Improving data security in small businesses

Kent N. Schneider
East Tennessee State University

ABSTRACT

Data security is critical to the operation of any business. Large companies undoubtedly have information technology (IT) experts who design and maintain data security through sophisticated techniques and expensive hardware, most of which are beyond the budgets of small businesses. Using a life cycle approach, this article provides an overview of common business practices that can subject confidential data to risk of loss or misuse, along with suggestions for reducing such risks at little or no cost to the small business owner.

Keywords: keystroke logger, two-factor authentication, cloud storage, remote access, password

INTRODUCTION

For all businesses, maintaining control over electronic data is paramount. In the early years of computers, the primary focus was on physical controls over the storage media. Keeping the filing cabinets locked and the floppy disks safely stored solved most data security problems of that earlier era. Today, however, physical controls are not enough to protect digital data. The pervasive use of both wired and wireless devices for exchanging and storing data on or through the internet requires businesses to supplement their use of physical controls with increasingly sophisticated logical controls, such as data encryption and hardware authentication tokens. Large companies undoubtedly have information technology (IT) experts who design and maintain data security through sophisticated techniques, most of which are beyond the scope of this article and beyond the budgets of small businesses. This article will provide an overview of common business practices that can subject confidential data to risk of loss or misuse, along with suggestions for reducing such risks. These vulnerabilities will be examined by considering the four stages in the life cycle of data: data creation, data storage, data transmission, and data destruction.

DATA CREATION

Data security begins at the point of its creation. To ensure that confidential information is not leaked as it is created, steps must be taken to prevent its interception. If computer monitors are positioned in a highly visible location, “shoulder surfers” can view or photograph the screen. This can be avoided by arranging the workstations so that the monitors are not visible to unauthorized personnel located either inside or outside the building.

An even greater risk is posed by keystroke loggers. These can come in the form of software installed on the computer or in a hardware device that is physically connected to the computer. Software keystroke loggers can be purchased commercially and installed for the purpose of monitoring children or employees. (Rubenking, 2012) In the context of data loss, it is more likely that the logger is “spyware” or “malware” surreptitiously installed via a malicious website or email message. To defend against this type of invasion, each workstation should be continuously protected with antivirus software like AVG Anti-Virus Free Edition, Avast Free Antivirus, or Panda Cloud Antivirus. (Mediati, 2012) In addition, each computer should be subjected regularly to deeper scans using rootkit detection software. (Romano, 2012) To protect against hardware loggers, visually scan the USB ports and keyboard of each workstation on a regular basis. If any change is noted, the workstation should not be used until this modification has been evaluated and determined to be legitimate.

DATA STORAGE

When addressing data storage, the most common concern deals with providing safe, routine backups of mission-critical data. Most small businesses typically do a good job of addressing the issue of data recovery, but they may fail to consider the risks of data “leakage” and unauthorized access to company or customer data. Restricting physical access to the company’s computers is seldom overlooked. On the other hand, many small business owners may be unaware of the subtle risks posed by their password policies and the commingling of business and personal data by the company’s employees.

Employing poorly designed password practices

Passwords are intended to limit access to authorized users of the computer resource. If the password policies are too weak, they offer little protection to the stored data. Conversely, if they are draconian, users will be tempted to undermine the process by writing their passwords on a post-it note placed near the computer. This is the inevitable trade-off of security and convenience.

To strike a balance between security and convenience, many password policies permit users to create their own passwords that include upper-case and lower-case letters, numbers, and special symbols and are of at least a minimum length. (SANS, n.d.) This sounds good, but human nature tends to subvert the results. One problem is that the user of a truly secure password tends to use it on multiple web sites and networks. Thus, if that user's account is compromised on one system, then the user's other accounts become vulnerable. The other problem is that password cracking technology has improved dramatically in the past decade. Free password-cracking software is available for download and use by anyone. In addition, by adding multiple graphics display cards to off-the-shelf computers, hackers can process billions of password combinations per second. (Verry, 2012) As a result, passwords can be cracked with frightening ease. For example, in June 2012, hackers stole 6.5 million hashed (encrypted) passwords to LinkedIn accounts. Six days later, more than 90 percent of these passwords had been cracked. (Goodin, 2012)

To remedy the weaknesses of passwords, the security industry is moving toward two-factor authentication. (Gibson, 2007) Two-factor authentication requires a user to supplement his or her password, which is "something you know," with "something you have" in order to log in. The "something you have" factor can be (1) a biometric reading, such as a scan of a user's retina or fingerprint, (2) a hardware token, such as the RSA SecurID or the Yubikey, or (3) a software token, such as Google Authenticator that provides a unique, randomly generated six-digit number transmitted to the users' cell phone for entry on the login screen. Thus, data is protected even if the user's password is compromised.

To optimize the user's secure access to systems, one can combine the use of a password manager, such as LastPass or Password Safe, with two-factor authentication. For example, LastPass can generate unique passwords that are long and contain numbers, uppercase and lowercase letters, and symbols. After generating these passwords, LastPass will encrypt these passwords using your LastPass master password and store them for later use. To use passwords stored in your LastPass vault, you must remember and enter your master password. If you choose to use two-factor authentication with your LastPass account, you must enter your master password *and* your Yubikey or Google Authenticator information in order to use your stored passwords. (Henry, 2012)

Mixing business with pleasure

A conscientious employee who wants the ability to work on company business after hours or on the weekends may be tempted to store company data on his or her smartphone or USB drive and take it home. The primary risk of storing company data on personal devices and cloud accounts is that the data may be stored in an unencrypted format that can be read by any user with access to the device. More recently, free cloud storage accounts, such as Apple's iCloud, Google's Gdrive, and Microsoft's SkyDrive, have added a new twist to this practice by allowing the employee to store company data on his own private cloud storage account.

As storage devices get smaller, the likelihood of losing or misplacing these mobile devices increases. Similarly, as more company data migrates to employee cloud storage accounts, the risk of unauthorized access by hackers increases.

A related vulnerability involves the use of company computers, laptops, and tablets for personal purposes. Although convenient for the employee, this practice increases chances of inadvertent introduction of viruses, worms, spyware, and malware into the company network. Once installed, these malicious programs can compromise a company's data in a variety of ways, ranging from surreptitiously sending confidential data files to an attacker's computer located outside the company's firewall to crashing the network and deleting all data stored on the network's file server.

To reduce these risks, a company could establish a policy that proscribes both the storage of company data on personal devices and the installation of personal software and data on company machines. Of course, to be effective, these policies must be monitored and enforced. Alternatively, the company could explore more nuanced approaches to this problem, such as wireless security management systems (WSMS) and "thin computing." (Aldhizer and Bowles, 2011)

DATA TRANSMISSION

Even if the company has locked down the secure business information by protecting the stored data with secure passwords and segregated it from personal data, these protections can be forfeited if the data is transmitted in an insecure manner. The risks of insecure data transmission range from the nontechnical mistakes of authorized users to the high-tech issues of remote access and cloud storage.

Email hazards

The most embarrassing type of data leakage is the misaddressed email message. Sending confidential information to the wrong customer or to the opposing party in litigation can be devastating. To avoid this calamity, remove the "Reply All" command and icon from the company's email client. (NoReplyAll, n.d.) If the message is important and is intended only for select recipients, require the sender to separately enter the email address of each recipient. In addition, implement a company policy that requires all email to contain concise, meaningful subject lines in a standard format. Finally, encourage users to review the email addresses and subject lines for inconsistencies before clicking the "Send" button.

A more insidious type of email data loss is technical in nature. Email is sent over the internet without encryption. With the use of a "packet sniffer," email and its attachments can be captured and read as they are transmitted over the internet. In other words, an email message is more like a postcard than a letter sealed in a routing envelope. Anyone with access to the postcard can read its contents. To eliminate this risk, encrypt all confidential email messages and attachments. To improve compliance with this policy, the company could automatically encrypt and decrypt email messages passing through its email servers. A convenient way to implement this process is to install a Unified Threat Management (UTM) device on the network. These devices, such as the Sophos UTM, not only boost email security, but also protect the network from intruders attempting to infiltrate the company’s network via the internet or the company’s wireless routers. (Ashford, 2012)

Remote access by authorized users

When a trusted employee is on a business trip, he or she often must access the company’s network or email server. The risk of remote access is a “man in the middle” attack. For example, the road warrior obtains internet access via the hotel network. Unless proper precautions are taken, another computer on the same network could intercept the commands sent by the employee, read them, and then relay them to the intended remote site. When the remote site sends a response, the “man in the middle” captures that information and relays it back to the user in the hotel room. To avoid this risk, the employee must connect to the company network using a Secure Sockets Layer virtual private network (SSL VPN). The VPN is a secure tunnel between the remote user’s computer and the destination network’s VPN server. The tunnel is secure since all data passing through it is encrypted. To a “man in the middle,” all traffic sent over the SSL VPN will appear to be random noise, rather than messages to be captured and read.

Cloud storage

Storing data in “the cloud,” that is on remote file servers such as Amazon Simple Storage Service or “Amazon S3,” offers significant benefits and conveniences to users. First, cloud storage can provide off-site backup of critical data. Physically located in a different part of the country or world, this remotely-stored data will be safe in the event that the company is a victim of fire, flood, or other natural disaster. Second, data stored in the cloud can be accessed by employees working at customer sites via smartphone, tablet, or notebook computer. This is a great convenience since it eliminates the need for carrying storage equipment or media while on the road. In addition, it can improve data security. Since the data, or at least the bulk of the data, is not stored on the portable device itself, the loss or destruction of the device typically will not result in the loss or compromise of the data.

The promised benefits of cloud storage must be balanced against the new risks that are inherent in the use of the cloud. Most of these vulnerabilities can be identified by a careful reading of the cloud storage provider’s terms of service. First, as with remote user access of the company’s network, all data sent to and retrieved from the cloud storage site must be sent via an SSL connection to prevent “man in the middle” attacks. (Gibson, 2009) In addition to providing secure transmission, data must be stored on the cloud in encrypted form. Otherwise, one’s data would be vulnerable to misappropriation by a hacker who breaches the storage site’s security or by a dishonest employee of the cloud storage facility. Finally, even if the data is encrypted and transmitted via SSL, control over the encryption key is still a concern. If the storage facility has the encryption key, the stored data remains vulnerable. To be truly secure, the company must encrypt its data using a strong encryption algorithm *before* transmitting the data to the cloud storage site. Moreover, the encryption key must remain solely in the custody of the owner of the data.

DATA DESTRUCTION

When paper documents containing confidential information are to be discarded, it is routine practice to shred them before throwing them in the dumpster. Similarly, when old electronic storage media are retired, the data stored on that media must be destroyed.

Degaussing

Heavy-duty shredders can render CDs and DVDs unreadable, but the same cannot be said of USB drives and hard drives. For these devices, degaussing or demagnetizing the device can be effective if done properly. Simply placing a strong magnet near the storage device can destroy the data, but it is unreliable. In contrast, degaussers approved by NSA and the DoD are effective but expensive and time-consuming.

Physical destruction

Another option is physical destruction of the storage media. Admittedly, this approach may not be "environmentally friendly," but it can be an economical and effective method of rendering many devices unreadable. Most USB drives are easily dispatched with a hammer. Surprisingly, the same technique is effective with all but the oldest hard drives. Originally, platters inside hard drives were metal, but modern hard drive platters are constructed of glass or ceramic material. To destroy the data on these drives, simply toss the drive onto the sidewalk. To make sure the platters are destroyed, shake the drive and listen for the sound of sand moving inside the drive. For older hard drives with metal platters, one must drill a couple of holes through an entire drive to render it unusable.

Overwriting stored data

If the goal is to destroy the data and yet be able to reuse the hard drive, a software approach is needed. Deleting all of the files is ineffective, since these files can be recovered using simple "undelete" utilities. Instead, one must use a "data shredding" program that overwrites all of the data stored on the drive. Free software tools that accomplish this task include CCleaner, Darik's Boot and Nuke, and SDelete. (Best, 2012) These tools are effective, but they do require a significant amount of time to accomplish the process.

Covert data storage risks

The decommissioning of computers, hard drives, and other storage media are events that obviously require data sanitation. Less obvious are the photocopiers, multi-function printers, and telephone answering machines that are capable of storing images of confidential documents. Both types of devices scan documents and store them, at least temporarily, while awaiting the printing or transmission of the document. Some of these copying machines encrypt the stored images or automatically overwrite the images after printing, but many older machines store the images for long periods of time without any attempt to obfuscate the data. Consequently, companies should implement and enforce a decommissioning policy that requires all office machines to be examined for data storage capabilities prior to disposal. If a retired machine is found to contain stored data, the policy should require that the embedded storage device be destroyed or “sanitized” prior to disposition.

CONCLUSION

This article provides small businesses with an overview of common practices that can subject confidential data to risk of loss or misuse, along with suggestions for reducing such risks. These suggestions are summarized in Figure 1 (Appendix). Hopefully, many of these security practices are in place already. If not, please consider this to be a wake-up call to improve your company’s data security with a modest investment of time and money.

REFERENCES

Aldhizer, G.R. and Bowles, J.R. (2011). Mitigating the Growing Threat to Sensitive Data: 21st Century Mobile Devices. *The CPA Journal* 81(5), 58-63.

Ashford, W. (2012). Sophos combines endpoint security and UTM. *ComputerWeekly.com*. Retrieved October 24, 2012 from http://www.computerweekly.com/news/2240159617/Sophos-combines-endpoint-security-and-UTM

Best free secure erase utility. (2012) *Gizmo’s freeware*. Retrieved October 24, 2012 from https://www.techsupportalert.com/best-free-secure-erase-utility.htm

Gibson, S. (2007). Multifactor authentication, *Security Now!* Retrieved October 24, 2012 from https://www.grc.com/sn/sn-090.htm

Gibson, S. (2009). “The SSL/TLS Protocol,” *Security Now!* Retrieved October 24, 2012 from https://www.grc.com/sn/sn-195.pdf

Goodin, D. (2012). Why passwords have never been weaker—and crackers have never been stronger, *Ars Technica*, Retrieved October 24, 2012 from http://arstechnica.com/security/2012/08/passwords-under-assault/

Henry, A. (2012). How to build a (nearly) hack-proof password system with LastPass and a thumb drive, *Lifehacker*. Retrieved October 24, 2012 from http://lifehacker.com/5879117/how-to-build-a-nearly-hack+proof-password-system-with-lastpass-and-a-thumb-drive

Honan, M. (2012). How Apple and Amazon security flaws led to my epic hacking. *Wired*. Retrieved October 24, 2012 from http://www.wired.com/gadgetlab/2012/08/apple-amazon-mat-honan-hacking/

Mediati, N. (2012). Free antivirus you can trust. *PC World*. Retrieved October 24, 2012 from https://www.pcworld.com/article/254121/free_antivirus_you_can_trust.html

NoReplyAll Outlook Add-In. (n.d.) Retrieved October 24, 2012 from https://research.microsoft.com/en-us/projects/researchdesktop/noreplyall.aspx

Rubenking, N.J. (2012). How to spy on people. *PC Magazine*. Retrieved October 24, 2012 from http://www.pcmag.com/article2/0,2817,2402527,00.asp

SANS (n.d.). SANS password policy. Retrieved October 24, 2012 from https://www.sans.org/security-resources/policies/Password_Policy.pdf

Verry, T. (2012) Are FPGAs the future of password cracking and supercomputing? Retrieved October 24, 2012 from http://www.extremetech.com/computing/133110-are-fpgas-the-future-of-password-cracking-andsupercomputing

APPENDIX

Figure 1
Steps to improve security throughout the life cycle of company data

Data Creation
● Periodically evaluate the placement of computer monitors to protect against "shoulder surfing." ● Run up-to-date anti-virus and anti-spyware programs continually. ● Promptly install all vendor-provided security updates to operating systems and applications. ● Examine all computers on a periodic basis for hardware keystroke loggers.
Data Storage
● Prohibit the storage of company data on employee personal devices or cloud storage accounts. ● Prohibit the use of personal programs and the storage of personal data on company devices. ● Require the consistent use of computer-generated, rather than self-selected, passwords. ● Require the consistent use of two-factor authentication to access computer resources.
Data Transmission
● Prohibit the use of the "Reply All" command when responding to email. ● Require encryption of all confidential email messages and email attachments. ● Require the use of a Virtual Private Network (VPN) when accessing the company network. ● Require that all access to company cloud storage accounts be conducted over SSL connections. ● Require that all data be encrypted before sending it to company cloud storage accounts. ● Require that the encryption key for data sent to company cloud storage accounts remain in the sole possession of the company and not be disclosed to the cloud storage site.
Data Destruction
● Require the secure destruction of confidential data on digital storage media before disposal. ● Require the secure destruction of confidential data passively stored on computers, photocopiers, multi-purpose printers, and fax machines before retirement.