

Written and researched by:
Dr. Kirk Mousley
and Karl Mousley

Computer Security – Database, Network, and Internet – Part II

EDC Today is an independent publication on current information and issues in Electronic Clinical Systems (ECS) strategies and technologies for the Biotechnology and Pharmaceutical (Biopharma) industry. Each month we examine topics related to ECS theory, technology, practice, or implementation.

In last month's issue, we discussed the basics of computer security and the risks to computer systems and users. This month, we provide a strategy for computer security involving educating users, providing appropriate controls such as accounts and passwords, and using such tools as corporate firewalls. Ultimately, a heightened awareness of security issues, a good security protection strategy, and solid backup policies can help mitigate security risks and provide a basis for implementing a geographically-disperse ECS.

Introduction

Computer security should be a concern for all computer system users, and particularly for Biopharma companies that are employing ECS. Security is something that everyone must be aware of and everyone must be an active participant in any protection strategy.

Last month we covered basic computer security concepts and the risks one takes when they are not security minded. The cost of a security breach provides more than sufficient incentive for all computer system users and Biopharmas to develop effective strategies for mitigating these security risks, and using the Internet as a means for improving the process of clinical trial data processing.

It should be noted that the oldest form of computer security is keeping the computer (and the data on it) off of a network and secured from access (i.e., from unauthorized users, such as people carrying virus laden floppy disks!). However, this is impractical in today's client/server, web-enabled, home office world. Still, limiting exposure to attack is a very important and viable security concept.

In the next issue of
EDC Today:

An Update on CDISC

About EDC Management:

EDC Management is the leader in Clinical and Data Management and Electronic Data Capture (EDC) consulting services for the biopharmaceutical industry. EDC Management publishes well-researched and timely information about Electronic Data Capture technologies and processes through EDC Today® and EDC In Depth. We do not sell or endorse any specific EDC software application or vendor. Improve process today; position for tomorrow.

EDC Management

P.O. Box 384
Conshohocken, PA 19428
484-530-0300 (voice)
610-567-0357 (fax)
info@edcmanagement.com
www.edcmanagement.com



With an effective security policy in place, one can replace paranoia with forethought and vigilance. In this month's issue, we present some basic points for a security protection strategy. Our strategy involves a mix of user education, well thought-out processes, and protective tools. In addition, computer system backups and other disaster recovery strategies are necessary components to a complete security plan.

Finally, we conclude with a discussion of the tradeoffs between security and productivity. A completely secure system will have a negative impact on productivity. Security indisputably adds extra steps to each person's work, increasing the time required to complete the task. However, too lax of a protection strategy opens many "holes" and exposes the Biopharma's computer assets to potential loss.

Protection Strategy

Protecting one's computer-based assets begins with common sense. Some universally applicable security guidelines Biopharmas should teach users / enforce are:

- Don't leave your cellular phone, Personal Digital Assistant (PDA), Blackberry device, laptop, or desktop unattended.
- Log out of applications when stepping away for a few minutes.
- Log out of Windows or use a screen saver with a password to lock your workstation when you are nearby but not using your workstation.
- Turn off devices containing sensitive information when not in use.
- Keep mobile devices in a secure place when traveling.
- Keep your networked device, laptop, and office locked when you are away.
- Don't leave group or shared accounts/passwords written down on or near computers.
- Download and install Microsoft Critical Windows Updates when they become available. According to Microsoft:

Security updates help shield your computer from vulnerabilities, viruses, worms, and other threats as they are discovered. Windows XP has an Automatic Updates feature to download the latest updates automatically on a schedule you choose.¹

- Be extremely careful when downloading ANYTHING from the Internet, either directly or in the form of e-mail and multimedia files! Be sure a web page uses Secure Sockets Layer (SSL) before submitting sensitive information over the Internet.
- A personal firewall program such as Zone Lab's ZoneAlarm can be used instead of buying a hardware firewall.² Many broadband connection-sharing devices (e.g., Linksys' EtherFast Cable/DSL Router with 4-Port Switch) have built in firewall capabilities. When using a firewall, it is important to understand and correctly configure it!

(continued on page 3)



Biopharmas should also create policies for their internal IT departments to follow:

- Define roles that limit access to only those privileges that are needed to perform day-to-day tasks.
- Create a password policy that includes minimum lengths and maximum lifetimes, exclude easily guessed words, and do not allow reuse. Require users to change pre-supplied or default passwords immediately.
- Avoid e-mailing passwords when possible. Require users to change passwords that are e-mailed to them as soon as possible.
- Assign limited access to shared accounts (such as guest accounts). Remember, 21 CFR Part 11 regulations require electronic signatures that usually consist of username and password. Therefore, shared accounts are not allowed in a regulated activity.
- If multiple users are allowed to use local computers, each authorized user should have their own account on the local machine.
- Require an Internet Firewall on all remote computers. Again, according to Microsoft:

An Internet firewall is a piece of software or hardware that helps screen out hackers, viruses, and worms, which try to reach your computer over the Internet. If you are a home user or small-business user, installing a firewall is the most effective and important first step you can take to help protect your computer. It is important to have a firewall and antivirus software turned on before you connect to the Internet.³
- Investigate and deploy VPN gateways where appropriate.
- Use an up-to-date Anti-Virus program. According to Microsoft:

Antivirus software is a program that either comes installed on your computer or that you purchase and install yourself. It helps protect your computer against most viruses, worms, Trojans, and other unwanted invaders that can make your computer “sick.” Viruses, worms, and the like often perform malicious acts, such as deleting files, accessing personal data, or using your computer to attack other computers.⁴
- Use an Anti-Malware/Spyware program. These programs, such as Lavasoft Ad-aware, find and remove malware and spyware.⁵
- Help users by providing reminders and links to download security updates.

User Education

User education should include understanding security-oriented Standard Operating Procedures (SOPs) and training that includes the specifics of a Biopharma’s protection strategy. Biopharmas should have in place, or implement, SOPs covering various aspects of computer security. Such SOPs should cover, amongst other areas: password, antivirus and updates, home office, mobile computers (including laptops), and computer system backup policies. Employees should be trained on all aspects of a Biopharma’s protection strategy during new employee orientation (and perhaps even on an annual or “as-needed” basis).

(continued on page 4)



In such training, the IT staff should offer explanations of any workstation “lock downs” that are part of their security policy. It should be understood by the employee that the Windows desktop configuration, software installs, and other attributes (e.g., network access) established on the workstation assigned to them are all usually done in a pre-packaged, validated setup that is maintained by the IT department. The workstation is not necessarily their “Personal Computer” and is not necessarily to be “customized” by the employee (e.g., the addition of personal software such as games). However, any IT department that restricts user configurations/customization actions by “decree” or “fiat” (that is, without explanation of their reasoning) merely challenges power users to circumvent those IT actions seen as “silly” or counter-productive. The power user’s circumvention could prove dangerous and make the Biopharma computer assets vulnerable to security breach.

Back up/Disaster Recovery

Employees should know that important files should be on the appropriate server (network folder) and not left on their workstation, home office computer, or mobile PC. In many cases, Biopharmas only back up files and data located on servers and ignore user workstations.

A thorough protection strategy will include a Disaster Recovery plan that covers computers and computer assets. A comprehensive disaster recovery plan will include back up (and restoration) of files and data. The important thing to remember though is the disaster recovery (e.g., the restoration of computer files and data) should only be considered as the absolute last line of defense in a protection strategy.

Security/Productivity Tradeoff

Security involves limiting access to applications and data. Security also involves scanning files for viruses. Each of these actions can have a negative impact on productivity. The ideal balance is to have enough protection in place to satisfy one’s tolerance for risk without making it too burdensome for computer users to accomplish their jobs.

User accounts are necessary to secure workstations, applications, and data. Most employees log into their workstation on a daily basis, and as such, that level of security is not usually problematic. However, oftentimes employees will have to log into different software applications, such as the Clinical Data Management System (CDMS) or the Internet Portal. The repeated need to log in slows people down. Plus, as the number of applications that a user has to log in to increases, the number of passwords does as well, challenging the user’s memory. If a Biopharma thinks users may write down passwords, they should attempt to provide a single log in and password that grants the user access to all of their applications. While this also boosts productivity, it, too, is a security risk in that once that single password is compromised, then all applications are open to intruders.

Different accounts have varying privileges within a given application. For example, one might have data entry privileges but not administrative privileges. Giving more privileges to a particular account will enhance what a person can accomplish as part of his job. However, granting too many privileges increases the likelihood of inappropriate tasks being performed, either intentionally or otherwise. Many companies are very restrictive about administrative level functions for good reason, but sometimes developers need administrative access to set up applications. Care must be taken that developers can get their work done in a timely fashion, and not have to wait for administrators to run certain scripts or perform certain functions.

(continued on page 5)



Virus scans and firewalls need to be carefully implemented. Virus scans can start at inopportune times, such as when someone is in the middle of doing a task, and can be very disruptive. Virus scans can also create problems with files being locked when a person attempts to access them. Firewalls, in a similar manner, may prevent access to certain applications that are required for a person to perform his/her job. As a matter of policy, some Biopharmas prohibit the use of certain “ports”. These limitations prevent malicious access, but may also prevent intended application behavior.

One factor to consider is that a certain level of security contributes to employee awareness. With employees mindful of security, they will be more likely to be conscientious and not careless.

Each Biopharma has to decide what level of protection they want, and how much they are willing to accept in terms of lost employee productivity. Unfortunately, there are no easy answers.

Conclusions

Security is the responsibility of every computer user. It is very important for all users to be aware of security issues and concerns. Security starts with a user’s local computer, whether it is a desktop or a laptop computer. Biopharmas must make sure each person’s local machine is secure, and that they do not share their password(s) with others. If other authorized users (such as network administrators) are allowed to use the local computer, each authorized user should have their own account on the local machine.

In addition, when users are working away from the office (and away from their IT support staff), they need to assume the role of Chief Security Officer (CSO). Users are solely responsible for any computer equipment when they are out of the office, including loading Windows updates and Anti-virus updates. However, a company’s IT staff may help users by providing reminders and links to download any security updates that are required.

With well-educated and conscientious computer users, a company can feel fairly confident that necessary precautions are in effect. With a good security policy in place, a company can then evaluate the benefits of ECS, including EDC and mobile workers, and compare these benefits against the risks of security breaches. We believe that the benefits outweigh the risks when a strong security policy with educated and careful employees is implemented.

References

¹ <http://specials.msn.com/msn/security.asp>

² <http://www.zonelabs.com>

³ <http://www.microsoft.com/security/protect/firewall.asp>

⁴ <http://www.microsoft.com/security/protect/antivirus.asp>

⁵ <http://www.lavasoft.de>



Who's behind the research?

Our lead researcher, Kirk Mousley, PhD received BS and MS degrees in Electrical Engineering from MIT and a PhD in Computer Science from Lehigh University. He has been the President of Mousley Consulting, Inc. since its founding in 1993 and has directed the company's efforts in the areas of clinical database design, data editing/cleaning, document management, and submissions.

Karl Mousley received his BS in Mechanical Engineering from Rose-Hulman Institute of Technology and a MS in Computer Science from Villanova University. He has been a senior member of the technical staff at Mousley Consulting, Inc. since 1993. Among his significant accomplishments are the investigation, evaluation, and implementation of new computer technologies for clinical data management systems and developing strategic plans for integrating these technologies into current systems. He has extensive experience preparing Standard Operating Procedures (SOPs).



EDC Today and EDC In Depth

EDC Management publishes well-researched, timely information about EDC technologies and processes.

EDC Today is a free electronic technical bulletin.

Each month we examine topic areas related to Electronic Clinical Systems (ECS) theory, technology, practice, or implementation.

Each *EDC In Depth* research report comes with an executive summary and may be purchased individually for \$395 or as a group of related reports for \$975. Available via downloadable electronic version or paper version sent via mail.

To subscribe to ***EDC Today*** or purchase a specific ***EDC In Depth*** research report:

Order online at
www.edcmanagement.com

Email us at
info@edcmanagement.com

Call us at
1-484-530-0300