Standardizing Security Processes to Minimize Mobile Threats

Five essential aspects of protecting corporate networks, information, and infrastructure

1 Mobile Threats, Past & Future

Researchers measured **a nearly 600% increase in the use of malicious web sites** year over year. **Legitimate web hosts** were home to **85% of those sites.**

51% of Ponemon survey respondents said their organization has **experienced a data breach** due to insecure devices. **Another 23%** said they **weren't really sure** whether they have or not.

Of young consumers surveyed, **91% say that the age of privacy is over** and believe they can't control the privacy of their information, with **one third of respondents** reporting they **are not worried about the data that is captured** and stored about them.

The Ponemon Institute conducted a survey of 4,640 organizations, in which **a whopping 77% of respondents** said that the **use of mobile devices in the workplace is important** to achieving business objectives. But a nearly equal portion of survey-takers – **76% – believes that these tools present a "serious" set of risks.**

The number of variants of malicious software aimed at mobile devices **has risen from about 14,000 to 40,000** in less than a year, **an increase of about 185%,** according to the GAO.

In an age where information is everything, most people seem to lack information about IT security. The best way to combat these issues is to constantly update employees on the importance of security and potential threats, while upholding the highest standard of security on devices.

Mobile devices face a growing number of challenges in the wake of a sea change in the nature and type of threats targeting the devices and the organizations they connect to.

The 1990s and early 2000s saw relatively unsophisticated forms of malware and attacks, propagated by perpetrators with limited resources. Today, **well-financed organizations** with access to upgraded threat technology **are behind the exploits,** creating much more risk.

New technology also means new entryways for viruses and malware. Using **fake apps, app stores, and wireless networks,** hackers can all too easily steal personal information. Particularly troubling are **Advanced Persistent Threats,** where hackers repeatedly target key employees in order to steal their credentials and gain entry into sensitive corporate systems.

The theft of an end user's personal information can quite often cause irreparable damage. But that's nothing compared to what can happen if critical or private business information is stolen, which is the focus of many threats and exploits targeted at the enterprise. **The goal is to capture valuable information** such as social security and bank account numbers, health records and information from corporate accounting systems.

Fake apps, among the newest threats to the enterprise, have become an overnight phenomenon, and a dangerous one. Users can easily make the mistake of downloading a free fake app and inadvertently share vital personal information. **With everything a fingertip away, smartphones and tablets are an especially easy target.** Fake apps may also be the linchpin of an enterprise-focused attack, such as with the fake anti-virus malware variants popping up across all classes of devices. Some apps hold the device hostage for ransom, while others have a goal of deeper penetration.

> Spyware and malware will constantly morph as long as there is an opportunity for hackers to profit. And because many hacker groups are now affiliated with substantial funding sources, the rate of "improvement" in malware will continue.

In addition to fake apps, **another new threat category is fake app stores.** With user interfaces that look authentic, it is easy for consumers to be duped by these stores. Even if the fake store has a different look from what visitors are used to, they may simply assume the store has been updated, a common occurrence with ever-changing technology.

Another emerging threat type involves **fake wireless networks,** typically found in public areas. Much like fake apps and app stores, they look realistic and are designed to trick users into connecting to what looks like a legitimate hot spot but is actually a hacker's own system. There are also new threats that are focused on attacking via Bluetooth on mobile devices.

Defending against these new threats requires IT to update security processes, and use virtualization or secure cloud access tools to protect corporate data and applications. Companies should also be mindful about outfitting any new or upgraded laptops and tablets with the most modern security tools, to protect both their users and corporate information.

Some older laptops and first-generation tablets are more vulnerable than today's models, which generally have more secure operating systems and improved tools like Mobile Device Management (MDM). It may well prove too costly to retrofit older devices with these latest tools.

Educate your employees about the specific mobile threats they will encounter and how to best protect themselves. In the ever-changing global technology landscape, **new threats will always emerge and preparation is the best protection.**

2 The Risk of Insecure Mobility

Mobile threats increased 35% from Q3 2012 to Q4 2012.

32% of malicious links in social media used shortened URLs to disguise the threat and trick more users to click on the link.

Outdated versions of Android create **potential security vulnerabilities for 400 million users.**

65% of mobile devices do not have an Internet security solution installed.

32% of all mobile threats and malware are designed to steal information both from the compromised device and potentially from other systems to which it is connected.

One of the most basic protections for any organization is to own and operate the wired and wireless networks at its locations, where security risks are far lower. As soon as users go mobile, the risks of users falling victim to security threats jumps dramatically.

Now on top of all the issues that mobility brings, **we are adding another security wrinkle: Bring Your Own Device (BYOD),** where end users connect their personal devices to the corporate network, often over unsecured access points.

> Many of the previous generation of mobile devices, and even some current ones, do not have data encryption to protect corporate or private information that may reside on a lost or stolen device.

The BYOD trend is exploding, bringing with it new risks. To protect itself, **the organization must develop an effective, comprehensive plan** to secure information assets and IT infrastructure, while implementing new products and solutions to help derail threats to mobile users. The rate of change in the threat landscape is so rapid that plans just 12 months old may no longer afford the protection they did upon deployment.

An important starting point is to **assess all the mobile devices your organization uses,** keeping in mind that older devices are the most vulnerable. Starting with laptops, many aspects of newer systems improve security. It is important to note that **it is now impossible to properly secure any Windows XP-based laptop.** In addition to being inherently less secure than Windows 7 or Windows 8, Windows XP is coming to end of life in 2014, meaning it will no longer receive monthly security patches. Essentially, that will mean a field day for hackers targeting Windows XP systems.

Many older laptops also lack strong disk encryption. Rather than the native disk encryption present on newer laptops, older models rely on software solutions that, because they often compromise performance, users frequently disable.

One of the newest mobile devices to make its way to the enterprise is the tablet. Even though many are less than three years old, they still represent a large entryway for malware and intrusions. To start, substantial differences exist in the security capabilities of the various tablet operating

systems. For example, Windows 8 is designed to be the kind of secure and manageable platform that enterprises require. And while the Android environment is improving, older versions of the operating system on tablets have well-known security holes. With the rate of change in tablets, **staying current with devices that have enterprise-class security is essential.**

Many IT professionals report that end users are becoming more willing to work with them to secure mobile devices as they realize that their personal information is also at risk.

The stakes are high because liability is now intertwined with mobile computing. Consider:

- **More states are implementing statutes and legislation** that set substantial penalties for organizations that have a data breach where personal information is exposed.
- **The BYOD phenomenon** is creating a huge expansion in the number of mobile devices with access to corporate data.
- **The broad range of mobile devices** in use makes it difficult to implement a consistent level of security to reduce liability.

To deal with these issues, IT organizations need to develop and deploy an updated and more comprehensive “Acceptable Use Policy” for their organization to minimize any security breaches based on end user mistakes or ignorance. Many existing policies do not cover current usage patterns well, including the use of tablets and smartphones with all sorts of personal apps. **Failure to update policies may well leave both personal and corporate data vulnerable.**

3 The Role of the User in Mobility Security

Human error is the second leading cause of all data breaches, causing **35% of the total,** just behind malicious attacks at 37%.

65% of the economic loss from a data breach **is due to human error.**

In a recent survey, **55% of respondents said, "employee mistakes, incompetence or negligence combined presented the greatest contributing factor to digital breaches ."**

Microsoft conducted a study that says **57% of end users download personal or non-business software** on business-provided PCs .

The Verizon Data Breach Investigation Report stated **66% of the breaches examined took months or more to discover.**

A chain is only as strong as its weakest link, as the saying goes. When it comes to IT security, in many cases **end users are that weak link** and serve as the entry point for viruses, malware and breaches. Chief Security Officers (CSOs) often say one of their most important tasks is to provide guidance, training and policies that help end users understand and avoid security threats.

This used to be a fairly simple issue because most employees used laptops provided by their employer that were loaded with security tools and managed by IT. Today, **employees are far more mobile** and, given the BYOD phenomenon, they are **using their own laptops, tablets and smartphones** – often all three. Clearly the security problem is becoming more complex and widespread.

As a result, there is a compelling need to update end user security policies and processes. This chapter will consider some of the most important elements of end user-focused security.

> Organizations need to update Acceptable Usage Policies (AUPs) to cover personal devices and to include information on how employees may use and transfer corporate data. Without clear guidelines, end users may put critical corporate data at risk by employing file-sharing sites, unsecured networks or simply by sharing it too broadly.

USER SECURITY TRAINING

The first issue to consider is **the role of training and policies** in helping end users understand security threats and comply with basic security best practices.

The good news is the vast majority of employees and end users are receptive to training. They want to be a partner in IT security and act in a mature, responsible fashion. But knowledge levels about safe computing vary widely, so it is important to start with the basics.

Begin with education about phishing scams, drive-by downloads, compromised sites and how basic security tools provide protection for both personal and corporate data. Also cover safe practices, such as never using a USB flash drive that you aren't absolutely sure is safe. Microsoft's TechNet has a good tutorial on this topic. Of course you'll have to tweak the advice to cover any unique aspects specific to your organization. Use of newer laptops

and tablets may help to reinforce key aspects of your security training because they can be configured to disallow use of USB ports for storage and file swapping, for example.

One of the most important elements of a security training program is **educating users on how to protect corporate data** and ensure it is not replicated to unsecured environments. Of primary concern here are file-sharing solutions such as Box, Google Drive, Dropbox and the like.

Providing end users with collaboration and social media tools through a corporate agreement, and with some management tools, will help IT limit the impact of rogue applications and provide greater control over corporate data.

These tools present two common problems. First, they involve users moving sensitive data out from under corporate control and security protection. Second, few users bother to remove the data once they no longer need it, meaning potentially sensitive data is sitting in an unsecured state for months or longer. A solution such as Office 365, which has a managed service for file sharing, is a better alternative.

Every organization should have an Acceptable Usage Policy (AUP) that lays out what is considered acceptable use of corporate IT resources, and what activities, services and applications are not allowed. It is important to make clear that the AUP applies no matter what device a user is employing, even if it is their own. Some end users think if they own their own device, anything goes. Make sure they understand that, so long as they are accessing a corporate network, that is not the case.

The AUP should also detail the consequences for non-compliance with corporate security policies, up to and including termination. But do not make that the focus on the document; remember, you are trying to foster a partnership approach.

The AUP should also be a living document, so make changes as needed. And remind employees about the AUP by having them sign it each year, rather than once when they are first hired.

4 The Role of Virtualization

Each major virtualization supplier claims about **1.5 million VDI licenses deployed** for a total of **approximately 1%** of the total PC client market .

The virtual client computing market will grow to **$3 billion in 2015** with **one-third of that coming from centralized virtual desktops** or VDI, and the remaining **two-thirds from other virtualized client solutions.**

North American and European IT decision makers are citing new and different reasons for adopting virtualization.

The ability to support remote employees has become the primary reason for virtualizing, with **53%** of respondents citing this factor in 2013. Respondents report **slightly less interest in manageability issues and cost savings,** which each come in at **48%.** Clearly, employee flexibility has become a key driver.

VDI adoption will continue to increase at a steady rate for three to five years.

27% of surveyed IT departments planned to implement client virtualization in the next 12 months.

25%

Almost one quarter of all businesses have some implementation of virtual desktop solutions.

Most enterprise IT groups have been unable to discern ways to use virtualization to increase security in a cost-beneficial manner.

Virtualization is a key technology in terms of improving IT efficiency, but it also provides an important way to improve security in a mobile environment. **What is virtualization?**

- **A computing environment that exists in software,** not necessarily tied to a specific set of hardware.
- **Promotes greater utilization of servers** by enabling a single physical server to host multiple "virtual" servers.
- **Available via new technologies** to drive solutions anywhere on almost any device.

The security benefits of virtualization are tied to the first bullet point. Simply put, in a mobile environment the end device – whether a laptop, tablet or smartphone - is effectively a "terminal" that is allowed access to applications and data that remain on the server. **No information or applications reside on the mobile device,** so if it is ever lost or stolen, it houses no data that can be compromised.

Data security and virtualization have become inseparable in worldwide IT departments for four reasons, as follows:

1. **Providing improved physical protection of data and applications.** Use of virtualization allows central control and management of all data, ensuring the consistent application of strong security policies. IT can tightly control physical access to data storage, unlike data stored on mobile, handheld devices and PCs.

2. **Delivering layered protection for corporate data.** Strong and consistent security layers protect data stored centrally via virtualization within the data center. These layers normally include strong access controls, secure data communications, and

mechanisms to prevent and detect unauthorized data access. Many virtualization installations use encryption on server storage systems for additional protection.

3. **Virtualization provides a consistent, up-to-date operating environment.** Virtual desktop technology enables IT to stream or download a desktop image from a central server. That means IT only has to update the server with the latest operating system patches and security updates, rather than each individual remote device – a far easier, more reliable proposition.

4. **Virtualization reduces the target profile.** An enterprise with data in many locations on many devices, managed and unmanaged, presents a wide target to hackers. By keeping data in a central location, virtualization solutions reduce the organization's target profile.

Cloud computing has obvious strengths in accessibility and productivity. But traditional VDI solutions are unable to support newer devices connected at lower speeds that use non-standard video and keyboard configurations.

The most common way to use desktop virtualization involves Virtual Desktop Infrastructure, or VDI. VDI has several variants, but the most common is to create a virtual PC on a central server for each user. Users then tap in to the server to display their desktop or the image is streamed to their device. Either way, all data and applications remain on the server.

Security with VDI is excellent but **the technology suffers from some noteworthy issues.** For one, it takes expensive, high-powered servers to support VDI, making it challenging to come up with a workable ROI equation. Network performance must be excellent or response time will be subpar, and users will be unhappy. On-screen graphics quality will likely be inferior to a PC with a good graphics card and won't approach that of most tablets. Lastly, VDI typically does not support access from smartphones and tablets, or at least not fully.

Increased regulatory pressures including privacy laws in Europe and most U.S. states create a large financial incentive to protect critical enterprise data on all devices.

Lenovo's Stoneware division (www.stone-ware.com) has a simpler and better approach. Stoneware's webNetwork creates a virtual desktop for each user in a secure web browser. Any application or third-party web service can be presented to users in the browser. The result is webNetwork can support more users with fewer servers as compared to other VDI solutions, resulting in big cost savings with better performance over WANs and other networks.

webNetwork also enables devices to use local PC graphics hardware to improve the experience. Access from phones and tablets is easy and works well, giving users all the security advantages of virtualization without the usual complexity and cost.

Many companies are searching for ways to implement virtualization and cloud technologies. **Stoneware provides the ability to move vital company applications to the cloud at an extremely low cost,** and makes those applications available to employees on any device that supports a web browser. Users can also securely incorporate web applications hosted by third-party providers into the virtual desktop.

The result is a solution that includes strong central control and security, easy inclusion of third-party web applications, unequaled accessibility, and the lowest possible cost, all available from Lenovo.

5 Building a Simpler Security Process for IT

35% of users do not have a password
in use on their smartphone or mobile device.

By 2014,
the number of employees who bring their own mobile device to work will more than double
as compared to 2012, **to 350 million.**

With a score of **7.1 out of 10,**
respondents to Symantec's **State of the Data Center Survey** rated
security as the most complex issue
they have to deal with, **more so than infrastructure, disaster recovery, storage and compliance.**

35% of companies do not encrypt data
on mobile devices.

By 2016,
65% of organizations will implement an MDM solution, either cloud-based or on-site.

Clearly the challenge for enterprises is to provide more security solutions with greater capabilities, without overwhelming IT staff and the corresponding budget. **This is a classic case of doing more with less.**

One of the most effective ways to meet the challenge is to **substantially simplify the security framework** such that IT requires fewer resources to provide the required level of security. Several approaches to simplifying security make sense.

The cost of complexity for mobile security can be substantial. A large part of the problem is that once a complex solution is in place, it is hard to replace it with a simpler solution.

Another successful tactic is to **cut the number of suppliers of mobile devices,** such as laptops, so IT has fewer permutations to evaluate for effective security.

Lenovo also provides a number of capabilities as part of its standard enterprise product offering to help simplify security implementations, including disk encryption, password management, patch management and virtualization solutions. **Standardizing on a single-vendor solution,** especially fully-featured ones like those Lenovo offers, **can yield substantial savings in IT resources.**

The second method of simplification to evaluate is the use of Mobile Device Management (MDM) software. **MDM tools provide a platform for securely monitoring, managing and supporting mobile devices.** The tools give IT control over access to data as well as configuration settings for all mobile devices connected to the network, helping to reduce support costs and security risks.

MDM software can work with corporate-provided as well as employee-owned devices. One caveat: **not all MDM software will continue to work with Windows XP after that operating system's end of life,** which is set for April 8, 2014. MDM vendors have yet to make clear and definitive statements regarding support for Windows XP after that date.

Mobile Device Management (MDM) solutions can help provide a standard layer of control and management across numerous device types to ensure that the correct security tools are in place and that the device has not been compromised. This helps to greatly simplify mobile security.

User identification and management is another aspect of mobile security that IT can substantially simplify to help improve security. Organizations need to move toward a single, secure method of identity management that ties closely to a core solution such as Active Directory. This benefits IT as well as end users, as it simplifies tracking and enabling privileges for end users as determined by IT policy.

However, providing strong user authentication is not yet that simple. It is important to realize that most mobile devices, other than laptops, do not support two-factor authentication, which is one of the strongest forms of authentication. While this is not common on all laptops, Lenovo offers this feature on many ThinkPad systems.

For smartphones two-factor authentication remains a bit of an issue, with the best solution being a “soft token” system from vendors such as Microsoft, RSA, Symantec, SafeNet or Celestix. A soft token is an application resident on the phone that provides a method for two-factor authentication, such as the sending of a one-time code when a user wants to securely log on to a web site that is coupled with a password.

Moving forward, **IT must consider device, platform and security solutions** with an eye toward efficient operations. The magical “single pane of glass” that provides comprehensive monitoring and control over mobile devices doesn’t yet exist. As a result, the issue of operational simplicity has to be part of the decision criteria for mobility solutions.

If you start by focusing on vendors with more native security features and improved management and security solutions, such as MDM and virtualization, you’ll see savings and operational effectiveness.

SOURCES

"The 2013 Data Breach Investigations Report." *Verizon Enterprise Solutions*. 2013.

"2013 Internet Security Threat Report, Volume 18." *Symantec*. Apr. 2013.

"35% of Companies Worldwide Don't Use Encryption to Safeguard Business Data." *Kaspersky.com*. 14 Mar. 2013.

"6 Shocking Statistics about Internet Security Threats to Mobile Devices." *Techjaws.com*. 11 Apr. 2013.

Adamson, Matt. "BYOD: Value, Cost and ROI – The Debate Continues." *Solutions-review.com*. 27 Aug. 2012.

Ahmad, Munir, Lukman Sharif, Muhammad Kabir, and Maha Al-Maimani. "Human Errors in Information Security." *Warse.org*. July-Aug. 2012.

Bell, Lee. "Outdated Android Devices Are Exposing 400 Million Users to Security Threats." *The Inquirer*. 11 Jan. 2013.

Bent, Kristin. "The Mobile Device Threat: Shocking Mobile Security Stats." *CRN*. 8 Mar. 2012.

Clancy, Heather. "Desktop Virtualization Market Size Grows; Small Companies Represented." *SearchITChannel*. Nov. 2012.

Cooney, Michael. "10 Common Mobile Security Problems to Attack." *PCWorld*. 21 Sept. 2012.

Cooney, Michael. "Gartner: Mobile Device Management Tech Set to Take off." *Network World*. 26 Oct. 2012.

Dohnert, James. "Business Cost of Malware Spirals to $114bn a Year." *V3.co.uk*. 7 Mar. 2013.

Drew, Brian. "VDI Adoption Indications 2012." *Slideshare.net*. 2012.

"Facts and Figures behind the Current Threat Landscape." *Infosecurity*. 31 Jan. 2013.

Frost, Sharon. "Data Breaches: Expectation and Reality." *Faronics*. n.d. Web.

Johnson, David. "Has VDI Peaked? A Change in the Adoption Drivers Sheds New Light, and New Life." *David Johnson's Blog*. Forrester, 1 Apr. 2013.

Milrad, Danny. "State of the Data Center Survey Reveals Increasing IT Complexity." *Symantec*. 17 Sept. 2012.

"Mobile Threat Report Q4 2012." *F-Secure.com*. F-Secure Labs, 7 Mar. 2013. Web.

Shaw, Eric D., Ph.D., and Harley V. Stock, Ph.D. "Data Breach Trends & Stats." *In Defense of Data*. Dec. 2011.

Waldron, Harry. "End User Education in the Real World." *TechNet*. Microsoft, 20 Mar. 2013.

WebSense Security Labs. *Websense 2013 Threat Report: Nearly 600 Percent Increase in Global Malicious Websites; 85 Percent on Legitimate Sites*. *Websense.com*. 13 Feb. 2013.

Wolf, Chris. "Desktop Virtualization Trends at Gartner Data Center." *Blogs.gartner.com*. Gartner, 10 Dec. 2012.

Interested in learning more about mobile security for your organization?

Visit us at **www.lenovo.com/enterprisemobility**