Enterprise Desktop Management Security Strategy

Liz Cummings

July 16, 2014

Table of Contents

***Abstract*—** Information Security is currently a hot topic, with the recent data breaches of reputable companies. Cybercrime is widespread and the landscape has changed drastically. Businesses can't protect assets, as they need five years ago. In the past, businesses were concerned with securing a desktop pc, servers, and the network architecture. Today, however, company data is accessed from desktops, laptops, servers, mobile devices, virtual machines, wirelessly, the cloud, and personal technologies. As employers seek to find more productive and cost efficient avenues to do businesses, they will need to develop an all-encompassing approach to secure company data. It is important to understand the threats and vulnerabilities that impact information security. Some of the risks include theft, vulnerabilities in unpatched applications and operating systems, malware, identity theft, loss of data and intellectual property. A multifaceted approach is key to securing enterprise systems that safeguarding data against this array of threats. The purpose of this research is to develop an enterprise desktop security strategy to protect and secure data. This research will provide a strategic approach for securing desktops, laptops and other devices and pinpointing alternatives to increase security. Security breaches have the most substantial impact on a business resulting in monetary loss, privacy, and damage to the corporate reputation. This research paper will develop a strategy that includes desktop security best practices, virtualization, zero and/or thin clients, management tools, user training and policies and procedures. It is the responsibility of the business to ensure confidentiality, reliability and performance. The outcomes of this security strategy will offer businesses a resource to better identify the associated threats and a strategy to diminish and/or eliminate those risks.

Introduction

Information Security is a topic that is on everyone's mind with the recent data breaches of reputable companies. Cybercrime is widespread and the landscape has changed drastically. Businesses can't protect assets, as they need five years ago. In the past, businesses were concerned with the physical access of computer technology, along with the perimeter access of the network architecture. Today, however, company data is accessed from desktops, laptops, servers, mobile devices, virtual machines, wirelessly, the cloud, and personal technologies. As businesses seek to find more productive and cost efficient avenues to do businesses, they will need to develop an all-encompassing approach to secure company data. It is important to understand the threats and vulnerabilities that impact information security. Some of the risks include theft, vulnerabilities in unpatched applications and operating systems, malware, identity theft, loss of data and intellectual property. A multifaceted approach is key to securing enterprise systems that safeguarding data against this array of threats. The purpose of this research is to develop an enterprise desktop security strategy to protect and secure data. This research will provide a strategic approach for securing desktops, laptops and other devices and pinpointing alternatives to increase security. Security breaches have the most substantial impact on a business resulting in monetary loss, privacy, and damage to the corporate reputation. This research paper will develop a strategy that includes desktop security best practices, virtualization, zero and/or thin clients, management tools, user training, and policies and procedures. It is the responsibility of the business to ensure confidentiality, reliability and performance. The outcomes of this security strategy will offer businesses a resource to better identify the associated threats and a strategy to diminish and/or eliminate those risks.

Threat to Information Security

There is much vulnerability innate in computer technologies. These vulnerabilities are common among all platforms. The 2014 Internet Security Threat Report reported that there was a 91% increase in targeted attacks campaigns in 2013 and that 1 in 392 emails contained a phishing attack (Symantec, 2014). Based upon these statistics, as well as

others, it is evident that the need to take action to protect company assets is of direr importance. Information security can be summed up by the following quote (*Ahmad et al., 2012)

> "An information security incident occurs when there is a direct or indirect attack on the confidentiality, integrity, and availability of an information asset. Such incidents can include attacks such as malicious software, theft of information, the loss of power and supporting utilities and information leakage. It is inevitable at some stage that organisations will suffer an information security incident. Such an incident may result in multiple negative impacts, such as loss of company reputation and customer confidence, legal issues, a loss of productivity and direct financial loss."

It is the responsibility of the business to prevent or minimize the damage that such an incident can impose. When identifying these threats, all areas must be taken into consideration. Information security encompasses many areas such as desktop, server and network infrastructure security, virtualization, cloud infrastructure and user interaction. When identifying information security risks, Webb indicated that businesses must

> "(1) identify security risks (risk identification), (2) prioritize them according to severity (risk assessment), (3) determine the most cost-effective means of controlling security risk (e.g. avoidance, mitigation, transfer or risk) (risk treatment) and (4) monitor changes to the risk management system (risk review) (*Webb et al., 2014)."

Businesses must be proactive in their approach to preventing and/or minimizing information security incidents. Though, no one course of action will totally eliminate all risk. Businesses can be better prepared to tackle these issues head on with properly planning. This report will identify a multipronged approach in protecting company data.

Information Security Strategy

Information security is an integral component of a business's strategy. As more advancement in technology is reached, the risks become more evident and the necessity to take action becomes clearer. Businesses need to take ownership and responsibility for the new demands to protect valued company assets as the magnitude of breached and

identity theft becomes more ostensible. It is important to know what to look for to avoid risk. CNBC reported the following list of 10 ways that companies get hacked (Fox, 2012).

1. Email Social Engineering/Spear Phishing
2. Infection Via a Drive-By Web Download
3. USB Key Malware
4. Scanning Networks for Vulnerabilities and Exploitment
5. Guessing or Social Engineering Passwords
6. WiFi Compromises
7. Stolen Credentials from Third-Party Sites
8. Compromising Web-Based Databases
9. Exploiting Password Reset Services to Hijack Accounts
10. Insiders

Strategy is a key component in mitigating these risks. To effectively create a great strategy, a business must understand the threats and risks that are characteristic in their business. Once these threats and risks are identified, it is important to prioritize them based upon the threat to the organization. Wurzler documented the following risks and threats that a business can be exposed to (*Wurzler, 2013, p. 6)

1. Unauthorized access — generally, and for this purpose, an external threat.
2. Theft of non-public or private information.
3. Insider theft — to which the subject often has authorized access.
4. IT costs to remediate systems.
5. Business income loss.
6. Regulatory — Security Breach Notification.
7. Reputational injury.
8. Stock price impact.
9. Legal – shareholder lawsuits

Although this list does not include every potential situation, it provides a solid foundation to create a desktop management security strategy. The strategy can outline how each threat is prioritized, since it will vary based upon the type of business. In building a desktop management security strategy, this research paper will focus on desktop security

best practices, virtualization, zero and/or thin clients, management tools, user training and policies and procedures. The goal of this research is to aid businesses in protecting and securing corporate files and documents. This study will identify the threats and recommend best practices to lead businesses in creating a solid strategic plan to assist in eliminating security risks.

Desktop Security Best Practices

A primary concern for a business is the computers that generate, store, and disseminate corporate data. To ensure that these assets are protected, measures and safeguards must be put into place to diminish or avert risk. The computer operating system (OS), regardless of platform, Windows, Mac, Linux, or Unix, are vulnerable if precautions are not taken to secure the device. This report will identify best practices for securing the operating system. Therefore, curtailing the risks associated of office computers. The City of New York identified the following steps to secure an operating system (CCNY, 2013).

1. Keep operating system patches up to date
2. Use encryption to securely encode sensitive information
3. Install antivirus software; configure for daily updates
4. Install and configure a personal firewall
5. Keep application and software patches up to date (e.g., Microsoft Office, browsers, etc.)
6. Follow best practices when opening email attachments
7. Follow secure password policies
8. Follow best practices for user account security
9. Eliminate unnecessary network services, applications, and processes
10. Avoid peer-to-peer file sharing
11. Install and configure anti-Spyware programs
12. Configure system restore points to protect your current configuration
13. Perform regularly scheduled backups to protect data
14. Turn off computer when not in use; restrict physical access to computer

Other best practices include securing Wi-Fi, and Bluetooth features. Unmanaged devices are a prime target for attacks. Another measure is the hardening of Adobe Reader. By turning on the enhanced security in Adobe Reader, computers are protected from the hidden attacks in PDF files (Symantec, 2014). It is also recommended to disable local administrative and guest accounts on computers. This can be managed via Group Policy, which will be discussed in a later section. Computers should also be configured to lock after a predefined amount of time with a "screensaver/screenlock that requires a password (The University of New Mexico, 2014)" to regain access. Best practices pinpoint strategies that embody the most efficient or practical course of action. Understanding these benefits can assist a business in making better more informed decisions to protect assets.

Virtualization

An Enterprise Desktop Management Security Strategy should also include virtualization. "Virtualization is a combination of software and hardware engineering that creates Virtual Machines (VMs) - an abstraction of the computer hardware that allows a single machine to act as if it where many machines (Burger, 2012)." Virtualization provides many benefits. Using a virtual desktop infrastructure (VDI) allows businesses to use server hardware to run desktop operating systems and application software inside a virtual machine (Harbaugh, 2012). VDI's can be accessed through existing computers. This eliminates the need to upgrade workstation hardware, and allows the business the ability to offer multiple operating system environments. Virtualization provides server and desktop benefits. Server virtualization benefits for a business include the ability to consolidate servers, eliminate server sprawl, flexibility to do more with less, cost savings, ability to move running virtual machines to other hosts, increased uptime, image-based backup and restore capabilities, virtual labs, simplified disaster recovery, and an option to move to the cloud (Evans, 2011). Desktop virtualization benefits include, every desktop user can utilize the same image, processing moves from individual workstations to a VDI server, hardware costs can be more easily managed, since almost everything will reside in the data center, maintaining a single OS image can reduce management and support costs, and when problems are encountered problems, generally there is only one system

to troubleshoot (Harbaugh, 2012). As with all technologies, there are associated risks with every benefit. There are measures to ensure optimum performance and security of virtual desktops. Kamity, recommends the following 10 best practices to secure virtual desktops (Kamity, 2011).

1. Update Security Policies
2. Virtual Desktop Hardening
3. Virtual Desktop Access Control
4. Business Continuity
5. Remote Access Security
6. Isolation Control
7. Host Security Scanning
8. Host Operating System Check
9. Network Security & Segmentation

Virtualization is a viable tool to secure access to corporate data. Below is a list of additional security benefits when implementing virtualization (*Komperda, 2012):

1. Centralized storage prevents loss of data if a device is lost, stolen or compromised.
2. Attacks are isolated since virtual machines contain only one application on one OS.
3. Flexibility in that it allows the sharing of systems without necessarily having to share critical information across the systems.
4. Infected VM's can be rolled back to a prior "secure" state
5. Reduced need for hardware improves physical security
6. Desktop virtualization provides better control of the OS to ensure that it meets organizational requirements as well as security policies.
7. Data Protection & Encryption

Zero/Thin Clients

Zero or thin clients are another option that provides businesses with improved security and reduced support cost. Thin clients restrict access to specific computers, provides secure storage of files, and critical applications are stored on a server (Educause, 2005). Thin clients must have an OS, CPU, flash memory, and local storage. On noted feature of a zero or thin client is that data is not stored on the local device. If stolen, the device is rendered useless. Zero clients do not have an OS, CPU, flash memory, or local storage. They operate from a chip. Table 1 shows the security features and benefits of a zero client (VMware Horizon, 2014).

Table 1: Security Features and Benefits of a Zero Client (VMware Horizon, 2014)

SECURITY FEATURE	SECURITY BENEFIT
No operating system	No viruses or spyware, no patches, no maintenance
No persistent user data	No local storage to lock down
No application data sent over network	Only fully AES-encrypted pixels are sent over the network
SIPR hardware token support	Supports secure SIPR authentication mandated by DoD
Ability to disable USB device access	Full control over USB devices
802.1X network authentication	Allows network devices to be authenticated before use
Fiber support (100BASE-FX)	Fiber option to further secure endpoints on network

Zero and Thin clients provide an alternative to the traditional desktop computer and provide added valued based upon these security features. Table 2 shows the security features and benefits of a thin client (Tanwongsval, 2002).

Table 2: Security Features and Benefits of a Thin Client (Tanwongsval, 2002)

Security	• System administrator can centrally control, install, and update the necessary applications. This eliminates incompatibility or vulnerability issues that arise from users installing different software versions or forget to install a critical patch. • Since most thin -client terminals do not contain a hard drive, critical data is protected from theft or file corruption.
Financial Benefits	• Thin-client terminals have very few components therefore require less energy than conventional PCs. • Users will spend less time administering their workstation and concentrate more on their job. • Under normal circumstances, only the server's hardware or needs to be upgraded while the terminals can still be used.
Network Connectivity	• Conventional PCs and laptops require the user to download emails, attachments, and files (e.g. spreadsheet, word processor, slides, and etc.) before they are able to work on them. Downloading takes up local and corporate system and network resources. Furthermore, once the files are modified, they might need to be resent back to the server, requiring even more network and system resources. Thin-client allows remote users to work on the files without downloading the files, as everything is centrally stored on the server.
Fault Tolerant	• A thin-client terminal can easily be replaced without compromising user's data, because it is centrally stored. • Important data can easily be backed up and restored if needed.

Administrative Tools

There are numerous management tools that are available to assist businesses in securing technology. Of particular interest in this research paper, the following tools will be discussed: GPO's, ViewFinity. Group Policy is a Microsoft tool that allows an administrator to manage detailed configurations for users and computers. GPO's can be used to secure many things. Browsers configurations, options to grey out save passwords and prohibiting access to the control, just to name a few. Many software applications have been poorly written, requiring that the end user have administrative privileges for the software to run correctly. But, with administrative privileges come elevated risk for viruses and malware. Viewfinity has indicated that 53% of security incidents come from employees (Viewfinity, 2014). Removing administrative rights from users could reduce these incidents greatly. Viewfinity is a privilege management and application control solutions. The software is installed on the local machine and provides granular controls and allows administrators the ability to whitelist and elevates permissions on software applications, thus, providing the user with the tools necessary to do their jobs, without jeopardizing the entire network. Other tools that are essential to managing desktop computers include a patch management server, Windows Server Update Services (WSUS) (Microsoft, 2014), a Windows based management server, System Center Configuration Manager (SCCM) (Microsoft, 2014), and a Mac based management server, Centrify (Centrify, 2014). The above mentioned management tools are listed as examples only, and do not indicate that they are superior to any other product.

User Education

Information security is not just an IT issue, it affects everyone. Businesses must accept the challenge to create awareness of the probable risk associated with information security. User education is important to help user's understand the implications of their actions. User education should include training sessions, an informative website with security tips and best practices, communication based upon the Kiss principle, Keep it simple, stupid. Give the user the relevant information, but don't overload them with too much. Since, research indicated that most malware attacks use social engineering, users should practice the following (Symantec, 2014):

1. Only click through to trusted sources when conducting searches, especially on topics with high attention
2. Never update "media player," “codec," or “Flash” when promoted by a site hosting videos or not affiliated with that application
3. Do not use P2P applications on business machines and be cautious on home machines as well
4. Do not click on links or attachments in spam email

Policies and Procedures

Policies and procedures should clearly define the overall approach that a business takes on information security. It should also define how data is classified, processed and transmitted. Policies should also clearly state the consequences for violations. Policies and procedures also communicate to users that upper management takes these issues seriously. Businesses must work to craft standards to ensure a securer and productive environment. In every environment a situation arises that necessitates a user needing administrative rights on their computer. In these incidents proper documentation is a must. There should be documentation identifying the specific need and all necessary approvals. It is recommended that a formal document be drafted requesting such access, i.e. Administrative Access Application form. It is also recommended that a course be created and a test administrated to confirm that the user fully understands the implications of having administrative rights on a computer. After successful completion of the test, the access should be reviewed annually to determine (1) if the need still exists, (2) violations warranting the need to revoke permissions. Service level agreements (SLA’s) should also be established that document the terms of the agreement. For example, a professor who has a documented need for administrative rights, due to poorly written software. The SLA could indicate that technical support will be limited to 30 minutes, if issue cannot be resolved within that time period, a clean image will be applied to the computer.

Summary

It is a necessity that businesses implement best practices and strategies that will safeguard information security. As businesses pursue more productive and cost efficient avenues to do business, they will need to develop an all-encompassing approach to secure company data. Businesses must understand the threats and vulnerabilities that impact information security. Those risks include theft, vulnerabilities in unpatched applications and operating systems, malware, identity theft, loss of data and intellectual property. The recommended approach to securing enterprise systems is to develop an enterprise desktop security strategy to protect and secure data. The enterprise strategy will include implementing desktop security best practices, virtualization, zero and/or thin clients, management tools, user training, and defining policies and procedures. In identifying an enterprise strategy the business must identify the need that needs to be addressed, investigate the options to resolve the need, develop and plan to strategy to implement, get the proper approval and necessary resources, execute the plan, and review the plan to make necessary adjustments. Information security practices are critical to business success.

References

*Ahmad et al., A. A. (2012). Incident response teams - challenges in supporting the organisational security function. *Computer Security*, 643-652.

*Komperda, T. (2012, December 17). *InfoSec institute.* Retrieved July 21, 2014, from Virtualization Security: http://resources.infosecinstitute.com/virtualization-security-2/

*Webb et al., J. W. (2014). A situation awareness model for information security risk management. *Computers & Security*, 1 - 15.

*Wurzler, J. (2013, April 23). *Information Risks & Risk Management.* Retrieved July 21, 2014, from SANS Institute InfoSec Reading Room: http://www.sans.org/reading-room/whitepapers/bestprac/information-risks-risk-management-34210

Burger, T. (2012, March 5). *Intel Devloper Zone.* Retrieved July 21, 2014, from The Advantages of Using Virtualization Technology in the Enterprise: https://software.intel.com/en-us/articles/the-advantages-of-using-virtualization-technology-in-the-enterprise

CCNY. (2013, June). *The City College of New York Office of Information Technology.* Retrieved July 21, 2014, from Desktop Security and Best Practices: http://www.ccny.cuny.edu/it/upload/Desktop-Security-Best-Practices.pdf

Centrify. (2014). *Centrify*. Retrieved July 22, 2014, from Centrify: http://www.centrify.com/

Educause. (2005, December). *Educuase Library.* Retrieved July 21, 2014, from What are Thin Clients: http://net.educause.edu/ir/library/pdf/DEC0005.pdf

Evans, D. (2011, April). *The Internet of Things, How the Next Evolution of the Internet is Changing Everything.* Retrieved November 11, 2013, from Cisco: http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

Fox, M. (2012, July 6). *CNBC.* Retrieved July 21, 2014, from 10 Ways Companies Get Hacked: http://www.cnbc.com/id/48087514/page/1

Harbaugh, L. (2012, March 22). *PCWorld Tech Audit*. Retrieved July 21, 2014, from The Pros and Cons of Using Virtual Desktop Infrastructure: http://www.pcworld.com/article/252314/the_pros_and_cons_of_using_virtual_desktop_infrastructure.html

Kamity, K. (2011, February 11). *Virtual Strategy Magazine.* Retrieved July 21, 2014, from Desktop Virtualization: Top 10 Security and Compliance Best Practices: http://www.virtual-strategy.com/2011/02/11/desktop-virtualization-top-10-security-and-compliance-best-practices

Microsoft. (2014). *Server and Cloud Platform*. Retrieved July 22, 2014, from System Center 2012 R2 Configuration Manager: http://www.microsoft.com/en-us/server-cloud/products/system-center-2012-r2-configuration-manager/default.aspx?nv1if0=1

Microsoft. (2014). *Windows Server*. Retrieved July 22, 2014, from Windows Server Update Services: http://technet.microsoft.com/en-us/windowsserver/bb332157.aspx

Symantec. (2014). *Symantec Security Response Publications Annual Threat Report*. Retrieved July 20, 2014, from 2014 Internet Security Threat Report, Volume 19: http://www.symantec.com/security_response/publications/threatreport.jsp

Tanwongsval, S. (2002, April 5). *SANS Institute*. Retrieved July 22, 2014, from Sun Ray Thin-Client and Smart Cards: An Old: http://www.sans.org/reading-room/whitepapers/terminal/sun-ray-thin-client-smart-cards-concept-muscle-320

The University of New Mexico. (2014). *UNM Information Technologies.* Retrieved July 21, 2014, from Workstation & Data Security: http://it.unm.edu/security/best-practices/index.html

Viewfinity. (2014). *Viewfinity*. Retrieved July 21, 2014, from Viewfinity: http://www.viewfinity.com/#

VMware Horizon. (2014). *White Paper.* Retrieved July 21, 2014, from Key Considerations in Choosing a Zero Client Environment for View Virtual Desktops in VMware Horizon: http://www.vmware.com/files/pdf/view/vmware-top-five-considerations-for-choosing-a-zero-client-environment-techwp.pdf