit**. This will allow you to clearly understand your current security status and lay the foundation for a comprehensive security program that serves your company. The audit will also define who requires system access to specific data and identify the most pressing security risks. To be successful your assessment group needs to include key decision makers from all of your major business groups. Interestingly enough, over the years, I have noticed that this multi-layered responsibility has often been delegated to the IT Department to solve without the involvement of other key business areas. As a result the solutions implemented were driven solely by technology instead of addressing the organization's overarching business concerns.

Before you gather your busy colleagues together to form a posse and ride against these bandits; we recommend that you begin by formulating a strategy that serves both your business and technological goals. This strategy will incorporate the following areas of vulnerability into your security audit and generate a future security road map for your company. Your security audit document needs to include technical specifications for building and maintaining servers and the network as well as the human resources security policies and employee training regimes. With these three areas realistically assessed you can build an efficient and cost effective IT security system.

Level 1 Internet Protection: Firewall – Virus – Intruder - Secure Access

The first line of defense for your network is the **Firewall**. A firewall separates your valuable computer assets from the outside world. The word firewall comes from the practice of cutting gaps in the forest to create a fire break to keep forest fires from spreading to protected areas.

Think of a firewall as a gap to the outside world which is used to control access and act as sentry to control access to your organization. In practice firewalls are often used to keep Internet Bandits out of your network. Hardware firewalls are often incorporated as part of the router that connects your network to the internet. For firewalls to be most effective and flexible a combination of hardware and software firewall protection must be utilized.

The second line of defense is **Virus Protection**. Viruses are the most common and potentially costly security threats that your company will face. A virus is a malicious program that “infects” files and programs on your computer and then replicates itself to “infect” other files and computers throughout your network. There are two to three hundred new viruses written per month, so it is vitally important that you update your virus protection software running on all computers within your organization.

All of the major vendors update their virus protection files daily. It is essential that your security plan requires consistent virus signature file updating in order to maintain your safe levels of protection. Having old virus signature files will not protect the computer from any of the new viruses developed. Some of these viruses can be very destructive, such as the “KLEZ.H” Virus from earlier this year, which erased files when they were accessed seriously compromising the computer system.

Intruder Detection is the alarm system that tells you when a Bandit has tried to gain unauthorized access to your system. It may be as simple as disabling a Users Login ID after 3 unsuccessful attempts and generating a report or more comprehensive schemes which are supported by the router and firewall programs that stop Bandits from even accessing your system. It is essential that your security plan incorporate consistent monitoring of these security logs for potential security breaches. Along with Intruder detection vulnerability scanning is critical to insuring that all points of system access are protected from intruders. The vulnerability scanner is a software program that creates system attacks to seek out security holes. If a security hole is found, a report is generated that includes information on how to fix the problem.

A Virtual Private Network “VPN” for short is used when an authorized employee needs **Secure Access** to your corporate network from outside of your physical location. The connection to your computer network is “Virtual” as there are no hard wire connections between your employee and your company’s server; instead the network communicates through the Internet in a secure manner. This connection is “Private” due to several secure layers of encryption and authentication that are added to the usual Internet connection. The VPN utilizes advanced features of the firewall, encryption, and intruder detection to minimize the chance that a Bandit can gain unauthorized access your

network. Over the last few years VPN technology has dramatically improved in reliability, ease of installation and cost effectiveness offering every company access to this dedicated method of remote access security. One such system offers a LINUX based server which includes complex encryption algorithms, a powerful and flexible firewall, intruder detection capability and vulnerability scanners included in a single easy to use package.

Level 2 Access: Availability - Confidentially - Integrity - Recoverability

Your company's computer system must be **Available** for business usage by your trusted employee's. Most IT Managers strive for a system uptime number of 99.75% which equates to less than 1 day per year of system downtime. In order to achieve this required level of service availability the system will need to include several layers of physical fault tolerance and back-up redundancy of your system servers, disks, and computer network as well as a plan for disaster recovery. It is important not to overlook that redundancy and fault tolerance should also exist at the application level as well as the hardware level. In most large companies, e-mail is considered "mission critical" and is often a favorite point of attack by Bandits. This application must be safeguarded to prevent a loss of employee productivity that would result from an ambush or a hardware failure.

Confidentiality is insuring that the only trusted employees have access to the appropriate level of business data based upon their specific job functions. This requires that we have a solid understanding of what business functions require access and the ability to modify business data. For example, the company's CFO needs access to both view and modify accounts within the accounting database. The company's sales manager should on the other hand only have limited access to "view" specific database accounts; while the field sales representatives should be limited even further by restricting their access to "viewing only" their individual database accounts. By experience we know that all of this data resides within the company's information system and it is our responsibility to provide, both system access and protection as trusted individuals access the company's network.

Today's recent court rulings require that CEO's attest and personally stand behind the accuracy of their company's financial reports. Data **Integrity** today is critical to your personal and company's future success. It is our responsibility to safeguard and insure that the company's data is correct and has not been altered in inappropriate ways. Integrity can be achieved in part by physically securing the servers, and through the use of technologies such as audit reports and firewalls. It is vitally important to set up internal management procedures to limit access and audit trusted user's access within the system. For example, it is common in the banking industry to require that key individuals take their vacation time in one or two week blocks as most fraudulent accounting schemes require daily tending.

Entropy happens, hardware will eventually fail, end-users may accidentally lose data, and security systems may be attacked or even breached. It is important to have a robust backup and **Recovery** plan for your company. This plan must be part of your security model and above all it must be consistently utilized and tested. I was hired last year to

solve a recovery problem after Company XYZ had self-developed and installed a new data backup and recovery system for their computer network. When the fateful day arrived and their system needed recovery, the new backup system sprung into action and failed to properly restore their computer network due to a legacy programming error. This costly result could have been avoided by simply testing their recovery system as part of the system security model to insure that the recovery program was working properly.

The goals of IT System Security are to allow your trusted employees safe system access at their authorized levels of security in an efficient cost-effective manner with sufficient checks and balances that maintain a secure system. This technology plays an important role in maintaining and monitoring the daily systems activity but it's certainly not the most important aspect of a sound security system - your employee's are! Having solid **security training** and **computer usage policies** set up within your company are essential to maintaining a safe and secure system. The well-informed computer user is the safest computer user.

By successfully auditing your current security situation, creating a model of your business security needs, training your employees and implementing your plan you will be able to greatly minimize the risks of today's IT Bandit's breaching your system.

Mark McBurney is a 15 year Information Systems Veteran with extensive expertise in security system architecture, analysis, design, project management, infrastructure, technology transfer, business process modeling and data re-engineering . He can be reached for comments at (206)-261-7477.