

Secure It or Lose It

A comprehensive security policy for your laboratory can reduce vulnerability to attacks

Published in Scientific Computing - May, 2005

Michael H Elliott

In February of this year, ChoicePoint, a service provider of information for identification and credential verification, revealed that in October 2004, up to 145,000 consumer profiles were obtained by thieves using phony identities. In the same month, Bank of America "lost" backup tapes containing over 1.2 million charge card transactions and payroll processor PayMaxx disclosed that a security error left several customers' W-2 forms reachable over the Internet.

These are not isolated incidents. According to the 2004 Annual Computer Security Institute (CSI)/Federal Bureau of Investigation (FBI) Computer Crime and Security

Survey[1] over 50 percent of companies surveyed had at least one incident of unauthorized computer use within the last 12 months. Forty-nine percent reported thefts of computer equipment and 10 percent reported thefts of proprietary data and information. These incidents were not just from the local high school hacker — 58 percent of unauthorized incidents were from employees within their own company. Attacks on systems are coming from all directions.

In R&D, where scientific data management systems, electronic laboratory notebooks, instrument data systems and LIMS are increasingly being deployed to create the vision of the electronic laboratory, one would expect tight security over valuable intellectual property. Millions of dollars are being spent on systems to improve laboratory productivity and to support electronic patent filings and drug approvals. However, it is not surprising to walk into many of these laboratories to see usernames and passwords written on post-it notes, data servers left exposed underneath a bench, systems not being backed up, or passwords that never expire. Implementing a system security policy is essential to protect your electronic intellectual property.



Figure 1: System security diagram

The security policy

The threats to your data are increasing — external hackers, disgruntled employees, accidents, mistakes or malicious behavior. A security policy describes the steps, technology and processes you will use to protect your systems and data.

In essence, a security policy defines for your employees what can and cannot be done with your company's systems and information. Employees should not view security as a burden, but as a way of performing their responsibilities that protects the interests of their organization. Security is as much about people and processes as it is about technology. The policy should be a living document that is continuously updated to handle new security challenges.

Your security policy should, at a minimum, include the requirements and processes for:

- physical security
- operational security
- network security
- business continuity/disaster recovery

Once you have established a policy and have trained your organization on its use, random audits are necessary to ensure compliance. These audits are performed by a designated head of computer security. By establishing these standards, you will be better equipped to audit software suppliers for their ability to meet your security requirements.

A security policy is unique to each company and a complete list of typical requirements is extensive. The following is a summary of key points for security plan development:

Physical security

Physical access to computers or data storage devices is often overlooked. Physical security consists of the tools and procedures to restrict access to systems and media. Without physical security, unauthorized personnel can walk up to a computer and copy files, hack a system, steal a computer, or walk off with backup media. The increasing use of laptops has made it important to physically lock computers down via a cable or docking station or to place them in a locked drawer when not in use.

For networked client/server or Web-based applications, servers must be maintained in a separate locked room with access restricted to chosen staff. An electronic lock, which can identify and record who accessed the server room, is recommended. This closed environment must have the proper environmental controls and fire suppression systems. Uninterruptible power supplies (UPS) with surge protectors are used to prevent outages and electrical spikes from damaging systems and causing data loss. Backup media should be stored in locked, fireproof and waterproof cabinets and duplicate media should be stored off-site. System administrator passwords must be kept in a locked safe with no more than two people

Secure It or Lose It

having access.

Security is commonly breached by walking up to a system that is left in a logged-in state — or by reading a password left on a post-it note. If there are no access restrictions to the laboratory where client computers are located, the operating system or application should be configured to "time out" and log the user off after a period of inactivity. Screen saver passwords are easily hacked and are inefficient. Devices such as biometric readers, smart cards or USB tokens are increasingly being deployed to bridge physical and operational security. These require a user to insert a device into a reader or scan a fingerprint or retina in addition to the entry of a user name and password.

Operational security

Once a system is physically accessible, there must be a layer of security surrounding the operating system, application software and data. Accessing a system should not be easy, whether in research, development or manufacturing. An easy-to-sign-on system is vulnerable to attacks from both inside and outside your company. Your security policy should indicate the technology and procedures used for system sign-on and application rights.

Authentication to a system often involves a username and password sign-on to the operating system and application. System break-ins are often the result of sloppy

password management or the lack of coordination with the human resources department. It is not uncommon for terminated employees to continue to have access to their former employer's systems.

Application software used in the laboratory must restrict access to resources or functions within the system. For example, not everyone should have access rights to the system administration module. The rights to these resources are controlled through system privileges and are grouped together into roles. A role assigns rights to system functions and controls data access. A role might be created for technicians for data entry while a scientist role would allow data modification. An audit trail should record any data entry, deletion or alteration including who made the change and when. Not just for regulated laboratories, audit trails also are needed in discovery laboratories for patent defense.

Though currently used in only 30 percent of companies, PKI, or Public Key Infrastructure, is gradually gaining acceptance. PKI improves on the simple username and password by using encrypted key pairs to validate the identity of each participant involved in a transaction. Messages can be encrypted and decrypted using these keys. Commonly used for Internet financial data transmissions, PKI can be used for data transmission within a company's intranet or between outside research collaborators.

Any laboratory application that is being



evaluated for purchase should be reviewed in detail for its control of system functions and data access. Older applications with limited security should be replaced.

Network security

According to the CSI/FBI 2004 survey, companies surveyed lost over \$200,000 each as a result of viruses and worms attacking their computer systems. However, 99 percent used virus protection software. This shows that users were not maintaining their virus protection software and/or hackers were creating viruses faster than the protection companies could create new security updates.

Some of the attacks from hackers include:

- Viruses — A virus is a computer program developed to purposely attack another computer system. They can be as damaging as destroying all your data or as harmless as a message. They are primarily spread through e-mails and can replicate. The e-mails can be from captured addresses appearing to be sent from someone you know.
- Trojan horse — A program similar to a virus without the ability to replicate, a Trojan horse is created to gather information such as contacts, passwords or other sensitive information from your computer. A Trojan horse can be operating without your knowledge, trapping passwords as you type and sending them across the Internet.
- DoS — A denial of service (DoS) attack is an assault on a network that floods it with

data requests causing it to shut down. This can be from an external source or a malicious program within a company's firewall.

Each system on your network must have virus protection software and automatic updates. Your security policy also should reflect the acceptable use of the Internet, e-mail messages that should not be opened, e-mail filtering software, browser security settings, timing of security patches, and restrictions on personal software loaded onto company computers.

All networks tied to the Internet should have a firewall. A firewall is a physical device or software application used for controlling the flow of network traffic and to prevent unauthorized access to a network. All network traffic passes through the firewall and it screens which network packets are allowed through. A firewall also can encrypt/decrypt data.

A *DMZ* (demilitarized zone) network is a common firewall implementation. At least two firewalls are used to create a DMZ environment. The first firewall protects internal assets but allows the Web and mail server access to the Internet. The second firewall acts as an additional layer of protection, preventing external access to internal data sources and systems.

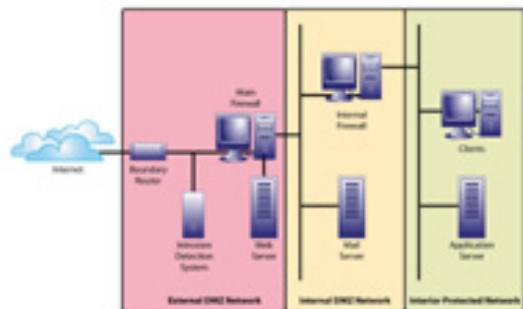


Figure 2: A DMZ firewall implementation

Intrusion Detection Systems (IDS) are devices or software that commonly work in conjunction with a firewall. An IDS detects and notifies an administrator of unauthorized attempts to breach a company's network or systems. IDS products are an important barrier to prevent DoS attacks. An IDS can instruct the firewall to block the Internet Protocol (IP) addresses of those systems that appear to be hitting the company's network too often.

Business continuity/disaster recovery

Disasters can strike an organization at any moment. They can be natural or man-made and prevent a business from operating. In this post-9/11 world, it is still amazing that there are organizations that do not have plans and practices in place for protecting their data and continuing the operation of their business.

Business continuity (BC) planning is the development of plans, processes and

procedures to resume critical business functions within an acceptable period of time. Disaster recovery (DR) planning documents the processes and technology for recovering and re-establishing related technology such as servers, networks, databases and clients. While disaster recovery is primarily about technical restoration, business continuity addresses the human and business processes. The level of BC and DR planning you need to undertake is dependent on the level of risk you are willing to accept. Your plan could be reverting to paper laboratory notebooks instead of using your ELN. Or, your plan could be installing redundant computers and data storage that are replicated with your primary systems and are maintained offsite.

Systems must be backed up on a regular basis to ensure the ability to recover from a disaster. Your policies and procedures should define the frequency of backups, the backup type, media, labeling and cataloging of media, and the physical media storage. There are various types of backup media, although we recommend magnetic media since optical formats change frequently. Backup software can automatically schedule and perform server and client backups at pre-determined periods of time, so there are no excuses for not backing up your systems!

There are three types of backups: full, partial or system image. Partial backups are usually more frequent, such as once a day. Full backups are generally once a week. It

Secure It or Lose It

depends on your level of risk and the amount of recovery time you wish to endure. The less frequent the full backups, the more time it will take to load and process the incremental media. Duplicates of backups should be made and stored offsite. Backup media stored onsite should be in fireproof and waterproof locked cabinet.

In summary, laboratories are implementing electronic environments to improve productivity, efficiency and collaboration. There are threats to these systems in the form of theft, accidents and malicious behavior. By developing and implementing a comprehensive security policy, organizations can reduce their vulnerability to attacks. As the 19th Century author Joseph Wood once said, "Security depends not so much upon how much you have, as upon how much you can do without." The question is: Can your organization really do without the significant investment you have made in data and information stored within your laboratory systems?

References

1. Ninth Annual CSI/FBI Computer Crime and Security Survey. 2004. Published by the Computer Security Institute.

Michael H Elliott is president of Atrium Research, a market research company focused on scientific informatics. He can be reached at info@atriumresearch.com.

