SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Missile Defense

Bob Hayes

Originally Published in SecurityInfoWatch

October 2012

Missile Defense

Security at the Raytheon Missile Systems plant in Tucson, Arizona is world class — in fact, the program received its second consecutive superior rating from the Defense Security Service this year.

Raytheon's security is built on relationships, awareness and training. Security personnel are "embedded" in every aspect of the business, with each employee conscious of both their own security requirements and how they fit into the big picture; while continuous training caters to the specific needs of each employee.

As a high-level defense contractor that deals every day with classified information, security at Raytheon must be measured perpetually and repeatedly, based on the highest enterprise standards and requirements.

Any organization can learn lessons from the security success at Raytheon, where achieving a superior-level security program is not cost-prohibitive. As the security program demonstrates, there are opportunities everywhere to make the operation leaner and to improve execution and attention to detail. For Jerry Charlow, Raytheon Missile Systems Senior Director of Security Services, a superior security program should not be seen as something that is profound or revered, but simply as a fundamental and necessary element of business execution.

March to Superior

Part of the transition from a "satisfactory" to a "superior" rating at Raytheon Missile Systems was a branded awareness campaign called *March to Superior*, which was implemented with the support of Dr. Taylor W. Lawrence, president of Raytheon Missile Systems, and Dan Schlehr, the company's Vice President of Global Security Services. "It was a commitment as an organization to be an A student," Charlow says. "We work constantly to be sure we are truly protecting what we are entrusted to safeguard."

The security operation also embraced a strategy of "Local Vigilance, Global Defense" — emphasizing the need for each employee to pay attention to what's going on around them. Focusing on local vigilance has broad implications at the global level, and promoting awareness built a sense of unity around a common purpose and common cause.

It Starts with the Basics

Initially, *March to Superior* focused on asking basic questions: What systems are currently in place? What are their maintenance and reconciliation requirements? Where is the classified material? The answers to basic questions like these highlighted opportunities to improve existing safeguards and run a leaner operation.

For example, in 2005, there were about 3,000 containers with classified information at Raytheon Missile Systems. Much of the information — including classified drawings, engineering information, magnetic media, disks, tapes, microfiche, etc. — was redundant, out of date or no longer needed; yet, protecting it was consuming valuable space and resources. To fix the problem, a team was conscripted to sift through the material, container by container, to review the inventory and tie it back to active contracts. The team pulled every document and piece of media, culled those that were no longer current, reduced duplication, and cataloged and assigned physical locations to everything that was retained. The exercise reduced the number of classified containers from 3,000 down to 600.

Eliminating duplication and material that did not need to be retained also translated into business cost savings in addition to better security of classified materials. For example, the material now takes up less floor space; it needs fewer GSA-compliant containers; and fewer lock combinations must be changed.

Building Relationships and Accountability

Transitioning from a “siloed” approach to more integrated security at Raytheon required creation of an organizational structure that included systems, processes and metrics that emphasize to employees that what they do affects someone else. For example, a security officer’s response time either helps or hurts a customer, whether external or internal; or a more complete report could shorten an investigation. Where there is overlap, processes related to an event should be addressed as a team, not as a single employee.

Business is built on relationships, so security at Raytheon uses relationships to maximize results. At Raytheon, security professionals are "embedded" in various product lines and functions in the company. They serve as business partners to those parts of the business and build relationships and rapport that help accomplish the security mission.

Charlow manages 320 security employees in the organization. Every aspect of the operation is interdependent, so overall success is based on each individual's contribution. Evaluations are not limited to managing a certain niche but on a stake in the entire organization. Such an interwoven environment requires collaboration for success.

Training is ubiquitous and geared to the needs of each employee. Raytheon, like other large companies, has many employees; they may be audio learners or visual learners, have a GED and plenty of practical skills or be a Ph.D.-level scientist. The diversity of employees requires the training approach to be specific to the learning style of the employee. "Sometimes the folks in the trenches don't realize that what they do can have a big impact," Charlow says. "Employees must perform on every level for the business to be effective. Sometimes employees don't see the bigger picture, so it's important that the company's leaders help employees make the connection."

The Role of Metrics

Being alert and analyzing business systems and metrics provides ongoing feedback about the operation of security. Looking at spikes in violations reports, for example, can aid Charlow's understanding of underlying factors. The information provides an ongoing "near real-time" picture of security success. "We work with business teams in partnership to cover those graphs and look at the output of business metrics, measures and data," Charlow explains.

Integrating appropriate metrics and measures into the "cadence" of the business is another way to make security a fundamental part of what the company does. Raytheon uses monitors (four full-time equivalent employees) whose job is to oversee any factors related to Raytheon and compliance with factors laid out by the National Industrial Security Program Operating Manual. The monitors travel to Raytheon operations across the United States and around the world and drive commonality in each the organization's facilities.

The ongoing monitoring program is one source of security metrics and data that guide decision-making. Others are incident reports by employees or reports from security officers on patrol. All the data is rolled into databases specific to IT systems, closed areas, violations, containers, etc. The information is reported to Raytheon's internal software system and to a Perspective incident management system from PPM 2000 (www.securityinfowatch.com/10214679).

An online scorecard and visual display provide metrics information by process and product line, focusing on the performance of each group. Fundamental security elements are assessed based on the National Industrial Security Program Operating Manual, which establishes the standard procedures and requirements for all government contractors regarding classified information, and on Raytheon's enterprise standards and policies

The internal software sends automated notices to affected persons specifying what corrective action must be taken, confirming when the action is taken and routing the response to management to validate that the fix is correct. "We know what the problem is, and we know how to direct our resources to intervene, and we initiate corrective action almost immediately when we see trends that we don't want." Charlow explains.

Embracing Six Sigma

Raytheon embraces philosophical elements of the Six Sigma process, a business management strategy originally developed by Motorola and used commonly in manufacturing. Six Sigma seeks to improve the quality of processes by identifying and removing the causes of defects (errors) and minimizing variability in business processes. "The Six Sigma elements are at the core of our success — it is in the company's DNA," Charlow says. "It's about making sure that when we correct a problem, the corrective action is sustainable. We make sure every process we put in place can adapt as the business changes."

The security program strives for continuous improvement and to be self-sustaining, self-governing and self-moderating in line with Six Sigma principles. Use of Six Sigma is an example of the value of reaching outside the security "comfort zone" to consult with people who have business degrees or who are quality professionals.

"By definition, continuous improvement means that the job is never really done," Charlow says. "We never stop striving to be better than we were yesterday. If you don't embrace that mindset, it is hard to keep improving."

Emphasizing processes over individuals and striving for consistency are strategies to eliminate the negative impact of human-element variables. "Leadership is important, but predictability and sustainability and consistency are critical to what we have accomplished," Charlow says. "It is not dependent on a single person filling out a form every day — it is a system that drives people and becomes a predictable model for future outcomes."

Support from the Top

Charlow acknowledges the contributions and support of Lawrence and Schlehr. "You have to be able to define the business plan at the C-level and help them understand," Charlow says. "It is important that security be driven from the top down. You can have the most passionate security leader in your business, but the chief executive also must see the importance and criticality of it."

Management should routinely consult with security for guidance on the front-end of a business decision to avoid negative consequences on the back end, he adds. Equally as important, Charlow says security organizations should look inward and seek to achieve consistency in all operations.

"Let's not criticize each other — let's figure out a program that can enable our environment," Schlehr says. "Let's sweep our own porch…this kind of work is more a calling than a job."

Bob Hayes is Managing Director of the Security Executive Council. He has more than 25 years of experience in security, including 8 years as the CSO at Georgia Pacific and 9 years as security operations manager at 3M.

About the Security Executive Council

We are a research and advisory firm for security leaders. We have a collective of close to 100 security subject matter experts that have been successful security executives or are recognized industry experts in their field. The resources and tools we develop are constantly evolving to provide maximum value. Some engage with us by way of multi-year “retained” services agreements (Tier 1 Stakeholders). Tier 1 Stakeholders are those that want support on an ongoing basis but also want to have an active role in identifying solutions for the industry. Others come to us seeking a specific solution to a contained issue. In all the ways people engage with the SEC the bottom line goal is to help define and communicate the value of the Security organization.

Contact us at: contact@secleader.com
Learn more about the SEC here: https://www.securityexecutivecouncil.com