WHITE PAPER

Security enables the competitive business advantages of wireless infrastructure

Executive Overview

Today, enterprises in retail, healthcare, finance, government, transportation, logistics and other industries are finding new and better paths to maximum customer responsiveness and competitive opportunities by relying on a business infrastructure with robust wireless mobility capabilities. Accordingly, there is a growing consensus (based, in part, on sound economic justifications) that wireless mobility should be formalized and viewed as a cardinal aspect of business infrastructure, with robust risk/reward metrics and an expected business return.

The enterprise case studies discussed later in this paper show that the business advantages of converged wireless/wired infrastructure are best achieved via a formal, engineered approach that works with an interlocking set of security, IT and business concerns (see Figure 1). The field work finds that wireless business process agility and cost savings are often at risk in leading enterprises due to strong network and operational interdependencies that fall between the operational scope of specific enterprise departments and diverse IT vendors. This chain of dependency is too often an easy path for blended attacks, cost inefficiencies and cascading failures:

- Successful business-enabling wireless and mobility environments are dependent on a well-executed wireless security program…
- …which is vulnerable and ineffective unless it is intelligently managed with a unified wireless and mobility framework…
- …but security programs are, in turn, dependent on IT Operations best practices…
- …and, ultimately, all the various security, IT and operational domains are themselves dependent on an internal management culture that systematically aligns technology resources with business objectives and strategic risk calculations.

Given the interaction between all the cardinal aspects of this functional chain, it's evident that a company's brand reputation and bottom line are enhanced by wireless and mobility but can be put in jeopardy when unknown vulnerabilities and risk exposure cross the many boundaries that exist in this rich, complex environment.

Formalization of a unified wireless/wired security program may sound daunting, but with the right tools and practices, it's achievable. The security, risk and operational concepts put forth in this paper will help enterprise managers establish baseline (minimum acceptable) goals for the security and operational dimensions of a wireless/wired-enabled enterprise. From the baseline, there is a viable path to security program maturity, and the significant business and economic advantages that maturity brings.

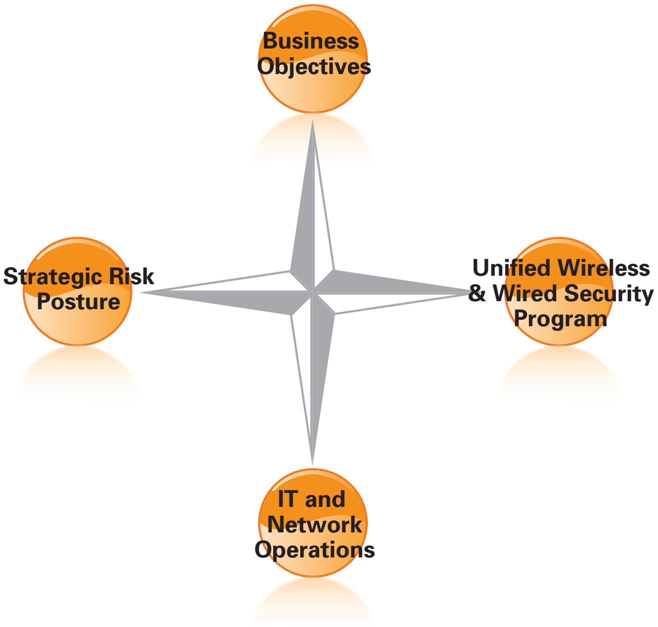
Business Objectives
Strategic Risk Posture
Unified Wireless & Wired Security Program
IT and Network Operations

Figure 1. A unified wireless/wired security program is a cardinal aspect of business infrastructure.

Introduction

Unified security is central to the viability of mobility-enhanced business processes. Wireless and mobile technologies have become increasingly critical enablers of innovation, operational cost-efficiency and service delivery in major horizontal and vertical applications. Mobility for handheld PDAs, smartphones, laptops, point-of-sale terminals, and other commercial/industrial mobile computing devices is critical to core business processes, but, unfortunately, a secure, well-designed wireless infrastructure is not something that's included in the product box.

The security assessments, design and managed security engagements that inform this paper show that security is a broad operational problem in many leading companies. If businesses don't address operational security considerations at the onset of wireless and mobility initiatives, they are putting critical assets and processes at risk. This point is underscored increasingly by the rising tempo of data breaches and serious financial consequences that occur when there is a mismatch between operational demands and unified security maturity.

Consequently, CIOs and IT managers who are not working aggressively on the formalization of wireless security programs expose themselves to unnecessary risk and adverse events that can drive significant expense and jeopardize customer goodwill.

In this complex new terrain, how should enterprises address the inherent operational security requirements of Confidentiality, Integrity and Availability (CIA) in current and near-term wireless infrastructure deployments? This paper addresses that question with tools and practices that lay the groundwork for a unified strategy for security and risk management that operates across:

- Wireless LANs (WLANs)
- Cellular employee and commercial devices
- Mobile unified communications and wireless VoIP
- Fixed/mobile business application convergence
- Wireless cloud computing and mobile ecommerce

What's needed to unlock the value of wireless business initiatives is a unified wireless/wired/operational security framework. One way into this brave new unified world is through the concept of a security baseline.

Baseline targets are used throughout business, operations and finance, showing up in business intelligence, compliance standards, management dashboards, and many other areas. Baselines are a fundamental part of business planning and strategy, and they are also a valuable tool for realizing the business advantages and cost savings of a wireless mobility infrastructure.

In the wireless/wired security context, a security capability baseline helps an enterprise rapidly achieve a state where there is greatly reduced risk of large data breaches, loss of intellectual property, compliance failure, or outright plundering of financial assets by cyber criminals. A unified security baseline can be seen as the minimum acceptable level of wireless/wired operational protections, which will, when achieved, create a reasonable expectation of business process resiliency, CIA, and sustainable success for mobility applications.

Unified security baseline targets are an excellent step on the road toward wireless/wired business infrastructure maturity: First, the current security state is assessed via vulnerability scanning and manual investigation of hosts and network devices. Then, this assessment is compared to a baseline built with a tailored set of protections and policies drawn from security industry best practices and standards (e.g., COBIT, ITIL, NIST, NSA IAM, ISO2700x series, etc). The baseline approach to mobility security and network design is ideal for organizations that have reached the conclusion that wireless networks and mobile devices should be treated as fully functional participants of the IT infrastructure.

Summary of key concepts in this paper: Throughout this paper, be on the lookout for these core concepts, which together contribute to a viable, cost-effective wireless/wired enterprise infrastructure:

- **Unified wireless/wired security:** Network and endpoint security and operational integrity cross seamlessly between wireless and wired infrastructure.
- **Business-centric security:** Security decisions are based on a clear understanding of the revenue-critical business assets that generate commercial and organizational value. (A unified security program requires inputs drawn from major business performance metrics, core operational goals, strategic risk posture and compliance needs.)
- **A unified wireless/wired security program:** A formal, engineering-based approach starts with an assessment of current state and then moves to a safe future state via a continual assess…design…deploy…manage cycle.
- **Baseline unified security targets:** A minimum set of protections and controls are in place. The baseline provides a foundation for maturity, as well as achieving the true economic and business performance advantages of wireless mobility.
- **Unified security maturity curve:** Security tools and practices are continuously improved in both wireless and wired spheres of the infrastructure in an orchestrated, operationally granular manner that extends from IT Operations to employee culture to the executive suite.
- **A unified wireless/wired security framework:** Specific expertise areas form the building blocks of a viable unified security program.
- **Unified security economics:** An integrated, formalized approach substantially reduces inefficiency and redundantly deployed IT resources. Regular streamlining and pruning of network resources results in performance benefits, and costs associated with attacks and breaches are controlled.
- **Security services:** Unified security programs and frameworks that include wireless and mobility require expertise that few enterprises possess. Hence the need to do extensive in-house training and recruiting, and/or work with a best-of-breed security services group, which has the demonstrated ability to handle the full cycle of program design and framework definition, as well as remote monitoring and management of security incident response.

The concepts above form an interlocking set of best practices and process improvements that can accelerate security maturity and enable a new, improved model for wireless and mobility security economics.

How the content is organized: The remainder of this paper is divided into the following sections that provide IT and business managers with a holistic set of practices and functional building blocks for an effective and scalable wireless/wired security infrastructure:

Section I – THE UNIFIED PROGRAM

Section II – THE UNIFIED FRAMEWORK

Section III – THE CASE STUDIES

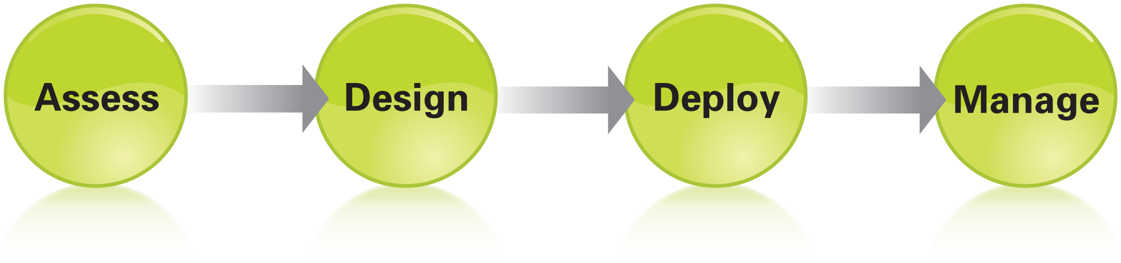

Figure 2. Major steps in the cycle of a unified wireless/wired security program

Section I – A unified security program for wireless and mobility-enabled business

A unified full-cycle wireless/wired security program to accomplish your business goals and reduce total costs and risk

In many enterprises today, IT infrastructure security is only marginally aligned with core business goals. Despite a strong security framework, often there are uneven levels of maturity found in IT Operations, wireless security, wired security, risk management and Information Assurance. In some cases, no formal corporate security policy exists. In other cases, steering committees write hundreds of pages of comprehensive security and compliance guidelines, which are overwhelming to under-resourced departments and business units that must execute policy.

In contrast, a unified security plan crosses all dimensions of the IT/network landscape and prioritizes actions based on a careful balancing of vulnerabilities, in-house capability maturity levels and available resources. Key building blocks for a holistic security program include:

Assessment Phase

Vulnerability assessment and management. Security engagements start with a thorough, expert assessment of interrelated wireless/wired infrastructure, IP network design/management processes, and all relevant physical facilities, business functions and operational resources. Note that an initial assessment may point to a number of significant vulnerabilities that require quick fixes to protect critical assets before an overarching security plan is created. The most threatening vulnerabilities are addressed with aggressive analysis and remediation.

Identify data of concern. Security improvements are impossible without an accurate picture of critical corporate and customer data at rest and in motion, including sensitive data in supply chains and partner relationships.

Gap analysis and baseline targets. Based on assessment and asset capture, the gaps between current state and minimum secure baseline state are defined.

Physical security assessment. Attacks are increasingly blended across vulnerabilities found in physical facilities and wireless/wired infrastructure. Ideally, the assessment phase will include a physical facilities security evaluation.

Design Phase

Defense-in-Depth architecture. The assessments, gap analysis and asset inventory become input to a holistic security framework that serves as a roadmap toward a converged mature security state. The architecture defines tools and practices for:

- Network segmentation, firewalls, traffic policies and security zones
- Host and application hardening, patching, firmware updates
- Mobile endpoint security configuration and hardening
- Wireless Intrusion Protection System (WIPS) and WLAN security design
- End-to-end access controls, authentication, sign-on systems
- Operational and administrative policies, separation of duties
- Monitoring, logging and reporting systems

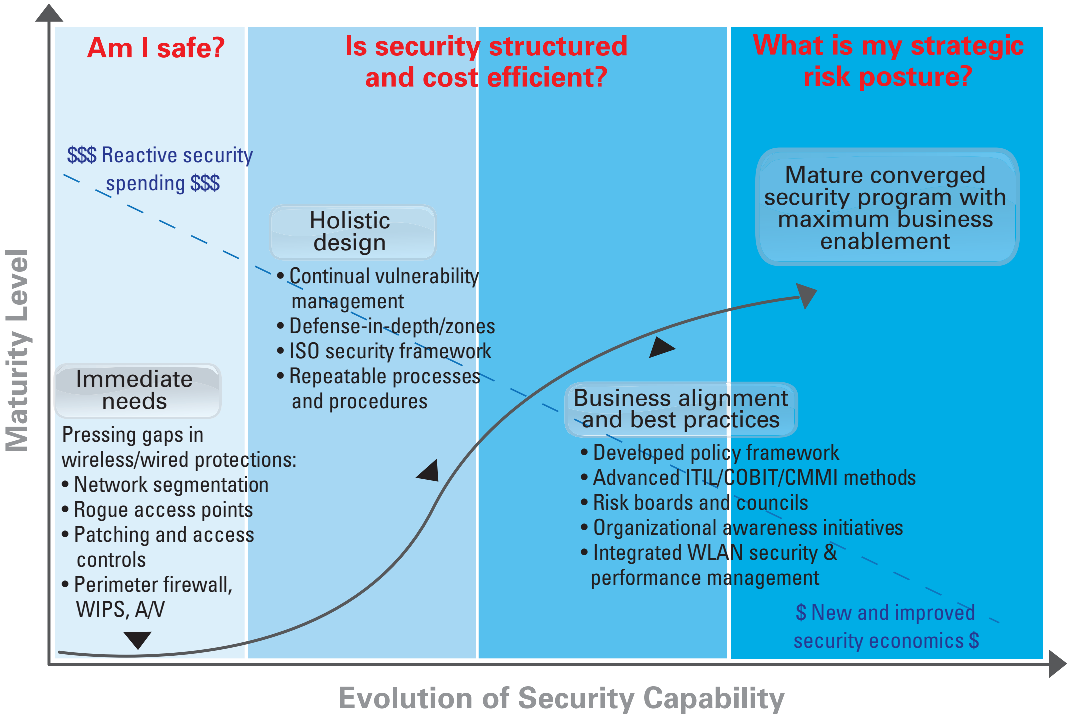
Am I safe?
Is security structured and cost efficient?
What is my strategic risk posture?
$$$ Reactive security spending $$$
Holistic design
• Continual vulnerability management
• Defense-in-depth/zones
• ISO security framework
• Repeatable processes and procedures
Mature converged security program with maximum business enablement
Immediate needs
Pressing gaps in wireless/wired protections:
• Network segmentation
• Rogue access points
• Patching and access controls
• Perimeter firewall, WIPS, A/V
Business alignment and best practices
• Developed policy framework
• Advanced ITIL/COBIT/CMMI methods
• Risk boards and councils
• Organizational awareness initiatives
• Integrated WLAN security & performance management
$ New and improved security economics $
Maturity Level
Evolution of Security Capability

Figure 3. Achieving unified security maturity means moving toward a state of continual improvement of wireless/wired security and IT Operations practices in a manner that is fully linked to business goals and corporate risk tolerance.

Compliance, governance and regulatory issues. Many security thinkers agree: Compliance is needed, but it is not a replacement for a holistic security program. Ideally, compliance is an outcome that occurs along with many other business benefits when converged security is done right.

Organizational security awareness. It's well understood that a large percentage of today's threat vectors involve employees, partners and contractors. The design phase can include organizational awareness and education practices that build a cultural orientation toward security and the need for continual vigilance.

Deploy and Manage Phases

Ongoing vulnerability assessment and management. After the initial assessment in the first program phase, there must be ongoing reassessments and continual vulnerability scanning, which will allow continual improvement of protections and the overall security posture.

Mobile device management program. Mobile device security is greatly facilitated with a strong centralized mobile device management capability.

Security Operations Center (SOC). A SOC provides continual around-the-clock remote monitoring and day-to-day remote management of wireless and wired security devices, software and processes.

Managed and outsourced security services. The use of a third-party security services provider can create substantially improved security economics and acceleration of a security program.

The above tools and practices are the building blocks for both a long-term roadmap and near-term security fixes that preserve brand value, customer reputation and compliance—while significantly lowering operating costs for wireless/wired infrastructure. When applied with technical and business expertise, this approach leads to a mature risk-based security posture that uses continual, business-centric security posture improvement to unlock the full business value of enterprise mobility assets.

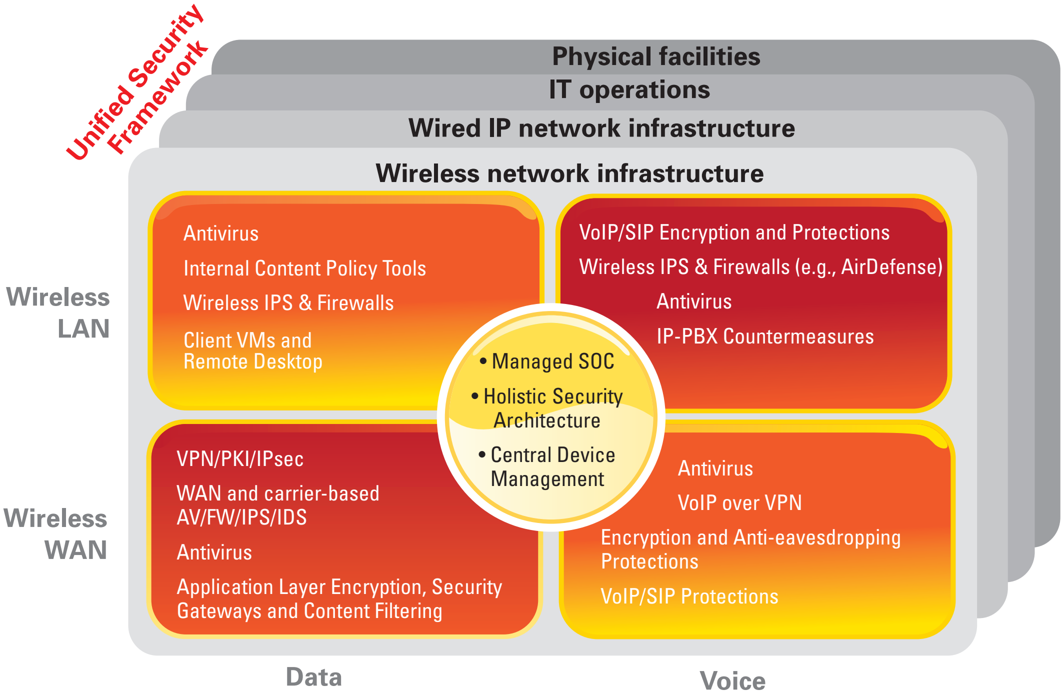
Unified Security Framework
Physical facilities
IT operations
Wired IP network infrastructure
Wireless network infrastructure
Wireless LAN
Wireless WAN
Antivirus
Internal Content Policy Tools
Wireless IPS & Firewalls
Client VMs and Remote Desktop
VoIP/SIP Encryption and Protections
Wireless IPS & Firewalls (e.g., AirDefense)
Antivirus
IP-PBX Countermeasures
• Managed SOC
• Holistic Security Architecture
• Central Device Management
VPN/PKI/IPsec
WAN and carrier-based AV/FW/IPS/IDS
Antivirus
Application Layer Encryption, Security Gateways and Content Filtering
Antivirus
VoIP over VPN
Encryption and Anti-eavesdropping Protections
VoIP/SIP Protections
Data
Voice

Figure 4. A successful unified security program requires an architectural framework that unites a number of protections and operational processes into a coherent working whole that crosses wireless and wired networks and applications.

Section II – A unified security framework for wireless and mobility-enabled business

Field-proven, business-centric security building blocks for end-to-end protection

When wireless handhelds, laptops, point-of-sale terminals, and other production devices are central to revenue-generating processes, security breaches can derail major business functions. For companies that depend on wireless and mobility converged with their traditional wired networks, holistic security practices enable a reliable, high- performance and cost-effective end-to-end IT fabric. The threat vectors and risk associated with converged network infrastructure can be viewed from the matrix perspective in Figure 4.

Implicit in the security solution matrix is a chain of security dependency: Wired networks are only secure if wireless security is effective… but, both wireless and wired network protections are themselves dependent on strong IT operational processes. Ultimately, networks and IT Operations are dependent on sound physical facility controls that form an indispensible aspect of Defense-in-Depth.

Wireless /wired security integration

As enterprise users increasingly cross between wireless and wired networks, it's necessary to move away from silo thinking about network security. Motorola security assessments and audits have found that many organizations have unmanaged, unauthorized access points and users who rely on questionable public hotspots. Even if the organization thinks that it has no wireless infrastructure—it often does! Hence, all enterprises need a wireless security policy definition, wireless security assessments and vulnerability scans—or major protection and compliance gaps will develop.

Virtually all of the security design principles for wired IP networks apply to wireless networks, with a few additional issues. These five key design principles should be applied to the entire end-to-end security fabric:

1. Scalable – protections and controls that have the flexibility to support inevitable network growth and expansion
2. Interoperable – security that does not interfere with system compatibility and multivendor solutions

3. Confidentiality and integrity – end-to-end protection of confidential or sensitive data in motion and at rest
4. High availability – security that ensures networks and services have maximum uptime and performance
5. Manageable – administration, monitoring and reporting that enable rapid resolution of breaches, outages and incidents

Wireless WAN security integration

The dominant trend in mobile devices is toward handhelds that work equally well on wireless LAN or wireless WAN (e.g., cellular, WiMAX) networks. In some cases, carriers are encouraging mobile voice/data users to roam back and forth between LANs and WANs. In commercial and industrial settings, the WAN can be used as a backup access method for mobile devices operating in locations that are out of the range of on-premise access points.

The rapid adoption of LAN/WAN mobile devices is great for business user agility, but the security implications are more problematic due the introduction of additional threat vectors and vulnerable software features. LAN/WAN mobility is part of a trend toward diverse access methods that include WiFi, cell network, Ethernet, and so-called PAN (personal area network) media—Bluetooth, USB, Firewire, etc.—on a single device. Multiple network interfaces and services open the door to blended attacks that access device resources via one network and then use another media to attack adjacent devices and applications.

For the security team, all of the various mobile device access methods and protocols are a growing challenge, which further underscores the need for a comprehensive LAN/WAN/PAN security architecture and policy set. Going forward, mobile LAN/WAN devices should be viewed as full-fledged enterprise client platforms that require all the hardening, countermeasures and policy considerations of desktop hosts… and then some.

IT Operations and security alliance

IT Operations are an important aspect of all security programs. The closer the security teams can work with IT Operations, the better. Enterprise mobility often is achieved in a decentralized way, driven by the choices and efforts of individuals and departments. IT Operations and Security must now work together on centralized management tools and policies if enterprises are to get their device fleets under control. Some examples of the great advantages of an Operations/InfoSec alliance:

Data management. IT Operations often is responsible for the backup and archive of data that can be restored in the event of a breach or malware attack that destroys data. This critical safety net for the security team justifies close coordination of incidence response plans, remediation procedures and forensic processes, with IT Operations kept in the loop at every step.

Asset management. According to numerous industry studies, including the widely read Verizon breach reports [1], many organizations don't fully understand the data they own. One of the greatest challenges of security engineers is the initial inventory of IT and data assets. Asset management, DBA reporting, desktop audits and application logging are sources of internal information that make the IT Operations department invaluable to security assessments and design.

Patch management. The IT Operations staff is typically involved in patch management, which is yet another area for close partnering between InfoSec and IT Operations. These teams should consult on a regular basis about the security- and non-security-related requirements for patches.

Device management. Businesses are using their wireless environments to achieve competitive advantage, which is unleashing a tidal wave of mobile applications and client devices—cell phones, PDAs, laptops, desktop PCs, portable payment terminals, field service PDAs, industrial handhelds, etc. The synergy and interdependency of security and IT Operations is not just in the core IP network and data centers; it also extends to the need for central mobile device management. The IT Operations team is concerned that mobile devices are correctly configured, patched via automated updates, tracked in the asset management system, backed up/restored, supported with a central helpdesk, etc. The security team extends these concerns into the area of remote data wipe or lockdown in case of theft, strong authentication, encryption, digital rights management and access logging, as well as mobile device antivirus, firewalls and VPNs.

[1] Verizon 2009 Data Breach Investigations Report

Managed security services and managed SOC

IT- and network-dependent enterprises are increasingly realizing that security is an advanced engineering discipline, similar to IT systems engineering and software engineering. Given the increasing reliance on converged wireless/wired infrastructures, managed services are, in some cases, the only way that enterprises can execute needed assessment, vulnerability testing, and advanced security designs for wireless and wired IT resources.

In addition to managed on-site security services, enterprises also can turn to remote Security Operations Centers, where highly trained security engineers monitor and manage enterprise wireless and wired networks 24/7, regardless of location. A SOC can even provide remote optimization, monitoring and proactive management of wireless intrusion sensors and Wireless Intrusion Prevention Systems (WIPS). In this case, the SOC will sense threats and anomalies, and conduct incidence response, forensics and remediation activities remotely, which cost-effectively applies deep security and IT expertise to the task of wireless network protection.

Compliance considerations

On a flat, poorly designed enterprise network, nearly everything is in compliance scope: LANs, WANs, business systems, production systems, warehouses, service departments, etc. The effect is often great extra expense to protect areas with low-sensitivity applications because they are interconnected to areas that contain customer data.

A comprehensive holistic wireless/wired security architecture often is the best and only true fix for an overly broad PCI, HIPAA, or other compliance scope. A holistic architecture will accurately classify data, establish access policies, improve monitoring/logging, and define use of VLANs, routers, firewalls, and wireless IPS (recommended by PCI DSS). The resulting network controls and segmentation can greatly reduce scope and cost of compliance. Other ways to reduce scope include isolation and consolidation of cardholder data storage, and isolation of wireless LANs used for point-of-sale and other transactional devices.

Common reasons for customer data compromise include: improper storage of sensitive information, unpatched systems, use of default passwords and other system configuration defaults, web server exploits, and open services on hosts. All of these are addressed by a proactive Defense-in-Depth security program. Additional security approaches that can increase compliance include:

- Tokenization with a token or reference number for a credit card number or other sensitive data to eliminate on-site storage of that data
- Network appliances that provide application white-listing; unapproved software and hardware can be blocked and flagged
- Virtual remote terminal approaches give users screen-only access to data and applications running in a secure data center
- Device- and application-level encryption, which can be expensive and complex, but justifiable in certain contexts

Compliance is a critical issue for many transactional enterprises and can be a good stimulus for security improvements, but it is widely agreed that compliance is just "the floor" for security practices, not "the ceiling." This is evidenced by an increasing number of breaches found in compliant organizations. And, just because an asset is out of compliance scope does not mean that it is out of harm's way. Bottom line: Compliance in itself will not ensure a secure infrastructure or resilient IT resources.

At its best, compliance is about metrics and precise goals for data protection. But why stop at compliance metrics and goals when there are so many other equally important indicators, including brand equity, market reputation, stock market value, performance in key partnerships, etc.? For this reason, the security team should develop an extensive set of metrics and measurements of success and failure, and apply these in a manner that goes far beyond the narrow compliance yardsticks. Ideally, the security team should be able to translate all granular security/IT statistics into business, governance and risk issues that are understandable to corporate executives and business unit owners who don't "speak geek."

Information Assurance best practices

A holistically oriented security team is in a good position to play an integrative role between all the technical, functional and business unit stakeholders that contribute to a secure, resilient infrastructure. By spanning enterprise silos, a synergistic Information Assurance (IA) program can extend the IT security program and address the need for cross-discipline collaboration on overall infrastructure security, risk and continuity issues. IA can provide valuable risk management inputs for informed enterprise planning and decision-making efforts. IA is particularly important if security teams are to get the organizational reach they need to move the enterprise down the security maturity curve toward full business alignment.

Section III – Case studies

Real-world examples of the business and economic advantages of a unified wireless/wired security approach

These unified security case studies contain real-world business advantages and security insights captured by Motorola Security Services (MSS) consultants and lab engineers. MSS is engaged regularly by leading enterprises to protect critical data and business processes in retail, logistics, healthcare, transportation, utility, government and other industries.

Compared to the average corporate security department, MSS has an unusual diversity and depth of expertise that is the basis for advanced end-to-end security architectures, security programs and focused security product solutions that cross traditionally isolated realms. In many cases, MSS works closely with the Motorola AirDefense Wireless Intrusion Protection experts and the Motorola Security Operations Center (SOC) on wireless enterprise security challenges and solutions.

Case Study: Global Consumer Goods Retailer

This multinational enterprise operates successful retail chains and depends heavily on wireless infrastructure throughout its retail and logistical operations. Most store locations, warehouses and corporate offices have exposure to customer credit card data and, hence, are within PCI compliance scope. Security and infrastructure considerations include:

- Each retail chain in the system has its own IT department.
- IT networks from chains interface to a large IT outsourcing provider.
- More than 3000 wireless (WLAN) access points provide critical operational capability but enable potential threat vectors if not configured, monitored and managed correctly.

The Motorola managed security solution began with a wireless security assessment that included a thorough review of the entire network topology, paying particular attention to the Wireless Intrusion Protection System (WIPS) sensors and appliances. The WIPS monitors traffic, senses rogue devices with wireless sensors, and generates security events based on detected threats.

The WIPS solution was not fully documented or consistently configured. There was no unified set of policies and processes to ensure protection of IT assets and PCI DSS compliance. Numerous store locations were not actively monitored due to WIPS sensors being offline. There was a prevailing view in this enterprise that WIPS in itself equaled compliance and audit success—which is, of course, not necessarily the case.

Installed WIPS appliances and sensors were running older software/sensor firmware. As with many large wireless networks, the WIPS devices were often using default configurations that were not tuned to the enterprise's real-world requirements. Log rotation policy was not established, causing forensic data to be lost. Regular appliance configuration backups were not being performed, which potentially could negatively impact the availability of the WIPS solution. In the administrative sphere, too many people had unmanaged access to network and security resources, making controls and policies difficult to enforce.

Business advantage/security insights

The operational approach to the wireless network was putting the enterprise at risk due to numerous vulnerabilities and manual processes that did not leverage the security capabilities of the deployed WLAN and WIPS infrastructure. This approach also was driving unnecessary cost while reducing operational capability.

The recommended solution required:

- Redesign, documentation and reconfiguration of the WIPS system and creation of a viable baseline security posture
- Convergence of an accurate picture of all network resources in WIPS device inventory on all appliances
- Tuning of the alarm database to ensure that only relevant alarms are acted upon
- Greatly increased compliance and reduced risk exposure via integration of AirDefense WIPS with Motorola Security Operations Center (SOC)
- The SOC provides around-the-clock remote monitoring of an enterprise's WIPS resources and alerts the enterprise to events that potentially pose risks to cardholder data

Business, economic and operational benefits:

- Immediate reduction in false rogue AP alarms to less than one-tenth of previous levels, which gave the enterprise a precise picture of unmanaged, unauthorized and rogue AP devices for the first time

Unified security in cellular WANs

Assessments of carriers and telecommunications companies by the authors of this paper have uncovered a wide range of WWAN vulnerabilities and the potential for voice/data breaches. Based on the findings, enterprises should carefully evaluate WWAN provider security and data protection measures, and, where appropriate, deploy additional end-point security hardware and software countermeasures (e.g., voice/data encryption, VPN, etc.) to protect mobile device traffic that traverses WWAN services.

A leading European cellular operator requested a thorough assessment of its core network and host assets using four different types of vulnerability testing and analysis:

- Profiling of target networks with publicly available information
- Mapping of the internal network topology
- Identifying available host targets and services
- Attack and penetration/vulnerability testing

It was found that a simulated attack could map virtually all of the core network and business systems using nothing more than a standard smartphone or a laptop with a PCMCIA WAN card. Beyond mapping, it was found that internal systems could be accessed and compromised so as to disrupt service or cause disclosure of customer data. The good news for business cellular device users is that the recommendations, when carried out, led to a major turnaround in the carrier's security posture. But, based on these findings, sensitive enterprise voice and data traffic should be protected on the endpoints and as it crosses public cellular services.

- SOC integration reduces need for expensive specialized security engineers
- SOC event activity reporting replaced several man-hours a month of manual report generation performed by the customer
- Documentation and reports generated by our SOC are key deliverables to assist the enterprise in proving to QSA that PCI compliance requirements are met regarding WLAN security monitoring

Case Study: Fortune 200 Apparel Products Company

Extensive wireless LAN infrastructure plays an important role in the ongoing success of this well-known brand-name manufacturer, which owns a large chain of its own retail outlets in many locations around the world. In this environment, wireless has become a business-critical component of the IT environment, providing essential access for mobile point-of-sale systems and handheld inventory devices, as well as a range of mobile computing devices.

In addition to several major operational vulnerabilities, the wireless retail network had considerable gaps between protections and PCI compliance, which worked against audit success. Adjustments were needed immediately to:

- Secure wireless infrastructure design and configuration
- Create unified security policy with administrative best practices
- Eliminate compliance gaps

In response to this enterprise's pressing wireless security needs, the Motorola Security Services team conducted a rapid but thorough assessment of the entire wireless retail network. MSS found that the lack of centralized security policy and controls had allowed numerous vulnerabilities and misconfigurations in the wireless network and supporting IT systems. Of particular concern was the use of weak pre-shared encryption keys for wireless access points and open administrative access to devices via telnet. Due to the lack of logging and reporting, there was little chance of effective forensics and incident investigation in the event of a breach or attack.

Business advantage/security insights

This enterprise had a great need for a unified WLAN security policy to address serious vulnerabilities and close the PCI compliance gap. Critical to this effort was a requirement for a new key management process that would support the existing needs of their business, improve the security of their WLAN environment and bring their enterprise into compliance with PCI-DSS.The recommended solution required:

- New policies to specify how wireless switches and access ports should be built to the standards, contained in a unified administration document that is consistent in all locations
- Centralized wireless configurations that can be accurately replicated to ensure consistent deployment of the WLAN throughout the entire retail environment
- Changes to device identification, configuration and encryption keys in more than 100 store locations in a wide, geographically distributed operating environment
- Administrative controls locked down to disable default telnet and SNMP management protocols
- Policy and operational guidelines to ensure that only approved encryption protocols and authentication processes are used across the enterprise

Business, economic and operational benefits:

- A highly improved compliance posture
- Performance improvements and expanded scalability
- Cost-effective central management of WLANs – with potentially lowered operating costs

Case Study: Global Distribution & Logistics Leader

The distribution centers of this well-known distribution and logistics enterprise depend on wireless networking for daily operations and revenue-critical applications. But, due to rapid growth and a multivendor IT environment, security policies and operational IT resources were fragmented into functional and technical silos that impeded security.

Motorola found that inconsistent WLAN configurations and traffic policies were contributing to both vulnerabilities and performance degradation that caused production users to experience intermittent loss of connectivity. As a result, production teams often used wired connectivity, which limited their flexibility and productivity. In the warehouse setting, certain work functions can be executed only via wireless connectivity, so the WLAN issues became critical. WLAN problems were made worse by an excessive number of wireless access points and poorly configured antenna hardware, which resulted in RF interference and loss of signal for end points. Finally, outsourced IT personnel did not have a thorough picture of network traffic and access policies, and had not isolated systems into secure zones that mapped to data value and application needs.

Business advantage/security insights
It became clear in the process of the engagement that the enterprise needed much more than just WLAN security improvements. Consequently, the recommended security program included a comprehensive Defense-in-Depth strategy with core network intrusion protection, web content controls and VPN access for additional protection at multiple layers of the network.

The recommended solution required:

- Assessment of entire operational picture leading to security recommendations that included creation of strong traffic policy boundaries between core internal systems and public facing systems based in a demilitarized zone (DMZ)
- An analysis of all wireless network segments and relevant radio frequencies, looking for misconfigurations and unauthorized nodes
- Implementation of a Wireless Intrusion Protection System (WIPS) and drastic reduction in the number of deployed access points
- Better design of an identification and authentication framework for WLAN APs, including discontinuation of LEAP authentication in Cisco® devices
- Hardening of host servers and a patch management program
- Better relations, communications and operational integration with IT outsourcers and vendors

Business, economic and operational benefits:

- Substantially lowered capital and operating costs due to elimination of unneeded access points and related overhead
- The unified assessment and security architecture recommendations provide the knowledge needed to address network and host vulnerabilities in a systematic proactive manner, which is a necessary ingredient for good compliance audit results and related confidentiality, reliability and integrity of the end-to-end network infrastructure
- A unified security approach addresses the inadequate network design that caused intermittent loss of connectivity experienced by production teams, resulting in more robust productivity and reduced negative impact on revenue stream by IT
- A related payoff is greater business agility due to the ability to plan business operations with confidence in the wireless infrastructure
- Lowered business risk and brand damage potential due to a formal approach to address network vulnerabilities, including wired and WLAN vulnerabilities, rogue devices, poor RF coverage patterns and unauthorized WLANs

Case Study: European Pharmaceutical Services Company

The wireless networks of this busy medical services firm are integrated with production laboratory systems and financial applications via a core backbone network. Consequently, any vulnerability in end-to-end IT Operations would expose sensitive corporate and patient data, including medical test results. The assessment relied on advanced vulnerability scanning tools that were used to analyze all wireless and wired devices. After the scan, the Motorola team followed up with hands-on verification of host and network device configurations, and checked patch levels to complete the picture. Motorola found that the network lacked even basic segmentation, creating vulnerabilities and an excessively large compliance scope. All external network connections were not protected by VPNs, and some firewall protections were turned off for some external users. Likewise, workstations and server end devices were not secure. On the wireless side, WLAN access points were unprotected and poorly configured. In general, the organization lacked awareness about sensitive data.

With an enterprise that is at an early stage of security maturity, it is necessary to carefully focus available resources on the most critical and high-risk problems. In this case, the findings supported the IT department's position that an overall network redesign and essential Defense-in-Depth countermeasures should be an urgent priority. In the current state, there was a lack of VLAN segmentation, which meant that a breach at any point could give attackers access to significant infrastructure, IT resources and, potentially, customer data.

Business advantage/security insights:
In this network-dependent medical lab, critical laboratory systems and patient data were at risk until a unified wireless/wired security approach was adopted.

The recommended solution required:

- Dedicated firewall interfaces where ingress and egress traffic could be controlled by a custom rule set; overall network redesign with layer 2 and 3 VLAN segmentation and suitable network control policies

- External systems, including email, web servers and DNS, should be moved to their own security zone on a separate firewall interface
- Review and clean up the existing firewall rules, and proactive logging enabled for the most important rules.

Business, economic and operational benefits:

- As the above recommendations are put in place, the business can achieve greatly reduced data breach risk, particularly if stronger authentication for data protection is adopted (e.g., EAP/Radius for sensitive patient data)
- A unified end-to-end picture of the wireless/wired networks enables precise, timely recommendations in all areas of the people, process, policy and technology environment, which is the only basis for an improved organizational security culture and truly effective protection of core processes
- Simplification of security best practices by the unified approach reduces operating costs because enterprise in-house staff are shielded from a mountain of recurring security audit findings
- Cost-effective utilization of available in-house IT assets and human resources due to a security program design that can eliminate waste by focusing on the highest-priority issues first

Case Study: U.S. Municipal Government

The administrators of this city government thought that their wireless LANs were entirely separated from their back-office systems and office networks. Unfortunately, this was not the case due to an improperly configured firewall that exposed portions of the core enterprise network to public-facing wireless access. This is a challenging network context because it requires a high degree of openness for citizens and public users, while, at the same time, very high levels of protection for internal systems and sensitive government records. If the public network could not be secured, citizens would not have easy access to online services that greatly reduce the cost of responsive government, including bill payment, police reporting, traffic event tracking, permits and surveys, which were all components of the customer's strategic business plan.

The MSS assessment team found that the municipal WLAN networks where not configured the way that the city thought they were, and there was little attention paid to the natural synergy between the wireless and wired networks. Through extensive wireless and wired vulnerability scanning and expert manual investigation of end and intermediate devices, vulnerabilities were uncovered, validated and logged. As is seen in many MSS engagements, serious vulnerabilities are often made worse when combined with seemingly unrelated weaknesses in other areas of the infrastructure. In this case, the misconfigured wireless LANs opened up public access to servers that were not hardened with public-facing security in mind.

Business advantage/security insights:
This is a classic case in which an overburdened enterprise IT team, even with credible security practices, may overlook vulnerabilities in a dynamic, complex operational environment. Motorola often finds these issues—and oversights—at the intersection of the wireless and wired networks, where the magnitude of the vulnerabilities can have significant impact to business plans and strategies.

The recommended solution required:

- Comprehensive mapping, documentation and analysis of the end-to-end network infrastructure
- Public versus internal traffic policy with robust network segmentation and new firewall configurations, hardening of shared services, and Defense-in-Depth protection of internal web servers
- Better administrative policies and operational procedures to address many host and network device vulnerabilities
- Central administering and distribution of user identities and passwords via a single-sign-on approach
- A thorough assessment of the physical security posture within the governmental offices and City Hall

Business, economic and operational benefits:

- With a unified security approach, the government department can sustain a strong public-facing open access policy
- High-value business system data can now be proactively protected from public networks and the Internet
- A full spectrum Information Assurance (IA) approach includes analysis of critical data and business functions, which can greatly reduce costs and speed time to an overall wireless/wired solution
- As program is deployed, expect reduction of wasted, redundant human effort and IT assets due to streamlined network architecture and policies
- A limited government operational budget can be intelligently and precisely applied to high-priority security controls

Get to Know Motorola Security Services (MSS)

Enterprises around the world rely on MSS security engineers for their unique ability to resolve challenging security issues that exist throughout wireless, wired and operational areas of the enterprise. MSS expertise crosses all major dimensions of wireless/wired IT infrastructure and all phases of the IT lifecycle:

- **Assess:** the current security state with advanced security assessment and vulnerability testing services
- **Design:** holistic policy and architectures for a secure future state
- **Deploy:** integration, configuration and testing of secure solutions
- **Manage:** on-site and remote (SOC) managed security services

In addition to the above lifecycle services, MSS can provide rapid-response security gap remediation and forensics where needed. In the area of security strategy and planning, MSS can be engaged to collaborate with IT Operations on process improvements in device management, patch management, data protection and network asset discovery. At the cross-organizational level, MSS can help companies build out viable Information Assurance that enables efficient security/business alignment.

MSS is available for small and large security engagements, and can be used as a managed service resource where in-house resources are not able to protect corporate and customer IT resources in a timely manner. In addition to its field engineering teams, MSS is closely integrated with the Motorola Security Operations Center (SOC), featuring global around-the-clock monitoring and remote management of wireless and wired infrastructure. Motorola's SOC has TL9000 certification to ensure the highest level of quality system management. Today, a large community of enterprise customers around the globe benefit from Motorola NOC/SOC operations.

MSS operates in a wide range of vertical industries: retail, healthcare, government, manufacturing, education, utilities, etc. A number of specially tailored services are available. For instance, in the retail industry, MSS provides a highly focused PCI Planning and Assessment Service, as well as PCI Policy & Procedure Design, Implementation and Monitoring Services.

Why Motorola?
Motorola is a world leader and trusted partner in wireless network solutions. From WiFi to WiMAX, cellular to mesh, Motorola is unique in our history of wireless insight and innovation.

Motorola was also one of the first companies to recognize the threat of Internet crime and wireless breaches, and developed many of the processes and procedures that become the core of any company's security posture.

When traditional IT professional service providers offer security services, they are often working outside of their core area of expertise. In contrast, Motorola security assessments, programs and products are developed by accredited security practitioners (e.g., ISACA CISM, CISA, ISC2 CISSP, Certified Ethical Hacker CIEH, SANS Certifications, etc.) using best-in-class Information Security practices and methodologies (Cobit 4.1, CIS Benchmarks, ITAF, ITIL v2/3 Security Management, NIST, NSA IAM, OCTAVE, SANS, ValIT) to satisfy international/national Information Technology standards, such as PCI DSS, German BDSG, Data Protection Act(s), EU Directive 95/46/EC, GLBA, HIPAA, ISO 17799/27001/27002, and SOX/Euro-SOX.

For more information, please visit
www.motorola.com/business/services

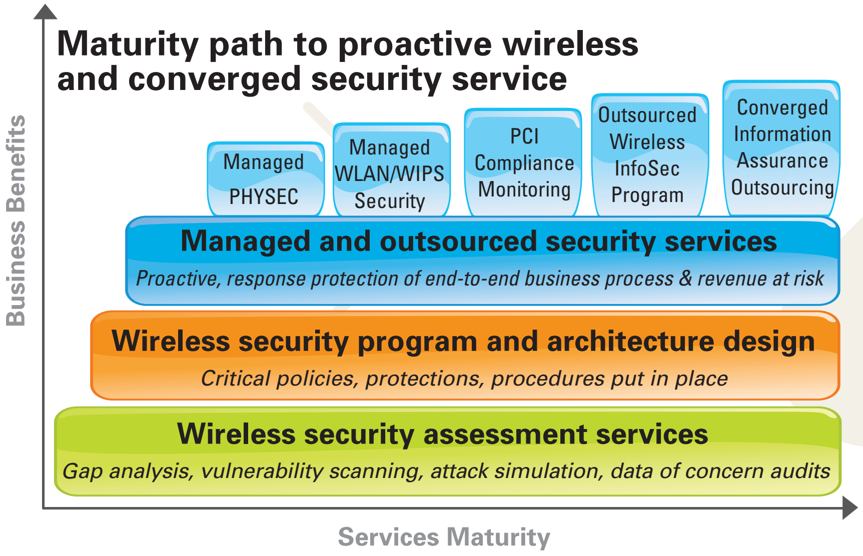
Maturity path to proactive wireless and converged security service
Managed PHYSEC
Managed WLAN/WIPS Security
PCI Compliance Monitoring
Outsourced Wireless InfoSec Program
Converged Information Assurance Outsourcing
Managed and outsourced security services
Proactive, response protection of end-to-end business process & revenue at risk
Wireless security program and architecture design
Critical policies, protections, procedures put in place
Wireless security assessment services
Gap analysis, vulnerability scanning, attack simulation, data of concern audits
Business Benefits
Services Maturity

Figure 5. The business benefits of a unified wireless/wired security program can be rapidly realized through coordinated use of in-house and outsourced security capabilities. A unified security partner can maximize the value of internal security resources while adding what's missing in the overall security program – which is a fast track to security process improvement and acceleration down the security maturity path.

MOTOROLA

motorola.com