Uniting Security Forces Against Risk

Save to myBoK

by Lew Wagner, CPP, CISSP

Threats to your facility's physical and information security become more complex all the time. To create a truly effective security program, consider developing an integrated security program that encompasses both traditional and information technology protection. The result? A strong, streamlined program that enables—not inhibits—healthcare delivery.

The roles of corporate security officers and enterprise security risk management programs (RMPs) are changing due to the penetration of information systems and networks into virtually every segment of healthcare institutional operations. As a result, the position of corporate security manager for executive protection, guard force, and physical security systems is giving way to an executive-level chief security officer (CSO) and an integrated security department—one that unites the traditional institutional "guns, guards, and locks" security with information technology (IT) security. In this article, we'll look at how to build an integrated security RMP and its advantages.

A History of Division

Corporate security and IT security regimes were originally seen as two distinct and separate security environments with little effective coordination between the two camps. Traditional security professionals had little, if any, understanding of the rapidly growing IT security arena. Further, IT security was seen as only relating to computers and networks and not the information those systems processed. For that reason, IT security was relegated to system and network administrators with little or no corporate security expertise or training.

Given the exponential growth of IT systems and subsequent threats to those systems, an integrated approach to protecting a company's assets and resources was needed. This approach needed to effectively coordinate manual and automated methodologies and processes under one security entity—that of the CSO and an integrated security RMP.

Strength in Integration

The result of this integration is reduction in the cost of maintaining redundant security administrative functions, increased ease of communication along one common security management chain, and a streamlined security work force because of consolidated security functions.

Benefits to the organization at large are powerful as well. First, the program enables healthcare operations because business roadblocks from an insecure environment have been removed. Second, e-health initiatives facilitate secure communications and transactions between the institution, its patients, government agencies, and medical commercial enterprises. Finally, there are three chief security enhancements resulting from enabling critical healthcare resources and assets. They are:

- integrity: the content of the information will have a high degree of accuracy so that clinicians, researchers, and other healthcare providers are assured that any recommended treatment is based upon valid data
- confidentiality: clinicians and staff will be able to conduct business in a more effective and secure manner because there are several federal and state laws, statutes, and regulations (as well as infrastructure security safeguards) in place stipulating the protection of sensitive data from unauthorized or inadvertent disclosure to people or entities who don't have a valid need to know such information
- availability: caregivers will be unable to provide medical care if information is not provided when they need it. Heightened levels of data availability accrue when security solutions prevent or at least reduce the number of occurrences of system or network outages or denial of service attacks

A common argument against rigorous security is that it forms a roadblock to accomplishing daily tasks or yearly goals. This is most often the result of security staff automatically rejecting requests or suggestions. Although certain practices are inherently insecure and must be stopped, there is a better way to respond to the customer. To be seen as a better security support organization, the security department needs to communicate and implement security solutions that give clinicians and staff integrity, confidentiality, and availability of critical resources and assets while minimizing the effect on their productivity.

The Security Triad

Any good security program depends on the skillful blending of three essential subcomponents: people, process, and technology (PPT). All three are needed to adequately support and develop your facility's risk management program. For example, writing policy and procedures does no good if the people or technology to execute them are missing. Similarly, directing money and policy at a security solution won't help without trained, competent staff to implement or maintain such technology. Finally, hiring staff without matching up needed skill sets to proposed and current technology or not providing skilled security team members with guidance policy and procedures will hinder the security effort. Below, we'll take a closer look at each component of the security triad:

People

To maximize the effectiveness of the security staff, key responsibilities should be earmarked for each level:

- management: vision, executive interface, information security steering council, staffing, and selling
- architecture: vision, interpreting business needs into secure information processing designs, advance security concepts and technologies assessment, and executing RMP
- implementation: facilitating porting of security architecture to business units for operational usage, trouble shooting, and security reviews
- operations: maintaining sensitive corporate-centralized security systems (authentication servers, firewalls, global password management system, user account management, facility protection, investigations, emergency response, and personnel security background checks)

Process

There are three primary areas to consider when developing and implementing a solid process approach to any security risk management program: program, model, and methodology. They must be developed sequentially so that the second and third areas build on a strong foundation. In other words, the RMP drives the corporate information security model, which in turn drives the security methodology. The areas are:

- program: the RMP is the foundation. Without prioritizing business risk and assigning threat countermeasures based on acceptable risk, any subsequent solution will most likely be focused on remediating the wrong problems or responding to lesser threats
- model: an information security architecture model will have to be integrated into the overall institutional security program. This model should focus on protecting critical and sensitive subcomponents of your infrastructure versus simply protecting it from the outside. The former is a more effective process whereby critical nodes in the institution are protected regardless of where they are in the network. The latter approach is flawed because it assumes there are not threats against critical assets and resources from within the institution. A more realistic view recognizes that critical functions within the institution are segmented based on their criticality and sensitivity even within the institution's IT infrastructure. These high-value assets are protected by multiple layers of security screens (a method known as dynamic defense in depth or D3). In this manner, attackers are presented with an array of protective mechanisms so that if they get past one or two, there is a high probability that they will either give up or be defeated in their penetration attempts
- methodology: methodologies consist of procedures describing how a particular program, policy, or architecture model should be implemented, performed, or accomplished. For example, if an organization has a security policy, but no specific operational checklists are created to implement that policy or ensure that the policy is implemented consistently across multiple departments and divisions, the security program will suffer. Consider using the following methodology:

- identify business security needs so that your program is effectively meeting security concerns of your customers
- formulate and implement security policy to build a consistent baseline security requirement from which to enact technical security architectures
- protect resources by implementing and maintaining security safeguards
- detect intrusions through extensive monitoring and sensor placement along key nodes within the information technology infrastructure
- respond to incidents so that any impact is quickly and effectively detected, reported, contained, and mitigated
- adapt to a dynamic security environment as threats and protective methodologies are constantly evolving

Technology

Technology is an equally important part of the security PPT triad. A security department needs to develop a strategic technology roadmap incorporating the following security controls (they provide the D3 layered defenses necessary to effectively combat the increasing number and sophistication of blended threat attacks both now and in the future):

- identification and authentication: this is the first line of technical defense. Users should provide enough non-repudiation information so that there is a high degree of assurance that they are who they say they are. Examples of identification and authentication controls include passwords, one-time passwords, user IDs, single sign-on, biometrics, smart cards, and role-based access controls
- audit: the second line of technical defense works once users are inside the system: their actions are tracked and recorded so that unauthorized activity can more readily be determined and acted on. Auditing yields a higher level of non-repudiation by an individual if surreptitious activity is discovered. Examples include server logs and application invalid requests
- encryption: although it does not ensure availability of resources, encryption provides heightened integrity and confidentiality to authorized users who are strongly authenticated to the encryption technology. In this way, the contents of sensitive information files are protected from view by unauthorized individuals or processes. Examples of such technologies include virtual private networks, software like Pretty Good Privacy, or protocols like secure sockets layer or Internet protocol security
- network-based filtering: these tools bar network traffic from attempts to violate access rules or send malicious code to unprotected servers behind network devices. Such technologies include server- and appliance-based firewalls, routers, and switches
- intrusion detection: attacks by individuals, entities, or processes must be detected before you can act on them. Technologies in this category are placed at key locations throughout an institution's IT infrastructure where the majority of traffic flows or at critical points. Once installed, normal activity should be determined so any abnormal activity can be detected, reported, contained, and mitigated. Examples of such technologies include network switch intrusion detection system blades and host-based server intrusion detection

The Shape of Your Security Environment

The overall security coverage a corporation uses is called the security environment. This environment is shaped by three interrelated concepts:

- what to protect
- countermeasures
- threats

To consider one or two of these factors without the other(s) leaves companies open to ineffective application of security safeguards. The first concept encompasses what the corporation is trying to protect with its enterprise information security RMP. It's critical to protect not just the computers and networks, but the vital information processed over them as well as the valuable resources supported by that information.

Countermeasures is a multidisciplinary concept. Seventeen security disciplines (physical, environmental, incident response, network, telecommunications, identification and authentication, audit, electronic media, software, management, the Web, encryption, directory/file permissions, anti-virus measures, personnel, procedures, and hardware) should be integrated into a

comprehensive countermeasure mix. These countermeasures encompass the spectrum of security philosophies that must be considered to adequately address protection of critical resources as well as a wide variety of threats facing enterprises today.

The third concept—the threat—drives all security programs. Threats are any capability, circumstance, or event (that is, a combination of threat mechanism and threat agent) with the potential to cause harm to a computer system or activity in the form of destruction, unauthorized disclosure, modification of data, or denial of service. Note, however, that the existence of a threat does not mean that it will necessarily cause harm to an enterprise's critical resources. The actual execution of a specific threat, directed at a specific asset or resource through a known vulnerability is what causes the damage to resources. If an integrated security RMP does not consider these targeted threats, then it is likely that gaps in security coverage will exist.

RMP Cornerstones

To obtain budgetary funding, garner enforcement support for your policies, and hire qualified security professionals to execute your security program, security RMPs should possess the following key corporate buy-in philosophies:

- executive commitment: this commitment is usually obtained through a series of initial one-on-one meetings with each key decision-making executive and then developing a communications plan to more effectively present how information security can enable healthcare operations and facilitate e-health initiatives
- integrated security disciplines: without all security programs under one leader like the CSO, there will likely be inefficiencies in security viewpoint, conflicting agendas between the disparate security groups, and overspent funds as each security group maintains its own core administrative capabilities. Integrated security disciplines create a set of overlapping practices, methodologies, and architectures so attackers can't slip through the cracks
- risk management—not risk avoidance—via defined process: there is no way to stop 100 percent of all threats against an organization. It would be cost-prohibitive and would probably shut down computing capability. For that reason, risk avoidance is a suboptimal process. It's more realistic to assign priorities to the threats that could most significantly affect resources and then determine an acceptable level of risk from an operational standpoint. Those impacts an institution will not accept should be the basis for funding a security solution that will mitigate that threat completely or at least to a more acceptable level. For those impacts an organization can live with, more conventional risk assumption practices can be used. It is equally important to note that such risk management be a sustainable and repeatable process. If this process is not followed methodically, an RMP will be impeded by lack of follow-through, unidentified impacts, or too little or too much money spent on the wrong priority
- shared responsibility and accountability between IS and business functions: security is everyone's responsibility. It is a team function, therefore the responsibility belongs to all the stakeholders. IS supports the healthcare business, which means the business need has to be expressed from the viewpoint of the institution's key medical and administrative leadership
- risk identification and assumption: a facility will have to be able to identify all the risks facing it as well as determine which risks will simply have to be tolerated versus active development of mitigating countermeasures

The RMP is a dynamic and cyclic process. In other words, an organization can't simply install a firewall and then forget about security, because there will constantly be new threats and countermeasures that will have to be considered and factored into the existing security matrix. The overall RMP requires you to:

- determine your baseline security needs and policy
- assess impacts of threats
- prioritize risks of impacts
- implement effective security enhancements based on priority
- manage the process

Security Enables Healthcare

When constructing a security program, remember that IT security and traditional corporate security are only parts of the solution. An integrated approach is needed for an effective risk management program. Additionally, when selling security to senior executives, don't present it as a cost center. Security is not insurance. Rather, it enables healthcare operations and e-commerce initiatives. Indeed, it can open new avenues of business cash-flow opportunities.

Lew Wagner (lwagner@mdanderson.org) is chief information security officer, information security department at the University of Texas MD Anderson Cancer Center.

An Ideal Security Department

Based on the planning/designing/implementation/operation (PDIO) model from industry best practices, the organizational makeup of a security department should consist of the following layers:

operations: department members handle the daily reading of security system logs, user account maintenance, and being the first tier of the security operations center and help desk

implementation: senior technical administrators are responsible for taking security architectural prototypes and implementing them across the institution as well as maintaining the operational security systems

architecture: department members match the needs of the institution with its threat profile as well as the key security technologies that are available to mitigate the risks of such threats to an acceptable level. This results in selection, design, and prototyping of security tools

management: the CSO serves as executive liaison to coordinate and mentor strategic security direction for the healthcare institution. Also includes security department managers who execute yearly goals to fulfill those strategic directions

The primary purpose of a security department is not to be a reactive entity, that is, only responding when an illegal or unauthorized event occurs, but rather to be a more proactive security support service. A security department is effective when its members are perceived as agents or internal consultants to help institutional divisions and departments accomplish their healthcare goals by providing security solutions. In any situation, people will respond better if they are approached as a shareholder in any security solution. By approaching your healthcare professionals in this manner, you ensure their buy-in because they will see you are basing the security solution on their business need.

Top Six Security Risks

The first step in an RMP is identifying the risks facing your healthcare organization. Then, determine which risks have the greatest effect on your operations. Finally, these risks must be prioritized: the “acceptable level of risk” will determine how an institution allocates remediation resources and safeguards to mitigate impacts of higher risks to a more acceptable level.

The top six security risks to critical information and resources are:

- **the Internet**: a connection to the outside
- **telecommuting**: potentially weak home system security
- **host**: vulnerabilities inherent in operating systems
- **network**: potential ethernet insecurities
- >**desktop**: users potentially modifying files
- **security awareness**: users’ level of awareness

Lew Wagner (lwagner@mdanderson.org) is chief information security officer, information security department at the University of Texas MD Anderson Cancer Center.

Article citation:
Wagner, Lew. "Uniting Security Forces Against Risk." *Journal of AHIMA* 73, no.6 (2002): 39-42.

Driving the Power of Knowledge

Copyright 2022 by The American Health Information Management Association. All Rights Reserved.