Is Your Infrastructure “Mobile Ready”?

One of the main responsibilities of every IT manager is to secure, support and manage the tools and systems workers use. This responsibility has become more difficult by an order of magnitude with today’s mobile marketplace.

New mobile devices, high-speed networks and proliferating mobile applications open a range of business opportunities and benefits for adept companies. Yet to fully exploit the technology’s potential requires IT managers to first create a mobility master plan, and to ensure that they have the infrastructure to support both current and future demands of their mobile workforce. They also need to understand what the leading solutions are so that they can ensure productivity without compromising security.

IT managers need to have a holistic view of their infrastructure. They need to know what the mobile security essentials are that will protect their data, devices and network. A VPN; firewall; anti-virus, spam, spyware and malware protection are all measures that midsize businesses can take to help protect the security of a business-ready mobile infrastructure. Data encryption can also help safeguard sensitive data stored on mobile devices. Midsize business leaders can use encryption technology without impacting their users; they can protect data when the laptop is offline in many instances, for example.

This Technology Guide will help IT managers navigate through the business-ready mobile infrastructure journey through advice and peer example.

And whether an IT pro is beginning the journey or has already begun one toward building a mobile-ready infrastructure, the checklist of issues to consider on the last page provides some valuable insights.

IN THIS ISSUE:

Securing Information on a Mobile Infrastructure

Introduction

Small and medium businesses are increasingly challenged to provide comprehensive security for their mobile infrastructures without sacrificing the productivity it was designed for in the first place. For many, the problem is not so much about understanding the primary security issues such as prevention, detection, and response, but rather how to provide that type of end-to-end protection in a mobile environment. Although no two situations are ever the same, the objective is always the same: protect the data that is so important to your business. That is, after all, the beginning, the middle, and the end of the story for computer security. Of course, it isn't easy. This guide, as compiled from the combined resources of BNET, TechRepublic, and ZDNet.com provides a basic overview of most promising strategies and solutions for securing information in a mobile infrastructure.

Mobile Security Threats

As the number of remote and mobile workers increases so does the threat to mobile data security. As a result, businesses of all types and sizes must be much more aware of the potential risks inherent to a mobile workforce:

Device Threats

As the most common tools in a mobile portfolio, laptop computers and smartphones also represent perhaps the greatest risk to mobile security. Lost, stolen, and even destroyed devices are nearly unavoidable and require a growing number of precautions to prevent any serious threat to either the data on the devices or the network resources that they are used to access. In addition, malicious software (malware) from email and the Internet is on the rise and can be particularly problematic with devices that access these services from multiple locations and access points.

Network Threats

In addition to the information that's actually stored on mobile devices themselves, laptops and smartphones also pose a greater risk to information stored on the network resources that they are used to access. In addition to the most common risks of Internet and email malware from unprotected laptops and smartphones, businesses also face a growing threat from unauthorized network access through lost or stolen laptops and smartphones. Another common threat that is easily overlooked in mobile infrastructures is unsecured wireless remote access solutions.

Data Threats

Of course, the whole point of mobile data security is protecting the access and use of proprietary, confidential, and private information. Compromised devices and networks can risk everything from business secrets and communications to customer and employee records. In addition to unauthorized access, businesses must protect themselves against the unexpected with proper disaster and recovery planning. Another top consideration should

As the most common tools in a mobile portfolio, **laptops and smartphones also represent perhaps the greatest risk to mobile security.**

always be regulatory compliance and reporting which inevitably requires additional security measures.

Protecting data on a mobile infrastructure requires a comprehensive security posture that considers all of the devices and pathways that are used to store, transfer, and access information.

Mobile Device Security

Based primarily on all the threats created by the rising use of so many different types of devices used to empower a growing mobile workforce, it is essential for businesses to secure data on mobile devices. End-to-end protection requires a comprehensive system of practices, policies, and solutions which are all designed to protect data at rest and in motion:

Physical Security

As the mobile workforce grows, so does the risk from lost, stolen, and compromised devices. Physical security solutions such as locking cables and tracking devices are always a good idea but also aren't always necessarily practical. Despite the best intentioned solutions and policies, laptop computers and smartphones will continue to be stolen or left in the back of taxi cabs and airports so additional measures besides physical security are essential.

User Authentication

Preventing access is the key to protecting information that is stored on mobile devices. Of course, physical access cannot always be prevented so other measures must be considered. At a minimum, all devices should be password protected but even password authentication isn't always enough. Fingerprint and electronic card readers can easily provide even stronger protection against unwanted access to computers and devices.

Data Protection

Without a doubt, viruses, spam, and malware are some of the greatest inconveniences and security risks for mobile workers and anti-malware solutions are critical to protecting data. However, anti-malware only offers protection from threats that originate from email and the Internet. For even more security against issues such as lost and stolen devices, some businesses may also consider data encryption, which renders all information that might be saved on a computer virtually unusable. Also, whenever possible, businesses may also consider solutions that permit them to remotely erase or wipe laptop and smartphone hard drives.

Effective mobile device security is dependent on a number of important factors that also require a number of different solutions and vendors. Now more than ever, it is extremely important for businesses to consult with their hardware and software providers to determine exactly which security solutions are best optimized for their hardware and applications.

Mobile Network Security

Protecting networks that provide the access to information from a growing number of mobile devices is increasingly more difficult and requires increased vigilance as well as solutions that improve security without sacrificing productivity. As always, there are basic steps that every organization can and should take to protect network access as well as highly sensitive data resources, applications, and services, all of which are highly dependent on well considered and communicated policies that prevent unnecessary breaches:

Network Access Control

The first step toward providing security for a mobile network is device authentication. Network access control solutions can not only confirm that a device is authorized to access the network but also that the device is up-to-date in terms of patches, updates, and policies. Another good measure for controlling access to network resources is virtual private network (VPN) solutions which provide mobile workers with highly secure access to the primary network from remote locations over a public network such as the Internet. Increasingly, mobile broadband, which utilizes the same networks as mobile phones, can be used with VPN as another solution for providing secure access to the network from remote locations.

The key to comprehensive, end-to-end security is **a combination of device, network, and data protection.**

Firewalls

Firewalls remain one of the most critical security tools that any business can use to protect a network against unwanted external threats and intrusions. Firewalls use software and/or hardware to create filter and policy-based barriers that prevent unwanted connections to company networks, data, and devices. While most computers are generally protected by a firewall that is part of the operating system, firewalls may also be included at the router level and offer additional benefits for security and protection of network servers and resources.

Security Support and Management

Many manufacturers now offer a wide variety of minimal security features that will help simplify the protection of data, devices, and the network. Also, systems management services are also available to help manage patches and upgrades which are essential for the detection, containment, and response to new and emerging threats to mobile infrastructures. Again, by working closely with the right technology partner, businesses can dramatically simplify the support and management of their mobile security as well as reduce costs and improve the overall mobility solutions that they provide to their entire organizations.

Security Policy Enforcement

Of course, all security must be supported by strong policies based on the needs of the organization. However, any policy is only as good as the ability—or willingness—of the organization to enforce it. The key to enforcement, of course, is proper clarification and communication of company security policies. In addition, policies must be constantly updated, which requires a regular and careful review of an entire organization's security needs and objectives. Security policies cannot be taken lightly and require a close and careful alignment of IT and business decision makers.

Mobile network security is essential and the goal is always data protection. The first step is minimal steps such as access control, firewalls, and updated information but everything is dependent on an organization's ability to communicate and enforce its security policies. By doing so, businesses can safely and securely provide access to network resources which are so important to mobile workers and ultimately protect the data and information of the entire organization.

Conclusion

Mobility is good for productivity but also poses some serious concerns for information security. The key to comprehensive, end-to-end security is a combination of device, network, and data protection. Minimal measures that include not just data protection but also user authentication, access control, and policy enforcement are essential. In all cases, the right technology partner can provide comprehensive support at every level, from basic security solutions and optimization to managed system management and recovery that will ensure the overall security, compliance, and integrity of the entire mobile infrastructure.

Intel Continues Innovations for Mobile Market

Among the features of Intel processors that are targeted to the mobile market include:

Intel® Core™ vPro™ processors have hardware-assisted capabilities for enhanced security, manageability, virtualization, and energy efficiency. The technology allows you to power on an entire PC fleet to update a virus patch or remotely diagnose and repair PCs out-of-band (OOB), even if the OS is inoperable.

Intel® AES New Instructions (Intel® AES-NI) accelerates the encryption of data in the Intel® Xeon® processor 5600 series and the Intel® Core™ i5 processor 600 series. It is composed of seven new instructions that accelerate encryption and decryption, improve key generation and matrix manipulation, and aid in carry-less multiplication. Intel AES-NI also helps alleviate the performance challenges inherent in cryptographic processing.

Intel® Anti-Theft (AT) Technology for Laptop Security. The security technology is built into the laptop's processor, and is active as soon as the machine is switched on—even before startup. If the laptop is lost or stolen, a local or remote "poison pill" can be activated that renders the PC inoperable by blocking the boot process. This means that predators cannot hack into the system at startup. It works even without Internet access and, unlike many other solutions, is hardware-based, so it is tamper-resistant. It is designed to give IT administrators maximum flexibility and secure control of network assets. Since it is built-in at the processor level, the IT administrator has a range of options to help secure mobile assets, such as:

Intel® Turbo Boost Technology 2.0. The result is a boost in power levels to achieve performance gains for high intensity dynamic workloads. Turbo frequency is adapted to conserve energy, depending on the type of instructions, and its power and averaging algorithm manages power and thermal headroom to optimize performance.

Intel® Hyper-Threading Technology. The technology enables each processor core to run two tasks at the same time. The benefits: more threads and smart multitasking result in better performance, as well as faster response times.

Hoover City Schools save $357,000 with server virtualization initiative using technologies from Dell and Intel

Public school districts may not come immediately to mind when one considers the types of organizations that tend to be early adopters of the latest technologies; however, that perception is quickly changing. As more educators and parents grasp the value of a technology-based education and IT skills become ever more critical in a tight job market, many school districts are emerging as technology leaders in their communities.

Hoover City Schools, the third-largest city school system in Alabama, is committed to keeping both its technology and its students current. The district's dedication to quality in education has been nationally recognized: Newsweek ranked two of its high schools among the nation's best. For its IT infrastructure, the district chooses the latest hardware and software solutions from Dell, Intel and Microsoft.

"Five Nines" Server Reliability

For years, Hoover City Schools has used Dell PowerEdge 2950 servers with Intel Xeon processors as the foundation of its IT infrastructure. "Dell gives us great service, reliable machines and a very positive overall experience," says Keith Price, chief technology officer at Hoover City Schools.

In addition to 25 Dell servers in its main data center, Hoover City Schools maintains a local server at each of its 17 schools that acts as a domain controller and student information system host. Prior to a recent consolidation effort, these two systems were in some instances hosted on different physical machines. "We had about 30 servers between all the schools, all with direct-attached storage," says Price.

The district recently completed a refresh of the in-school servers using Dell PowerEdge T710 and T610 tower servers and refreshed the data center servers with Dell PowerEdge R710 and R610 rack-mount servers, all with Intel Xeon 5500 Series processors. Designed with virtualization in mind, the servers come with a choice of embedded hypervisor. Intel Intelligent Power Technology lowers energy costs while minimizing impact to performance by automatically putting processor and memory into the lowest available power state.

"For us, server reliability is key," says Price. "We're dependent upon our applications being up and running 24x7. Using Intel-based Dell hardware, we've come to count on five-nines reliability from our server infrastructure. And with low power consumption, optimized memory and Intel Hyper-Threading Technology, Dell PowerEdge 11g servers are perfect for virtualization."

Saving $21,000 Per School

Since Hoover City Schools uses Microsoft software for many of its key applications, it was natural for the district to choose Microsoft Hyper-V, part of Microsoft Windows Server 2008 Datacenter Edition, as its preferred hypervisor. Now the Microsoft Active Directory domain server and student informa-

tion system server can run as separate virtual servers—each running its own operating system—on the same physical server. As a result of this hardware consolidation, the district has saved $21,000 per school for a total savings of $357,000.

"We're using virtualization so we can have just one physical server at each school while still eliminating the operating system compatibility issues that can arise when you're running multiple applications on a single server," Price explains. "We've separated the student and teacher workspaces onto different virtual servers as well, to improve security."

To provide scalable, shared storage for the virtual machines without adding Fibre Channel infrastructure and expertise, Hoover City Schools selected Dell EqualLogic PS6500E iSCSI SAN arrays. "With Dell EqualLogic storage, we are able to provide consolidated, centralized storage with improved reliability, full data protection and more efficient access over the network for our users," says Price.

Simplified Data Protection

To ensure that critical data from the local schools is backed up centrally, Hoover City Schools uses a Dell PowerVault DP500 Powered by Microsoft appliance based on Intel Xeon processors. "We use Microsoft System Center Data Protection Manager, which comes embedded with the Dell PowerVault appliance, to move data from the local school back to the data center," says Price.

The Dell PowerVault DP500 automatically captures data changes as they occur in real-time and synchronizes with the data center every two hours. All backup administration is now performed centrally in the data center. "The Dell PowerVault appliance has improved our backup and restore success rates, allows us to restore data faster, and since using it we've had no incidents of data loss," says Price. "We're confident that our data is well protected."

"We're able to empower students and give them the skills they need **to succeed in the 21st Century."** —Andy Craig, superintendent, Hoover City Schools

20% Reduction In Downtime For Software Repairs

Hoover City Schools has been standardized on Dell desktops for many years, and is currently using Dell OptiPlex 760 and 755 machines based on Intel Core 2 processors with Intel vPro technology. Intel vPro enables the Hoover IT team to reduce downtime in the high schools by troubleshooting software issues such as operating system problems remotely, without having to deploy a tech to the site. "We estimate that Intel vPro reduces downtime for software repairs by as much as 20 percent," says Price.

The Dell Warranty Parts Direct program allows the IT team to keep spare parts on hand and perform its own warranty repairs on Dell hardware, resulting in faster break-fix.

Tablets And Netbooks Enhance Learning

To offer the benefits of mobile computing to its elementary school students, Hoover City teachers are using Dell Latitude XT tablet PCs with Intel Core 2 processors. Dell 1409X projectors make the screens visible to the entire class.

"We decided that mobile, tablet-size devices would be best for engaging children from kindergarten through the

fifth grade," says Price. "Teachers and students can write and draw with the built-in pen instead of being confined to keyboard input. We felt that the design, ease of use and durability of the Dell Latitude XT tablets were just what we needed, and the price-performance ratio was excellent. With Intel Core 2 processors, the Dell Latitude XT tablet has the power and performance to run all of our applications, including graphics-intensive art programs. The energy-efficient processors also contribute to long battery life."

Dell CompleteCare Accidental Damage Service covers repair and replacement for accidental damage to the Dell tablets, including spills, drops, surges and breakage.

The district is also using Dell Latitude 2100 netbooks with Intel Atom processors, along with Dell Mobile Computing Station custom netbook carts, as mobile student labs.

"Dell actually listens to educators, and the Dell Latitude 2100 netbook is a good example," says Price. "The educational community asked for a mobile device in a smaller form factor that still runs a full operating system, yet was affordable and that students would want to use. And we've really found that with the Dell Latitude 2100s."

Deployment In 90% Less Time

Hoover City Schools relies on Dell ProManage Laptop & Desktop Deployment Services to meet stringent deadlines for its client hardware refreshes.

"Dell Deployment Services is the key for us when we have to cover 375 classrooms in less than 30 days and have everything ready when the teachers come back," Price says. "We estimate the Dell team completed the most recent project in approximately 90 percent less time than we would have been able to complete it ourselves. As a result, the teachers were able to focus on instruction from day one and not worry about how to set up the systems."

Dell ProManage Asset Recovery & Recycling Services provide the logistic and disposal capabilities to recover and dispose of computer equipment in a manner that follows local regulatory guidelines. "Following the most recent refresh, we actually received payment of more than $33,000 for the difference between the market value of the used equipment and the work done by the Dell recovery team," says Price. "Dell also provided us with the documentation required for our records, certifying that they disposed of the used items properly."

A Smooth Migration To Windows 7

The district is in the process of migrating its client systems to the Microsoft Windows 7 operating system. To confidently make the transition and ensure that all its critical applications would run on Windows 7, the district turned to Dell Global Infrastructure Consulting Services (ProConsult).

"Dell is a Global Application Compatibility Factory partner for Microsoft, so we partnered with Dell for application compatibility testing," says Price. "Dell saved us months of testing time. They helped us identify which applications weren't directly compatible with Windows 7 out of the box, and helped us find solutions for making them work. This allowed us to leap forward in our deployment of Windows 7, and saved us the expense and hassle of replacing those applications."

A Tradition Of Continuous Improvement

By providing students and teachers access to the latest technology tools, Hoover City Schools is continuing to improve the quality of the educational experience.

"Our community is very supportive of the technology in our schools and has really come to expect the best," says Andy Craig, superintendent, Hoover City Schools. "With technology partners like Dell, Intel and Microsoft, we're able to empower students and give them the skills they need to succeed in the 21st Century."

4G to cover more than 4 billion people by 2015

ABI RESEARCH PROJECTS LTE, WIMAX WILL SPREAD RAPIDLY OVER NEXT FIVE YEARS

BY BRAD REED, NETWORK WORLD

More than 60% of the world's population will have access to some form of 4G mobile broadband technology by 2015, according to a new report from ABI Research.

ABI analyst Neil Strother says that between LTE and WiMAX, 4G technologies will reach an estimated 4.4 billion people within the next five years. This is more than double the 2 billion people today who currently have access to 3G mobile data technologies such as HSPA or EV-DO Rev. A, he says. ABI estimates that around 770 million users around the world today have access to either WiMAX or LTE services.

"Operators around the world are realizing that fast data speeds are going to be important to them going forward," says Strother, who also notes that by 2015 there will be three different iterations of both LTE and WiMAX on the market. "The demand for mobile data services will not go away and that's especially apparent in emerging markets that don't have wireline infrastructure. For them, wireless is a big driver."

4G technologies such as LTE and WiMAX represent the next stage in the evolution of wireless data technologies and generally deliver average download rates of 3Mbps or higher. In contrast, today's 3G networks typically deliver average download speeds about one-tenth of that rate.

Sprint is currently the only major carrier to offer 4G services in the United States as its WiMAX network has been up and running commercially for more than a year. Verizon is expected to officially launch its 4G LTE services in 38 U.S. markets covering around 110 million points of presence next month. By the end of 2013, Verizon plans to have all of its current base stations hooked up with LTE capabilities, meaning that most of the United States will be able to receive LTE coverage. AT&T and T-Mobile have both committed to launch their own 4G LTE networks sometime in 2011, though neither carrier has made any official announcements about when their networks are expected to come online.

Five Things CIOs Need to Know About Mobile Printing

BY DAVID F. CARR, CIO

It's in demand. As mobile devices become more capable, users want the ability to print from them. Imagine an executive visiting a remote branch office and getting e-mailed a PDF of an important document to review. Which do you think he'd rather do: Ruin his eyes trying to read it on his 3-inch BlackBerry screen? Or send it to the nearest multifunction printer? Mobile devices are everywhere, and users increasingly expect to have the option to print when it's convenient.

There's no easy answer. Mobile devices, particularly smartphones, often aren't designed for printing. A solution that depends on loading printer-driver software on each device is likely a nonstarter. There may be no driver for your printer available on a phone's operating system. And getting access to a secured local wireless network can be awkward for someone who is just visiting and doesn't have the right security code programmed into their device.

There may be workarounds. Least-common-denominator protocols, like those for Web and e-mail, can serve as a gateway to printing. For example, an enterprise mobile print solution that Xerox (XRX) developed in partnership with corporate customers like Procter & Gamble works by allowing employees to e-mail documents to an address associated with its enterprise print services. An automated system opens the documents and prepares them for printing.

You have to plan for printer changes. There has to be a way to select the right printer for each job. In the Xerox solution, the document output doesn't start until whoever requested the print job walks up to a given printer and punches a code into its control panel—a code that gets sent to the user in an e-mail response to their print-job submission. This method of holding print jobs until someone is there to pick them up also saves ink and paper.

Wi-Fi presents challenges. Ernest W. Lehmann, CIO at Bryant and Stratton College, has a problem when visiting lecturers want to print because the college's printers are on secured networks, for faculty and student use only. If they were on the open network, "somebody could pull up in the parking lot and print to our internal printers," he says. Still, he is piloting a solution where a printer on the open network would be available under the supervision of a receptionist or librarian.

Checklist: Ready or Not: A Mobility Infrastructure Master Plan

It was only a few years ago that businesses and other organizations could get away with a piecemeal, tactical approach to workforce mobility. They could identify a specific, high-value mobile application, select a single mobile device platform for all the application's users, provide access to a wireless network, and manage the whole operation in an isolated application silo. For most companies, such a narrow and rigid approach to workforce mobility won't cut it anymore.

The mobile marketplace is among the most vibrant and rapidly evolving of any high-tech sector, and its high pace of change wields a double-edged sword for IT and business managers. New mobile devices, high-speed networks and proliferating mobile applications open a range of business opportunities and benefits for adept companies. But fully exploiting the technology's potential requires managers to first create a mobility master plan, and to ensure they have the infrastructure foundation to support both current and future mobility workforce demands.

As with any technology strategy and investment, managers should contemplate a mobility master plan only after they've first identified their core business processes and objectives. Only then can the managers begin to evaluate what business value different mobility approaches can bring to the table. The master plan itself must be comprehensive, addressing mobile device and network options, data service plans, management and security needs, mobile application licensing and/or development, usage policies and employee education and training. Another fundamental requirement that mobility strategies and infrastructure share with other business technologies is the need for flexibility and adaptability. Ideally, companies will create a mobility infrastructure platform that – unlike a silo approach—can support multiple, and evolving, applications and devices. To accomplish this goal, managers need to ensure their solutions—and the devices, software and networks supporting them—comply with standards whenever possible, and don't impose technical or policy restrictions that could come back to haunt them.

Once the business case and strategy for a mobility infrastructure is made, arguably the most critical "component" to consider is mobility management and security. "For a mobile-ready infrastructure, one of the first things you need is a strong set of security policies," says Jim Nathlich a systems administrator at the San Diego State University (SDSU) Research Foundation. "You've got to have such policies published before you even start putting passwords on the phones."

Beyond a management and security regime, other mobile-ready infrastructure considerations include the following:

- The form factors, software characteristics and wireless capabilities of different mobile devices.

- The potential need to customize applications or to build new applications from scratch. Some mobile platforms are more closed than others, which could restrict customization and development options.

- The needed coverage and bandwidth of both internal Wi-Fi networks as well as external carrier networks, and the interoperability among them. The SDSU Research Foundation's Nathlich notes that it's also important to understand the carriers' data plans and their security mechanisms and capabilities.

- The option of enlisting third-party cloud-computing mobility service and application providers, which can reduce the need for companies to purchase, install and manage their own mobility infrastructure.