OPEN SECURITY EXCHANGE™

Security Convergence Roadmap

2008

Table of Contents

Reviewers & Contributors 3
Official Sponsors 4
1 Executive Summary 5
2 Background – Physical Security 6
3 Background – IT Security 6
4 The Coming of Physical/IT Security Convergence 7
5 Convergence Roadmap^{SM} for Security Practitioners 8
5.1 Top Convergence Roadmap Goals: 10
6 The Business Case for Convergence 10
6.1 Compliance 10
6.2 Asset/Personnel Protection 11
6.3 Business Development 11
6.4 Cost Control/Productivity 12
7 my Convergence Roadmap 14
7.1 my Organization's Business Driver 14
7.2 my Organization's Strategic Milestones 15
7.3 my Organization's Tactical Milestones 16
7.4 my Organization's Operational Milestones 17
7.5 my Convergence Roadmap 18
8 Convergence Roadmap Case Study – Baxter Healthcare 19
8.1 Adding Business Value 19
8.2 Security Workflow Automation 21
8.3 Discovering Lean 21
8.4 Security Command Post: a Lean Opportunity 22
8.5 Reaching Out Across the Business 22
8.6 Keeping People in the Equation 22
9 About the Open Security Exchange 24

Reviewers & Contributors

OSE Convergence Roadmap Team

Organization	**Name(s)**
Quantum Secure, Inc.	Vik Ghai, Laurie Aaron
HID/Fargo	Gary Klinefelter, Greg Sarrail
Koffel Associates	Shayne Bates

OSE Convergence Council Members

Organization	**Name(s)**
First Data Corp.	Adam Stanislaus
Defense Manpower Data Center	Bob Gilson
National City Corp.	Gareth Webley
Symantec Corp.	Sreeni Kancharla
Lehman Brothers	Michael Engle
Baxter Healthcare - Cherry Hill, New Jersey	Derrick Wright, CPP

Other

Organization	**Name(s)**
Mateusa	John Szczygiel
N2N Secure	James Connor

Official Sponsors

Organization		Website
OPEN SECURITY EXCHANGE	Open Security Exchange	www.opensecurityexchange.com
QUANTUMSECURE the power to converge	Quantum Secure, Inc.	www.quantumsecure.com
HID	HID Global Corporation	www.hidcorp.com
tyco SOFTWARE HOUSE	Tyco Software House	www.swhouse.com

1 Executive Summary

Today’s security initiatives involve guarding buildings and equipment as well as protecting networks, dealing with privacy issues, and managing risk. Given the interrelated aspects of these initiatives, the question has always been, “How can I make physical and IT Convergence happen?" Until now, in most organizations, physical access systems and information access systems have operated as two independent structures, and have been run by completely separate departments. Information access, which grants admission to the IT infrastructure such as the intranet/internet, mail servers, web servers, and database applications, was run by the IT department. The facilities department controlled physical access systems, which includes the providing employee badges, controlling access to buildings, and life safety systems, e.g., HVAC, Fire and CCTV.

The Open Security Exchange (OSE) Convergence Roadmap describes a clear and easy to follow path to converge with greatest positive effect and recommends best pratice steps in this direction. The roadmap includes lessons learned, guidance and insights from first movers that have taken the initiative to converge physical security and IT. The roadmap identifies business drivers and strategic plans to achieving the numerous business goals of security convergence.

2 Background – Physical Security

Physical security seeks to prevent or deter attackers from accessing a facility, resource or physical equipment. It can be as simple as a locked door or as elaborate as multiple layers of armed guard posts.

Physical security systems control access to enterprise facilities based on time frame, access role and other similar conditions. A typical infrastructure consists of:

- Environmental design
- Mechanical and electronic locks
- Intrusion detection
- Video monitoring
- Physical access control such as card readers, or biometric readers (i.e., iris scans, facial recognition, palm/thumb readers)
- Physical blockade and locking mechanisms, e.g., electromagnetic locking devices
- Fire control and suppression systems such as sprinklers, smoke detectors, CO detectors
- Life support systems

These systems may interact with each other using network services deployed by the IT department. This for example, allows the door reader to be tied to the fire protection system that in turn is connected to the CCTV system, which is monitored by the physical security system. Physical security focuses on the protection of assets, people and structure against perceived threats. Furthermore, monitoring and managing the flow of individuals and assets throughout the premises is another important aspect of physical security. Managing access methods, perimeter intrusion, and tenancy are all issues that must be dealt with on a daily basis when monitoring physical access.

3 Background – IT Security

Information Technology (IT) security seeks to protect network and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. The terms information security, computer security and information assurance are frequently used interchangeably. These fields are interrelated and share the common goals of protecting the confidentiality, integrity and availability of information; however, there are some subtle differences between them. These differences lie primarily in the approach to the subject, the methodologies used, and the areas of concentration. Information security is concerned with the confidentiality, integrity and availability of data regardless of the form the data may take: electronic, print, or other forms. In a general sense, IT security controls the ability of on-line actors to interact with information objects. It is difficult to talk about IT security without talking about the on-line identities of the actors. This brings us to the concept of identity management.

3.5 Identity Management could be a separate section

Identity management as the "set of processes, tools and social contracts governing the life cycle of a digital identity for people, systems and services to enable secure access to an expanding set of systems and applications." Identity management is a core component of IT security environments and refers to administering account information for login access to systems and applications. Based on this definition an Identity Management System consists of the following interdependent elements:

- Data Storage – the logical repository and data model structure, often implemented in the form of a directory, holding policy information and data access usage
- Authenticator – is responsible for performing the authentication (verifying the identity) of a user associated with a given identity. These include passwords, biometrics, or X.509 PKI certificates
- Policy control – defines who has access to what information and under what conditions
- Auditing – tracks and records the flow of information when data is created, used and changed.
- Single-Sign on – allowing a user to perform primary authentication once to access the set of applications and systems that are part of the identity management environment
- Personalization – associating an application and information to an identity
- Access management – allowing applications to make authorization and other policy decisions based on privilege and policy information.

The identity management system forms a primary building block of an IT security system. The components interact with the services to grant access to corporate IT resources such as e-mail, database permissions, web access, and intranet/internet connectivity. Authentication becomes the mechanism to grant access to these resources relying on directories and access control policies to determine who has access to what resources. A key driving force for such a system is improving the user experience both from an administration and end-user perspective to improve efficiency and compliance.

4 The Coming of Physical/IT Security Convergence

Today, virtually all organizations with physical and IT assets protect those assets in a variety of ways. There are alarm systems to protect facilities and their contents from unlawful entry. There are firewalls to stop intrusion into corporate networks. Assets may also be safeguarded by the use of employee ID badges, software application passwords and a growing number of technologies, from magnetic cards and readers to biometric finger readers. The scope of security systems spans physical access, information access, video surveillance, storage, identity management, and more.

While all of these security technologies share a common purpose, those that protect physical assets and those that protect IT assets have virtually nothing else in common. They have always existed in parallel, evolving separately and residing under the control of separate organizations. This has resulted in a lack of integration and interoperability between physical and IT security systems. With today's heightened security concerns, this lack of integration is no longer simply an inconvenience. It increases security risks by preventing technologies from working in concert with one another. It limits corporations' efforts to establish centralized control of security and develop integrated risk management strategies. It prevents coordinated responses to security breaches by physical and IT security systems. With no integration between physical and IT security systems, organizations cannot pursue cost synergies, fully address privacy issues, or ensure compliance with a growing number of government and industry regulations. The solutions to these problems will come from the convergence of physical and IT security technologies. In other words, convergence makes good business sense.

The need to cut costs is another driving factor for this convergence. According to the Gartner Research firm, the integration of the budgets for physical and IT security can deliver substantial efficiency, particularly if provisioning is used. Corporate mergers also contribute to this paradigm shift. One visible outcome from the union of multinational organizations is the need for a multi-purpose common identity in the form of the corporate badge. This “standard” badge is designed to provide what has become known in the industry as “global roaming” where a single card is used to access all the facilities worldwide depending on the authorizations granted. Moreover, by combining multiple physical access systems organizations can yield significant cost savings.

Improving efficiencies is yet another factor driving this alliance. By managing the entire credential life cycle of the employee, the enterprise can control when the employee was badged, what buildings/facilities they have access to, what systems they can access and most important what happens when an employee is terminated, leaves or is transferred. The efficiencies become even more compelling when a common data repository is used for all identity related information. The data is entered into the system once and then replicated throughout the organization. This allows for common administration of users, privileges, and credentials—across the physical as well as IT realm—and means less effort and fewer possibilities for oversights or omissions whenever an employee is hired, leaves, or has a change in access permission.

Physical/IT security convergence will enable vendor-neutral interoperability among diverse security components to support overall enterprise risk management needs. As physical and IT security merge, networked computer technology and associated applications will provide enterprises with increased operational efficiencies and intelligent security.

5 Convergence Roadmap^{SM} for Security Practitioners

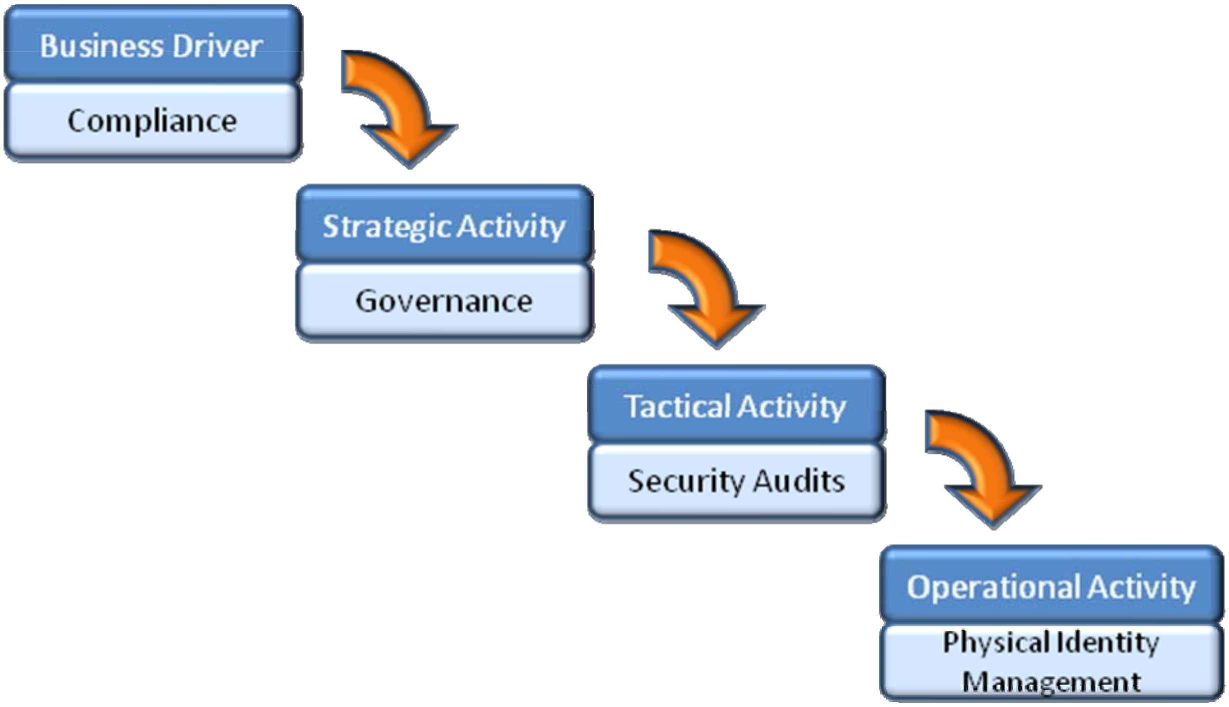
Recognizing the need for definitive guidance on Security Convergence, the OSE initiated a project to develop a conceptually sound framework providing integrated security principles, common terminology and best practice guidance supporting any organization’s security programs to develop or benchmark their converged processes.

A related objective is for this resulting roadmap to serve as a common basis for executives, directors, regulators, academics and others to discuss converged security management. The Convergence Roadmap illustrates benefits and limitations and provides a way to effectively communicate enterprise security management strategy.

The underlying premise of enterprise risk management is that every organization, whether for-profit, not-for-profit, or a governmental body, exists to provide value for its stakeholders. All organizations face uncertainty, and the challenge for management is to determine how much uncertainty to accept as it strives to grow stakeholder value. Uncertainty presents both risk and opportunity, with the potential to erode or enhance value. The Convergence Roadmap provides a framework for management to effectively deal with uncertainty and associated risk and opportunity and thereby enhance its capacity to build value.

Working together with its Convergence Council members, a group of senior security and IT executives from blue chip organizations, the OSE Roadmap Team has defined a reusable model, definitions, and tool to enable organizations to advance convergence.

In best practice the Security Practitioner should focus on their organization's "Business Drivers". Unless a security department's objectives are aligned with an organization's objectives – IT & Physical Security Convergence initiative will be difficult to achieve. The OSE Convergence Roadmap tool helps Security Practitioner think about convergence with regard to organization's business drivers and provides a detailed roadmap with tactical linkage of strategic objectives and operational capabilities. The goal is to help align your security department's operational activities, strategic direction with your business value. The figure below provides an example –



The Convergence Roadmap is a multi-faceted tool that provides personalized, illustrative, diagnostic, and theoretical aids to support convergence. The Convergence Roadmap includes taxonomy and definitions associated with convergence, and will be agnostic to an organization's current convergence status.

5.1 Top Convergence Roadmap Goals:

- Aligning Security with Corporate Business Goals
- Recruiting and Retaining Security Staff
- Measuring Security Organization Efficiency
- Using Security for Competitive Breakthroughs
- Reducing Security Costs
- Demonstrating Business Value of Security
- Developing an long term Security Architecture
- Improving Security Delivery

6 The Business Case for Convergence

Every organization has its own security needs, concerns and business goals. To begin identifying and prioritizing your organization's key convergence goals is necessary to consider common business drivers and their relationship to security convergence.

Risk management is a common security-related business driver. Therefore, risk assessment techniques are very useful tactful tools to use to help identify and prioritize an organization's security agenda. A risk assessment enables a company to identify scarce resources and the most likely and potentially damaging threats.

Among the most common business drivers are the following:

6.1 Compliance

The requirement to comply with certain mandatory actions and outcomes is common to IT and physical security, and is therefore a candidate for a converged approach. This driver involves staying abreast of changes in the requirements themselves, communicating the requirements to the organization, detecting and correcting any non-compliance, capturing and organizing an effective audit trail, and periodic reporting to the appropriate authorities. All of this must be achieved at the minimum possible cost without sacrificing compliance or making a negative impact on performance.

Besides enterprise-wide compliance needs, certain operations, departments, or divisions within a facility may have their own, more stringent compliance requirements. An interpretation of a compliance/regulatory requirement should first consider the group with the highest level of risk and use this group as a base line for the remaining groups. For example, in the financial services industry, it is not unusual for a retail bank to share a facility with a mortgage origination operation and a securities brokerage division. By addressing the most stringent security requirements among these groups, organizations can ensure better security for all.

Compliance factors include:

- Regulations. These are government or industry relatesd mandates, examples include: Sarbanes-Oxley, employment and privacy laws (SOX), Homeland Security Presidential Directive 12 (HSPD-12), Payment Card Industry (PCI), Drug Enforcement Administration (DEA), Food and Drug Administration (FDA), and the Health Insurance Portability and Accountability Act (HIPAA).

- Policy and procedure. These are the fundamental, internal requirements, typically related to and driven by Human Resources.
- Workforce security awareness. It is essential that all members of the workforce understand that security is everyone's responsibility, not just the responsibility of the security professionals.

6.2 Asset/Personnel Protection

Both physical and IT security systems are designed to protect an organization's revenue producing assets -- including people, equipment, products, tools, and information. Organizations need to understand which assets need to be protected and what level of assurance is required, then organizations must develop and operate a mechanism to grant access to those assets. While user authentication is important, they also need to monitor and analyze access (both historical and real-time), and ensure a timely response to inappropriate behavior.

Typical asset and personnel protection factors include:

- Authentication. Organizations need to determine whether a person, computer, or web site is indeed who or what they claim to be, and find a convenient and secure means to enable such determination..). Authentication is accomplished via the presentation of an identity and credentials. Examples of different types of credentials include badges, username/passwords, one-time tokens and digital certificates. The level of trust placed in establishing a user's identity should match the value of the assets being protected.
- Authorization. This is the process of granting appropriate access to assets based on the established identity, role and/ or other attributes. Authorization may be limited based on certain restrictions such as time of day, physical location or multiple simultaneous login attempts by the same user. access based on the time of day. Organizations need to make sure that the required access to assets is granted in a timely manner, that the access is properly monitored, and that they can respond effectively to inappropriate access attempts.
- Integrity (non-repudiation). This means having the ability to trust -- and prove the authenticity and change history of -- tangible and information assets. Examples include being able to prove a signature on a wire funds transfer, that particular users accessed certain information at a particular time or that a security videotape has not been altered.
- Brand equity/goodwill. This is a special class of asset protection that often merits special attention from both IT and physical security. It strives to assure that the public's trust in the organization and its products and services is not damaged through lapses in security.
- Personnel protection and life safety. Involves traditional executive protection, insuring a crime and offense-free workplace, and the ability to account for and assist personnel in emergencies.

6.3 Business Development

Most organizations treat both physical and IT security as a necessary cost of doing business, not a revenue or profit enhancer. It is difficult to quantify the business-building benefits derived from having employees who feel safe in their work environment, even though everyone would intuitively agree that the benefits are there. More and more today both IT and physical security practitioners are expected to recast and enhance their mission statement to include business value goals. Often this means transforming security from solely a cost center to a center for business efficiency. This may involve the acceleration of business decision-making and other management processes can help the organization capture opportunities for productivity. By combining best-of-breed practices and solutions across physical and IT disciplines security professionals can achieve a stronger business posture.

Key business value security factors include:

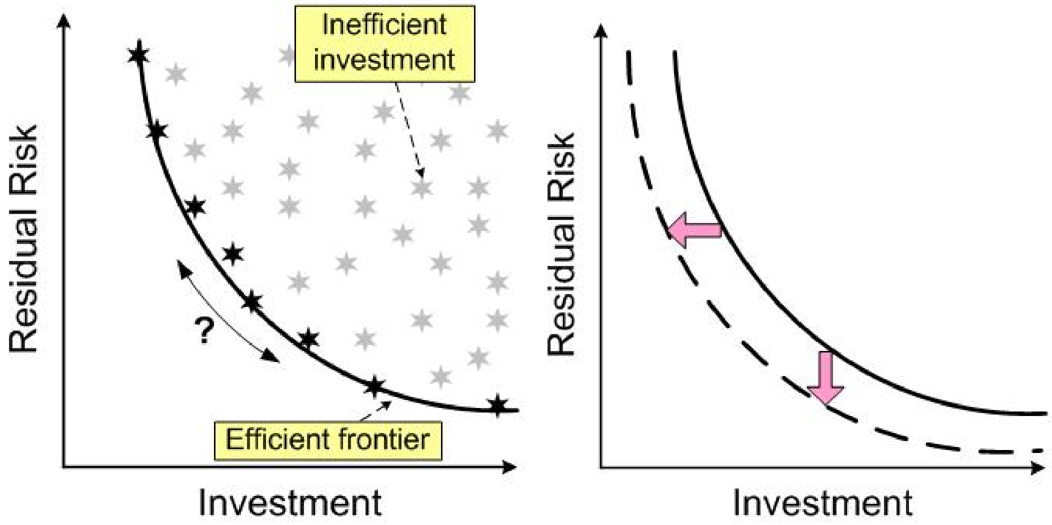
- New business models. Security measures must be able to keep an organization's assets secure while new business models such as outsourcing, contract manufacturing, partnerships, or other joint ventures are pursued.
- Mergers and acquisitions. Organizations need to be prepared to quickly assimilate another organization's security structure and IT processes
- Business continuity. By sharing best practices across IT and physical security, organizations can ensure that normal operations (and thus, revenue streams) can be restored more quickly after a loss event. These measures may also decrease the likelihood of the loss itself.

6.4 Cost Control/Productivity

Both IT and physical security require investment to lower risk. One can think of an "efficient frontier" curve on a graph of security investment versus risk, with each point on the curve representing the lowest risk for a given investment and/or the lowest cost for a given level of risk. Not only do IT and physical security professionals strive to operate on this most efficient frontier, they also strive to move this curve by lowering costs for all levels of risk. Once again, combining best practices and solutions from both physical and IT security can help make this happen.

Cost control and productivity factors include:

- Convenience and usability. When day-to-day secure behavior is effortless, it increases user productivity. Examples include making it easy to securely obtain or reset credentials, enterprise single sign-on, ease of requesting and granting access to assets (doors, servers, etc.), and the use of badges for cashless payment at facility cafeterias. The security goal is to allow a worker to go to from the street to a desk and be logged on to a company's network with as little effort as possible without compromising security.
- Process reengineering. This refers to efforts to drive efficiency into all security-related processes, such as incident response, security monitoring, credentialing, policy-making and exception granting, governance, vulnerability testing, security auditing, and reception.
- Workflow automation. By applying automation to the processes listed above, an organization may be able to shorten cycle time, eliminate human errors, and reduce effort.
- Workforce optimization. When an organization realizes greater efficiencies in security, it may reduce resource requirements or enable the reassignment of personnel to more strategic, business-building activities.

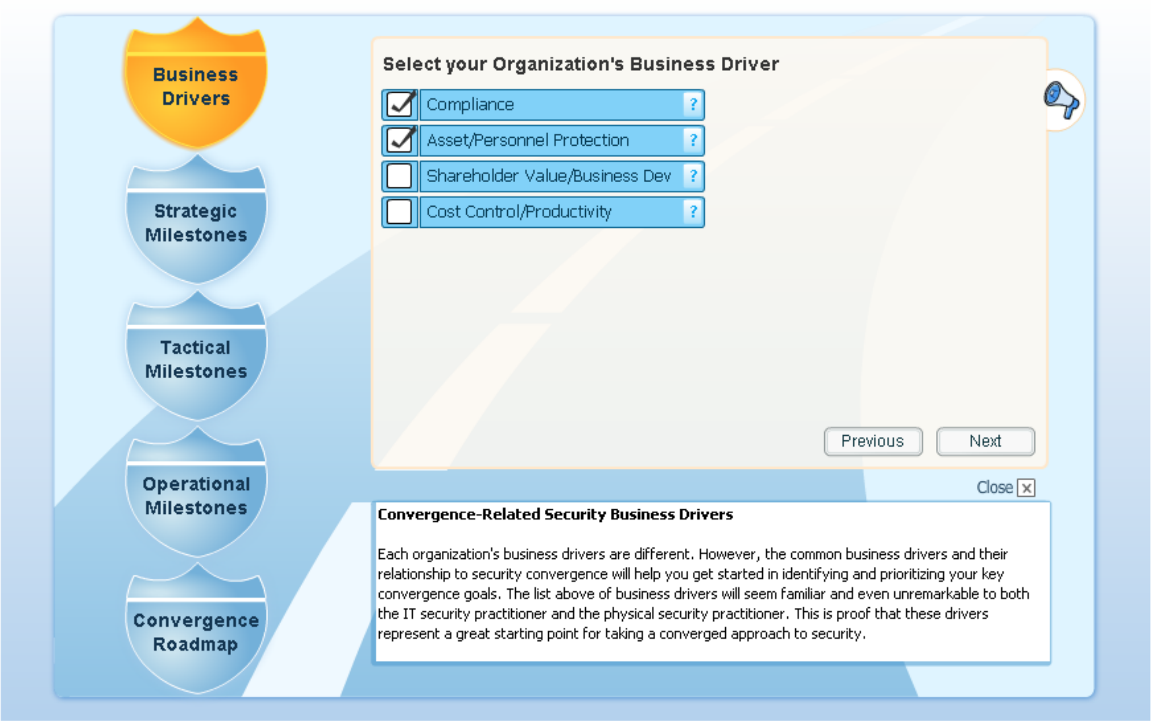

Inefficient investment
Residual Risk
?
Efficient frontier
Investment
Residual Risk
Investment

7 my Convergence Roadmap

7.1 my Organization's Business Driver

Each organization's business drivers are different. However, the common business drivers and their relationship to security convergence will help you get started in identifying and prioritizing your key convergence goals. The list of common business drivers will seem familiar and even unremarkable to both the IT security practitioner and the physical security practitioner. Considering this common ground these drivers are a great starting point for taking a converged approach to security.

OSE Convergence Roadmap



Select your Organization's Business Driver

- ☑ Compliance ?
- ☑ Asset/Personnel Protection ?
- □ Shareholder Value/Business Dev ?
- □ Cost Control/Productivity ?

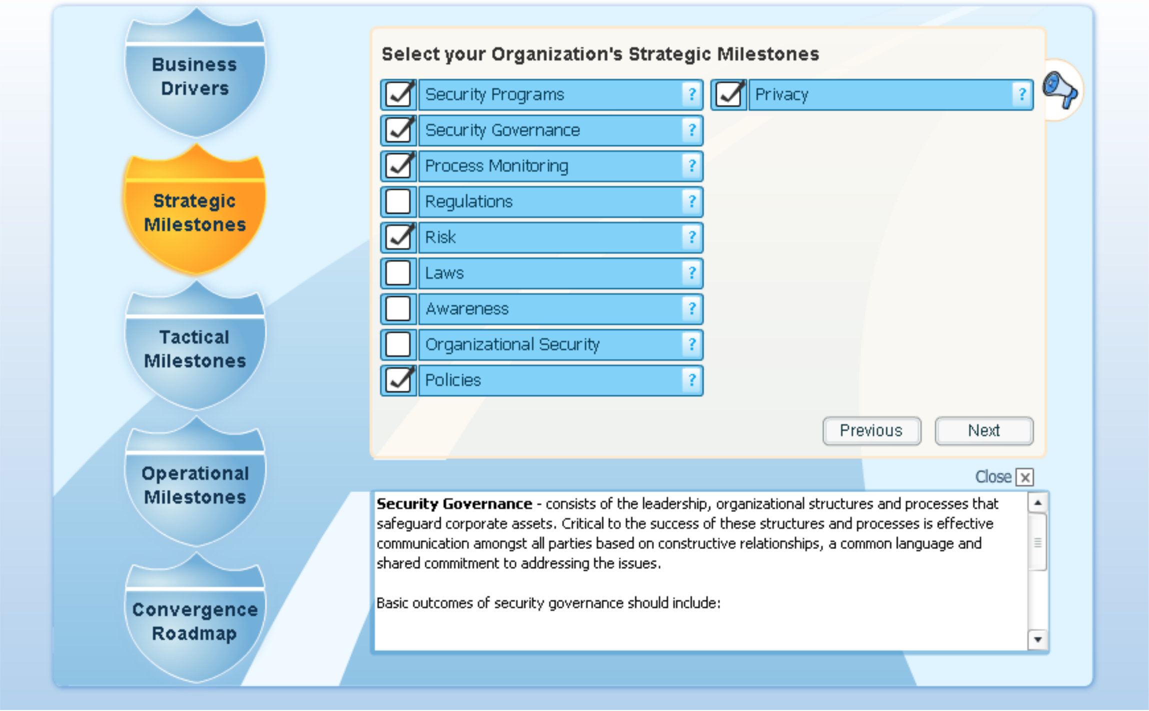
Convergence-Related Security Business Drivers

Each organization's business drivers are different. However, the common business drivers and their relationship to security convergence will help you get started in identifying and prioritizing your key convergence goals. The list above of business drivers will seem familiar and even unremarkable to both the IT security practitioner and the physical security practitioner. This is proof that these drivers represent a great starting point for taking a converged approach to security.

7.2 my Organization's Strategic Milestones

Strategic Milestones - The Strategic Milestones are critical in that they frame much of the milestones that follow. Strategic Milestones are those that uniquely define your security organization's character and are fundamental to the success of your security operations.

OSE Convergence Roadmap



Select your Organization's Strategic Milestones

☑ Security Programs ?
☑ Security Governance ?
☑ Process Monitoring ?
□ Regulations ?
☑ Risk ?
□ Laws ?
□ Awareness ?
□ Organizational Security ?
☑ Policies ?
☑ Privacy ?

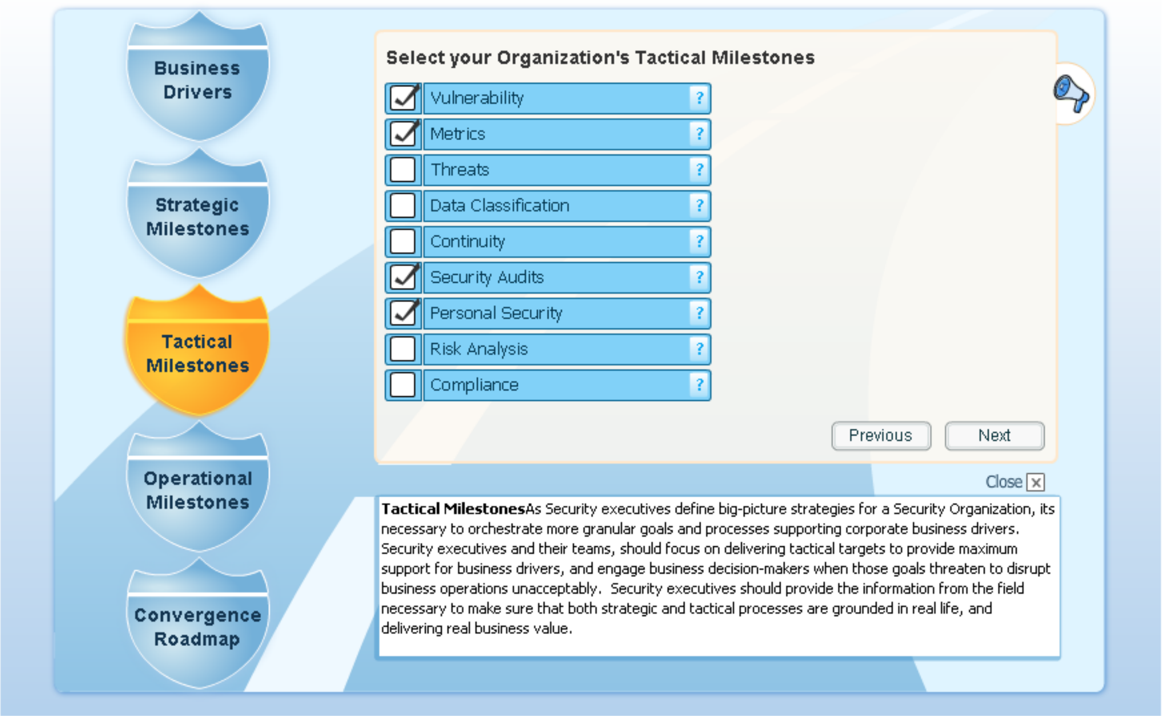
Security Governance - consists of the leadership, organizational structures and processes that safeguard corporate assets. Critical to the success of these structures and processes is effective communication amongst all parties based on constructive relationships, a common language and shared commitment to addressing the issues.

Basic outcomes of security governance should include:

7.3 my Organization's Tactical Milestones

Tactical Milestones - As Security executives define big-picture strategies for a Security Organization, it is necessary to orchestrate more granular goals and processes supporting corporate business drivers. Security executives and their teams should focus on delivering tactical targets to provide maximum support for business drivers, and engage business decision-makers when those goals threaten to disrupt business operations.. Of course it is critical that Security Executives gather enough information from the field to make sure that both strategic and tactical processes are grounded in real life, and that they are delivering real business value.

OSE Convergence Roadmap



Select your Organization's Tactical Milestones

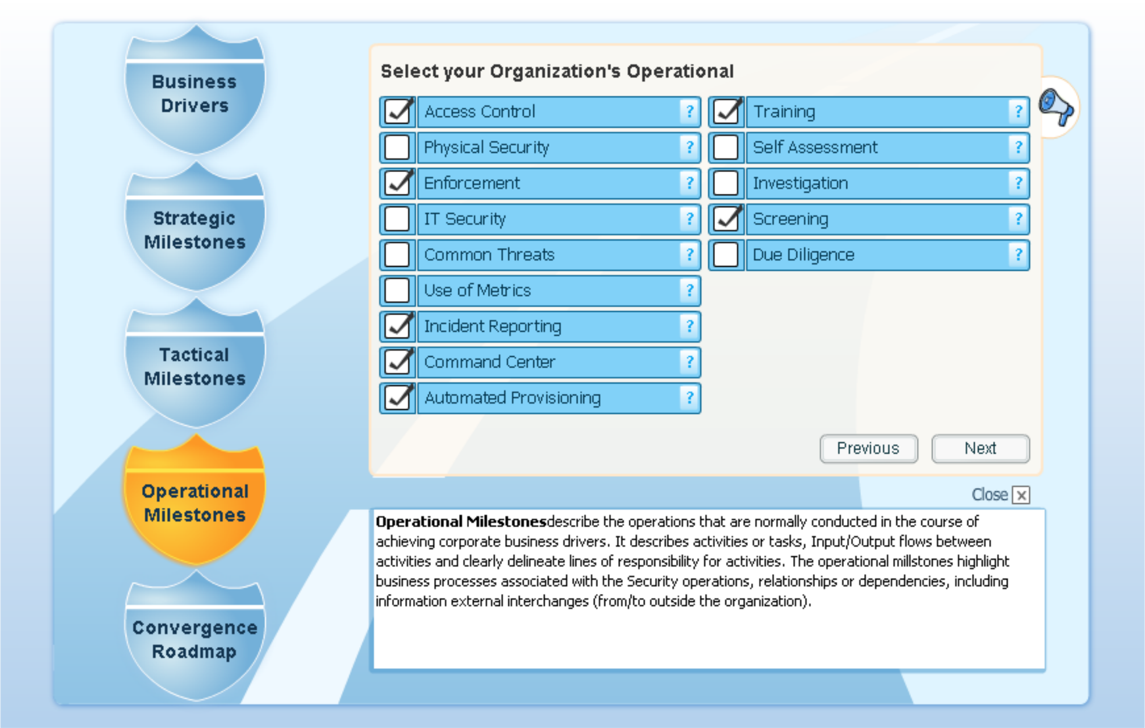
- ☑ Vulnerability ?
- ☑ Metrics ?
- ☐ Threats ?
- ☐ Data Classification ?
- ☐ Continuity ?
- ☑ Security Audits ?
- ☑ Personal Security ?
- ☐ Risk Analysis ?
- ☐ Compliance ?

Tactical Milestones As Security executives define big-picture strategies for a Security Organization, its necessary to orchestrate more granular goals and processes supporting corporate business drivers. Security executives and their teams, should focus on delivering tactical targets to provide maximum support for business drivers, and engage business decision-makers when those goals threaten to disrupt business operations unacceptably. Security executives should provide the information from the field necessary to make sure that both strategic and tactical processes are grounded in real life, and delivering real business value.

7.4 my Organization's Operational Milestones

Operational Milestones describe the operations that are normally conducted in the course of achieving corporate business drivers. It describes activities or tasks, Input/Output flows between activities and clearly delineates lines of responsibility for activities. The operational milestones highlight business processes associated with the Security operations, relationships or dependencies, including information interchanges (from/to outside the organization).

OSE Convergence Roadmap



Select your Organization's Operational

☑ Access Control
☐ Physical Security
☑ Enforcement
☐ IT Security
☐ Common Threats
☐ Use of Metrics
☑ Incident Reporting
☑ Command Center
☑ Automated Provisioning

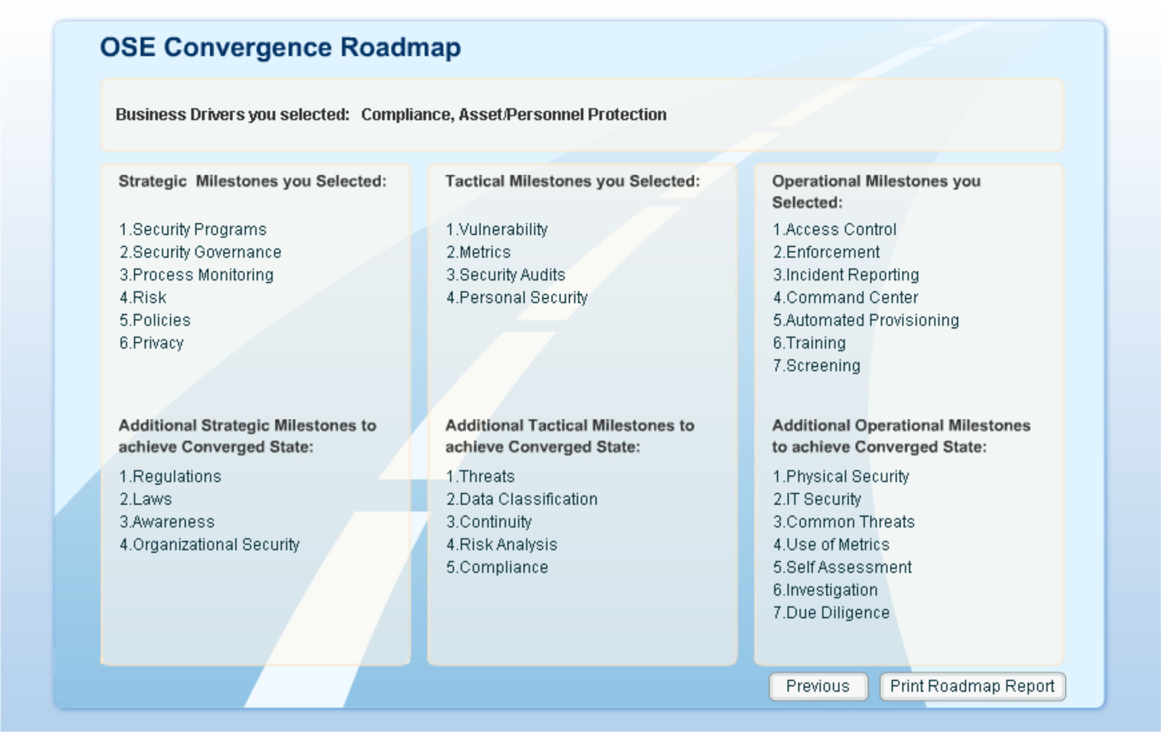
☑ Training
☐ Self Assessment
☐ Investigation
☑ Screening
☐ Due Diligence

Operational Milestonesdescribe the operations that are normally conducted in the course of achieving corporate business drivers. It describes activities or tasks, Input/Output flows between activities and clearly delineate lines of responsibility for activities. The operational millstones highlight business processes associated with the Security operations, relationships or dependencies, including information external interchanges (from/to outside the organization).

7.5 my Convergence Roadmap

OSE Convergence Roadmap – helps identify the proper business reasons for implementing a converged security approach. Cost control, productivity, compliance, asset and personnel protection, and revenue enhancement are clear, measurable reasons that when coupled with your unique requirements will help define a clear roadmap for convergence.. By helping identify security gaps caused by separate approaches to IT systems and physical security systems, the convergence roadmap demonstrates the transition plan needed to bridge the gaps. This transition plan can be easily implemented by capitalizing on the unique expertise, experience, and perspective that physical and IT security functions each bring to the organization.

OSE Convergence Roadmap



OSE Convergence Roadmap

Business Drivers you selected: Compliance, Asset/Personnel Protection

Strategic Milestones you Selected:

1.Security Programs
2.Security Governance
3.Process Monitoring
4.Risk
5.Policies
6.Privacy

Additional Strategic Milestones to achieve Converged State:

1.Regulations
2.Laws
3.Awareness
4.Organizational Security

Tactical Milestones you Selected:

1.Vulnerability
2.Metrics
3.Security Audits
4.Personal Security

Additional Tactical Milestones to achieve Converged State:

1.Threats
2.Data Classification
3.Continuity
4.Risk Analysis
5.Compliance

Operational Milestones you Selected:

1.Access Control
2.Enforcement
3.Incident Reporting
4.Command Center
5.Automated Provisioning
6.Training
7.Screening

Additional Operational Milestones to achieve Converged State:

1.Physical Security
2.IT Security
3.Common Threats
4.Use of Metrics
5.Self Assessment
6.Investigation
7.Due Diligence

8 Convergence Roadmap Case Study – Baxter Healthcare

Convergence Leader	Derrick Wright
Convergence Business Drivers	Compliance, Cost Reduction, Business Development
Site	Baxter Healthcare, Cherry Hill, NJ
Date	Feb 2007 – June 2007

Baxter Healthcare (Baxter) is a global medical products and services company with expertise in medical devices, pharmaceuticals and biotechnology. Baxter's (375,000) square foot facility located in Cherry Hill, N.J., produces a wide range of sterile injectables, allowing the company to ensure that its customers have a dependable and uninterrupted supply of products. The Security department at Baxter Healthcare Cherry Hill, NJ utilized OSE Convergence Roadmap to build a different and unique approach to the security operations.

8.1 Adding Business Value

The overriding principle of Baxter Cherry Hill's Security Department is, *"How can we add value to this business?"* The entire security administration team is focused on this principle. This aligns highly with the *lean* world. The first principle in *lean* thinking (Jim Womack, 1996) is the concept of value from the customers' perspective; always considering what the customer is willing to pay you to do.

When Baxter Cherry Hill's security administration team began their Security Master Plan, they started the planning process by interviewing their primary customers – the internal management team of the plant. First they worked with their customers to identify the critical assets in each area of the business. Next they consulted with them about the potential threats to those critical assets.

In determining what security measures to employ (people, process and technology) the security team worked with this question in mind, "*How can we align security operations with the goals and objectives of this business?*" Again, this ties into *lean* as all support functions are helping to add value to the customer through the entire value stream. The security administration team identified four key business drivers that impact security operations:

1. ***Compliance***. Some security requirements derive from federal, state and local laws. Others derive from corporate policies including those concerning privacy, ethics and business practices. There are also corporate IT standards to which the security systems technology must comply. As this facility manufactures small-volume injectable medications, federal compliance requirements include FDA and DEA regulations that apply to the handling of the pharmaceutical ingredients from initial receipt through manufacturing, to warehousing and shipping. Fire regulations and building codes provide

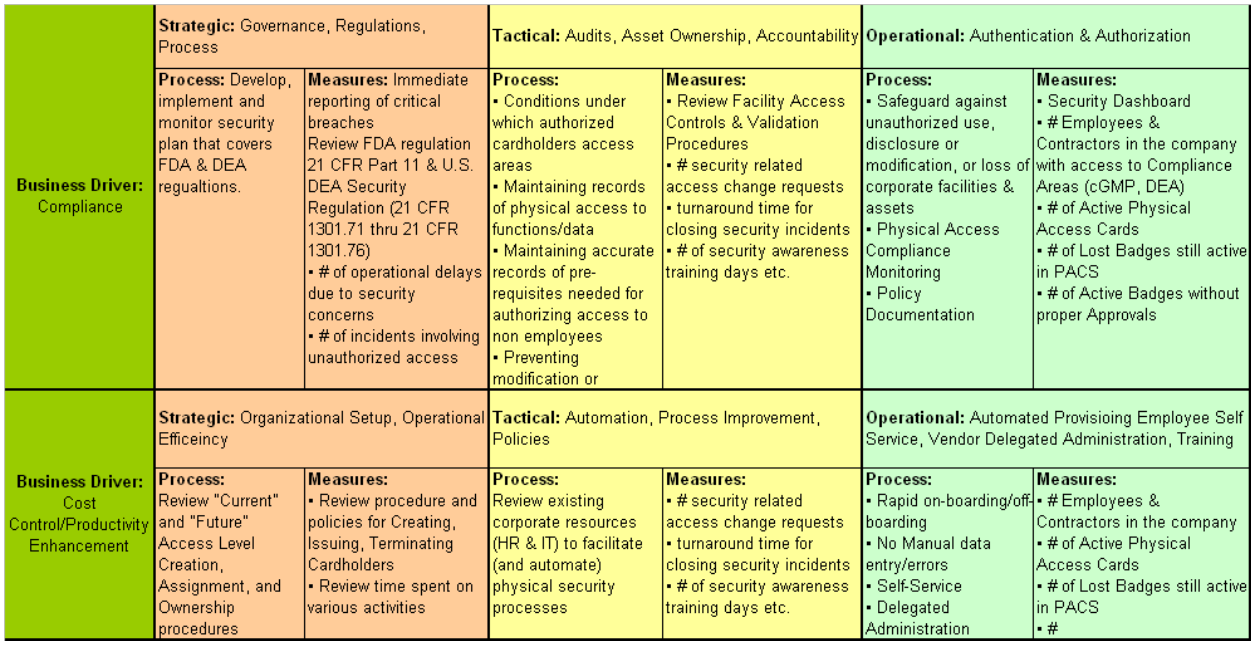
additional compliance requirements. Additionally there are voluntary compliance items such as the National Fire Protection Association's standard, NFPA 731, for the quality of security system installations, as well as NFPA 730 that deals with the establishment of a basic security program. Finally, there are risk assessment guidelines from ASIS International (originally the American Society for Industrial Security).

2. ***Risk Management.*** Security is a *risk management* function. Risk Management is a business function that involves the identification and acceptance or offsetting of risks that threaten the profitability or productivity of an organization. There are many types of risk, including *Market Risk* and *Credit Risk*, but many business risks fall under the general category of *Operational Risk*. Operational Risk is the threat of loss resulting from inadequate or failed internal processes, people and systems, human error, management failure, or external events. *Security risk* is a subset of *operational risk*. Security risk is the risk of loss resulting from accidental, hostile or environmental threats against the critical assets of an organization including its people, material assets, systems and critical business processes. The job of security is not to eliminate all risks, but *to reduce security risks to acceptable levels, at an acceptable cost*. What level of risk is acceptable? What level of cost is acceptable? These are business decisions. Thus Security planning is business planning.

3. ***Fiscal Responsibility.*** Fiscal responsibility is a business driver that applies throughout all departments of an organization. The security team understands the competitive nature of the business and the need for ongoing cost management across the organization. Thus they have come to understand the value of applying *lean* concepts like 5S, Kaizen, and work flow (process) improvement.

4. ***Business Development.*** The security administration team asked the question, "*How can we help secure new business for this plant?*" They realized that a well documented and visibly well-run security program could be used as a tool to differentiate this plant from its competitors.

Derrick Wright mapped Baxter Healthcare's "Business Drivers" and aligned his security organization's objectives using the detailed roadmap. This also included brainstorming exercise on tactical linkage of strategic objectives and operational capabilities. The goal of this exercise was to align operational activities, strategic direction and come up with transition plan as illustrated below:



Business Driver: Compliance	**Strategic:** Governance, Regulations, Process		**Tactical:** Audits, Asset Ownership, Accountability		**Operational:** Authentication & Authorization	
	Process: Develop, implement and monitor security plan that covers FDA & DEA regualtions.	**Measures:** Immediate reporting of critical breaches Review FDA regulation 21 CFR Part 11 & U.S. DEA Security Regulation (21 CFR 1301.71 thru 21 CFR 1301.76) ▪ # of operational delays due to security concerns ▪ # of incidents involving unauthorized access	**Process:** ▪ Conditions under which authorized cardholders access areas ▪ Maintaining records of physical access to functions/data ▪ Maintaining accurate records of pre-requisites needed for authorizing access to non employees ▪ Preventing modification or	**Measures:** ▪ Review Facility Access Controls & Validation Procedures ▪ # security related access change requests ▪ turnaround time for closing security incidents ▪ # of security awareness training days etc.	**Process:** ▪ Safeguard against unauthorized use, disclosure or modification, or loss of corporate facilities & assets ▪ Physical Access Compliance Monitoring ▪ Policy Documentation	**Measures:** ▪ Security Dashboard ▪ # Employees & Contractors in the company with access to Compliance Areas (cGMP, DEA) ▪ # of Active Physical Access Cards ▪ # of Lost Badges still active in PACS ▪ # of Active Badges without proper Approvals
Business Driver: Cost Control/Productivity Enhancement	**Strategic:** Organizational Setup, Operational Efficeincy		**Tactical:** Automation, Process Improvement, Policies		**Operational:** Automated Provisioing Employee Self Service, Vendor Delegated Administration, Training	
	Process: Review "Current" and "Future" Access Level Creation, Assignment, and Ownership procedures	**Measures:** ▪ Review procedure and policies for Creating, Issuing, Terminating Cardholders ▪ Review time spent on various activities	**Process:** Review existing corporate resources (HR & IT) to facilitate (and automate) physical security processes	**Measures:** ▪ # security related access change requests ▪ turnaround time for closing security incidents ▪ # of security awareness training days etc.	**Process:** ▪ Rapid on-boarding/off-boarding ▪ No Manual data entry/errors ▪ Self-Service ▪ Delegated Administration	**Measures:** ▪ # Employees & Contractors in the company ▪ # of Active Physical Access Cards ▪ # of Lost Badges still active in PACS ▪ #

8.2 Security Workflow Automation

A key strategy of the Security Master Plan is to deploy an enterprise security system that enables:

- *Centralized physical identity management* for employees, contractors and visitors
- *Role-based access management* for facility access
- *Self-service administration* for security services (for example, for facility access changes and the facility's area work permit process)
- *Real-time FDA/DEA compliance enforcement* for access to regulated areas of the facility

Thus the Baxter Cherry Hill Security Department uses Quantum Secure's SAFE, a software suite providing security operations workflow automation. SAFE provides rules-based monitoring and enforcement of compliance requirements, and integration between security processes (such as facility access management) and business processes (such as on-boarding and off-boarding of employees and contractors). Security Manager Derrick Wright explained, "Other business departments began years ago to deploy information technology to improve business process management and business efficiency. It's time that security departments followed suit."

8.3 Discovering Lean

The entire security administration staff looks for opportunities to reduce waste for security operations. The best part is they have done this with limited training. Wright attended a value stream-mapping event for one Baxter product family in the fall of 2006 and saw the very visual over-abundance of activity in the information flow, and how it was improved. Wright began to ask, "How can we similarly improve security operations, including our interactions with other departments?" After that, the security team has been involved in other Kaizen events and lean training. One team member, Molly Stager, was a member of the first Baxter Cherry Hill 6S Kaizen team (the 6th S is for safety) and has led the team to utilize 6S in the security work areas.

8.4 Security Command Post: a Lean Opportunity

The security command post has become a model 6S workplace, and the initial improvements continue to be sustained. Team members have commented: “6S has lightened our load”, and “Now our daily routines are more efficient.” Benefits derived from the 6S application to the security command post include:

1. More space to work effectively and safely.
2. Improvements in ergonomics due to better organized workspaces.
3. Time saved on searching for items.
4. Easier process to identify and replenish supplies.

8.5 Reaching Out Across the Business

The security team did not stop at 6S. They have two ongoing improvement initiatives. The first initiative is ongoing communication within the organization. They have developed a program called SEAT – Security Education, Awareness and Training. They use this initiative to make sure the entire plant is aware of all necessary security measures and protocols. This is for the security of the people, processes, and assets as well as for compliance to legal and regulatory requirements. They consider security awareness to be a two-way street that includes the objective of Security’s being aware of the security needs and considerations of the facility personnel. They have a multi-faceted approach to SEAT:

1. Communication boards
2. Newsletters
3. Internal security website
4. One-on-one management meetings and group management briefings
5. Briefings for all security staff to keep their own security awareness sharp and to share their observations of facility personnel and operations.

The second initiative is the ongoing waste elimination efforts. A recent improvement was the automation of the manual process for changing facility access privileges. This eliminated up to a mile of walking for each change request.

8.6 Keeping People in the Equation

The Security Team designs security technology applications to aid their customers—the entire facility workforce—with minimal or no impediment to plant operations. They do not use technology just for the sake of technology. As an example, their internal web site allows personnel to complete standard security forms online from their personal workstations or from employee services kiosks strategically located in the facility. This eliminates employee trips across the facility to the Security Command Post to obtain the necessary forms. Additionally, because the approval process is also an electronic workflow, employees don’t have to walk around the plant to obtain the required approvals. This does not mean that facility personnel cannot still come to security and speak directly to Security staff. It simply means that electronic workflow minimizes the time spent on routine processes. The Security Team will not let technology replace important human contact.

As Wright points out, "Security is an application of people, processes and technology. You can maximize contributions to the bottom line when you consider all three aspects, and use technology to improve security processes within the context of the business."

These activities are estimated to provide future savings of over $150,000 through process improvement and automation for things such as:

- Cost reductions for employee and contractor on-boarding and off-boarding
- Change management cost reductions (lost cards, temporary cards, access changes, disabling cards for leave of absence, etc.)
- Cost reductions for compliance enforcement, auditing and reporting
- Employee productivity regained by shortening processes and eliminating waiting times

Everything the Security Department does falls in line with this key guiding principle, "S*ecurity within the context of the business*".

9 About the Open Security Exchange

Corporate risk exposure. Security. Privacy. In recent years, these concepts have had a major impact on the way organizations operate globally. In both the private and public sectors, time-to-market considerations and customer expectations are driving the adoption of new business models and enabling technologies. End users, customers and partners are now trusted with access to organizational assets and systems, making overall security a more daunting challenge.

Exacerbating this situation, **the failure to integrate physical and IT security systems** has resulted in organizational and procedural gaps for virtually all enterprises worldwide — often leaving them vulnerable to attacks and unable to consistently implement security policies. At the same time, regulatory requirements have created additional areas of concern. Today, organizations need to mitigate risk and regain full control of their security management by optimizing their enterprise security resources.

The Open Security Exchange (OSE) is a not-for-profit association of security experts that provides a forum for end-users, manufacturers, integrators, consultants and allied organizations to mutually define opportunities for converging physical and IT security. Its goal is to help improve enterprise security through the collaborative development of reusable models, definitions, vendor-neutral interoperability specifications and best practice guidelines that accelerate the convergence of security systems.

Extensive member knowledge, combined with end-user input and industry advisor feedback, make the OSE well qualified to recommend interoperability specifications, create best practice guidelines and white papers and build a knowledge base for the industry.

The OSE's mission is to demonstrate how combining the disparate technologies that form today's security infrastructures can enable optimal security and operational efficiencies while respecting organization-specific operational requirements. Thus, more effective security management will result in:

- Accurate detection of threats and attacks
- Consistent definition and enforcement of security policies
- Enhanced organizational collaboration

Contact the Open Security Exchange

For General Inquiries or Media Inquiries:
Call 202-712-9058

Open Security Exchange
1444 I Street NW, Suite 700
Washington, DC 20005 USA
Phone: 202.712.9058
Fax: 202.216.9646

www.opensecurityexchange.com

The information contained in this document is a summary only.

For more information about Open Security Exchange and its products and services, please contact Open Security Exchange.