

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

Computer Security: Database, Network, and Internet – Part I

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.

Recently, a number of readers have requested we write about some areas of clinical computing that might be vulnerable to security lapses and what they might do to protect themselves. In fact, some readers continue to indicate that concerns about security have prevented their company from moving forward with Electronic Data Capture (EDC).

In this issue, we discuss the basics of computer security and the risks to computer systems and users. Next month, in part II, we will 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. The risks of security breaches can be as innocuous as lost data that must be re-entered with some expense, or it might be as severe as losing the patent on a blockbuster drug which goes without saying is very expensive.

For some Biopharmas, the concern over security has curtailed their attempts to adopt EDC. While these concerns are valid, Biopharmas can develop effective strategies for mitigating these security risks and use the Internet as a means for improving the process of clinical trial data processing. The key is to replace paranoia with forethought and vigilance.

(continued on page 2)

*In the next issue of
EDC Today:*

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

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



In this issue, we discuss basic computer system security concepts. Our discussion starts at the local computer workstation level and expands to the Internet. We start with what each user can and should do at their own computer, what departments should do concerning access to applications and computer resources, and how companies can open their networks and applications to Internet users.

Next we discuss what security risks are present. We also point out that, contrary to what many people believe, it is the employees of a company that are the biggest security threat to the company, be it accidental or intentional. An understanding of the risks being faced allows one to determine a protection strategy. In next month's issue we will present some basic points for a security protection strategy.

Basic Computer System Security

Users should respect the sign on (i.e., log in) process at their own workstation. Memorizing, and signing in with, a username and password may seem to be a "chore" to some, but it is often the first and last line of defense against malicious attacks. In most cases, computer assets are NOT to be left on an employee's workstation but rather on a company server. However, some users defeat in part or entirely, the security put in place on these servers by making local copies of day-to-day work. Documents and other files left on a workstation may not be protected from eavesdropping or loss (i.e., most companies only backup files found on servers.)

Quick Definition:

Eavesdropping: someone could "watch" the data as it streams by and capture un-encoded (clear) text information such as passwords and credit card numbers and could capture encryption keys and use them to decode encoded network traffic (i.e., text).

Most of the larger Biopharmas have an IT staff that manages the server or servers that house the company's vital computer assets. These servers are nearly always secured behind locked doors. The smaller Biopharmas, however, may not have a knowledgeable IT staff in-house, and may not know how to secure their server(s). Documents and files such as SAS datasets usually reside as files on a server. They are made available over the local area network and are protected using LAN-based security means, such as file sharing privileges and/or domain roles. Many Biopharmas use "Microsoft Domains" to manage their company's computers, files and other resources, along with their users. According to Microsoft: "a domain is an administrative boundary"¹ which basically means someone designated as the "network administrator" uses enterprise-level tools built into Windows server operating systems (e.g., Windows 2000 Server) to manage network resources (i.e., computer assets) and users. Microsoft domain roles work much the same way as Oracle roles described below and should be set up to protect computer assets found within a network.

(continued on page 3)



A clinical trials database is a special kind of network asset. Clinical trials data is usually stored in a Relational Database Management System (RDMS). The key difference between an RDMS and a database (such as Microsoft Access or perhaps Excel) is the “Management System” portion of a RDMS. This is where user accounts and access rights are established and maintained. Even though the data in an RDMS exists physically within files on the network, it is not viewable to those without user accounts and access privileges. Access to RDMS-stored data should be controlled with the use of roles, such as those found in Oracle. As described by Oracle:

“A role is a set of privileges that can be granted to users or to other roles. You can use roles to administer database privileges. You can add privileges to a role and then grant the role to a user. The user can then enable the role and exercise the privileges granted by the role.”²

Wireless Area Networks (WLANs) are an emerging technology that permits access to network resources usually via radio waves. As with company servers, wireless access within a Biopharma is likely to be managed by a knowledgeable IT staff and secured from unauthorized use. The smaller Biopharmas and home office users, however, may not know to change the common insecure default settings of their wireless “access points”, specifically establishing Wired Equivalent Privacy (WEP) encryption for their wireless networks (e.g., also known as Wi-Fi and Airport.)³ See Issue 25 of EDC Today, *Mobile Computing - the Basics*⁴ for more details concerning security and wireless computing.

Home Office and Working on the Road

Typically, home office computing involves some sort of connection to the Biopharma server(s) in order to either transfer files (e.g., documents) or other data. This connection might involve directly dialing up to the company’s network, which is probably the most secure, but most cumbersome and/or expensive way to establish a connection. With the increasing availability of inexpensive broadband, home office users more often connect to the company’s servers via the Internet. For security reasons, this connection is commonly established using an “over the Internet” networking protocol called Virtual Private Network or VPN for short. Occasionally, access to computer assets is via a web site (e.g., a portal – for more information about portals see Issue 12 of EDC Today, *Portals, and How They Can Make EDC Work Better*⁵) or other “Extranet” Internet application. We recommend this access be secured by the use of the Secured Socket Layer (SSL) encryption. In order to encrypt your Web page, the server and the client go through a very complex series of transmissions back and forth to one another in order to encrypt and decrypt information. See the Side Bar “Encryption via the Secured Socket Layer (SSL)” for details on how SSL works.

Computing on the road brings its own unique demands on security. The security threat is primarily theft or loss of the physical computing device (e.g., PDA or Laptop) carried by the traveler. The traveling computer user who is a “guest visitor” to a network (e.g., a medical monitor at an investigator site) could also be deemed a security threat, for instance, the source of a computer virus if the traveler doesn’t safeguard against them.

(continued on page 4)



Side Bar: Encryption via the Secured Socket Layer (SSL)⁶

Here is a basic explanation of the encryption process:

- First: A client requests a SSL (Secured Socket Layer) connection with the server
- Second: The server sends a Certificate
- Third: The client validates the Certificate, creates a session key and encrypts the Certificate with the key
- Fourth: The server decrypts the session key and establishes the encrypted connection

At this point, all you have is an established connection. “Real” information, e.g. actual user data, has not yet been sent.

The Certificate that the server sent out is what makes this whole process work. A Certificate is obtained from a Certificate Authority, which is sort of like a notary public that verifies the Certificate's authenticity, hence the name. The Certificate contains the common name of the server, making it impossible to use on other servers. It also uses a public and private key to create and verify a secured connection. The keys are an important part of the verification process.

Using a “public” computer brings another security issue to light — browser cookies and history. Often Biopharma staff use an Internet café or other public use computer (such as a school library or work break room) to check e-mail. Services like Hotmail.com offer features that “remember your username” and even passwords. Users should always look for and select the “Do not remember my e-mail address for future sign-in. (Select this when using a public computer.)” option when logging in. Avoid the “Log me in automatically” option that records your account name and password in a cookie that is left on the computer. Always remember to sign out when done, and try to delete cookies, history, and the browser cache.

Security Risks - In Terms of Threat and Potential Loss

Common No-no's

Perhaps because the value of the computer asset is not visible or tangible, computer security is often compromised by careless or thoughtless behavior. Often, the excuse offered by the offender for thoughtless behavior is that maintaining security is “inefficient” or slows down work efforts. If they thought about or knew how many dollars the computer assets they left exposed to damage or theft, they might recognize the need for keeping the assets secure. A common way for someone to permit a security breach is leaving a post-it or notepaper with username(s)/password(s) on them on or near a computer that is accessible by a number of people. Another common security problem is the failure to lock up hardware, particularly servers and server rooms/closets, when it is not in use.

(continued on page 5)



Outright Loss

So what are the risks to your computer assets if your wireless device (cell phone, pager, blackberry device, PDA, or notebook computer), ePatient Diary Device (ePD), or even desktop PC is stolen? What data do you keep on them? Can someone else access the data stored within the device if they are turned on? Obviously, a cell phone can be used to make expensive calls very quickly after being stolen, but perhaps the address book containing your contact information is of significant value too? Beyond the cost of replacing both the phone and the address book, are exposure of unlisted numbers and other loss of privacy issues. A monitor's cell phone might list all the site investigators for a clinical trial. What is the cost of losing this information? Far-fetched as it might be, what could your competitors or a malicious prankster do with this information if they had it? Do you have any "important" files on your computer that would be expensive to replace? Does your computer contain sensitive information regarding your company or clinical trial you are working on? Do these files belong on the corporate server and not on your hard drive?

Unauthorized/Unintended Access

What are the consequences of someone simply using your computer because you either left your username and/or password on or near your computer or left the computer logged in and walked away? Could a malicious prankster send an embarrassing e-mail using your name? Find credit card information? Browse clinical data and alter or delete it under your name? What files and information might the malicious have access to? What computer assets do you have access to? Do you know what value they have? If you thought you might be blamed for the loss of these computer assets, do you still believe that you "require" access to those assets to efficiently perform your work?

Stolen Data

What are the consequences of losing your data? If someone were to copy it, would you be able to tell? What is the value of this computer asset? Can this stolen data be used by someone for profit or used to embarrass you?

Data Stream Is Snooped

The data that runs from a computer to another computer on an intranet or Internet network (either wire or wireless) is, at least in theory, vulnerable to eavesdropping. While this may sound improbable, there are instances where it has been done. The less secure the network, both in terms of physically (e.g., wireless is usually less secure than wired) and in configuration (e.g., clear text versus encoded text) the more susceptible it is to a breaching attack.

(continued on page 6)



Virus Infection

Virus infection seems to be more of an embarrassment than a threat to many, but consider your loss of productivity if your email server becomes clogged with emails caused by a virus, or your EDC server becomes subjected to a “denial of service” attack that prevents you from accessing your clinical trials data? More traditionally, but probably far more rarely, what if a virus did damage or destroy files on your computer? Common ways for viruses to get to your computer include opening non-business related e-mail attachments from “friends” or visiting websites and downloading, installing and running computer programs that seem like “fun”.

Malware/Spyware

Closely related to some viruses are malware and spyware. An unsuspecting website visitor may be informed that they need to download a program in order to fully experience a web page. The downloaded program that is installed may contain malware and/or spyware, that is, software or files that aids in gathering information about a person or organization without their knowledge. Malware is unwanted code against which antivirus software is usually powerless. Malware consists of “electronic burglar tools like password crackers, network traffic sniffers, keystroke loggers, data scroungers and remote access programs that are being used by attackers to capture passwords, spy on network traffic, record private communications, and stealthily receive and transmit unauthorized commands to and from remote hosts.”⁷

Conclusion

Security is the responsibility of every computer user. It is very important for all users to be aware of security issues and concerns. Education goes a long way. One who is educated about car theft would not leave a car unlocked with the key in the ignition in a crowded unlighted place at night. Likewise, one who is educated about computer security issues would not leave an application running on their computer unattended.

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

Next month, we will build upon the understanding of security risks by presenting a protection strategy that both Biopharmas and their users can adopt to reduce their exposure to loss. In addition, we will discuss the tradeoffs between security and productivity.



References

¹ <http://www.microsoft.com/mspress/books/sampchap/3173.asp>

² <http://www.hec.ca/mireault/bde/doc/ch4g.htm>

³ <http://workingmac.com/inetd/22.wm>

⁴ *EDC Today*[®], Issue 25, "Mobile Computing – the Basics"

⁵ *EDC Today*[®], Issue 12, "Portals, and How They Can Make EDC Work Better"

⁶ <http://www.developer.com/net/asp/article.php/931501>

⁷ <http://www.computercops.biz/article744.html>

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