Securing the Global Enterprise

How one global network provider pioneered a converged security approach

By Michael Miller and Paul Kouroupas

Security within the corporate organization has historically been fragmented, with many departments responsible for their own security. Network provider Global Crossing quickly recognized that the convergence of all security matters under one department was necessary to obtain a complete understanding of the threats to the company's assets, personnel and intellectual property. This was made all the more critical in a rapidly changing post-911 world.

In 2002, Global Crossing pioneered a converged security philosophy and a strategic plan for protecting its infrastructure, information, and personnel through a comprehensive defense-in-depth approach that transcends physical and logical security. Much like the company's global IP network, which delivers converged voice, video and data communications to enterprises around the world, Global Crossing's converged security strategy now uses multiple independent and interlinking layers of security that together provide greater protection.

Global Crossing has differentiated its network solutions by delivering a combination of advanced technology, customer support, reliable security and flexible control. Security is a key cornerstone for delivering such a solution, since converged IP networks often connect to other private and public IP networks.

As part of its defense-in-depth strategy, Global Crossing protects its information and tangible business assets by setting in place multiple layers of security that include specific hiring and personnel practices, physical access controls and network systems protection. These elements converge to provide a holistic view of security.

The success of the converged approach to security depends upon centralization, policy command and uniform use of technology.

Accountability at a High Level

Recognizing the deficiencies of a fragmented approach to security, Global Crossing centralized all security functions under one leader, the VP of Global Security, reporting directly to the chief information officer (CIO). Additionally, the VP of Global Security reports directly to a Security Committee of the Board of Directors. This Security Committee was established pursuant to the company's Network Security Agreement with federal U.S. law enforcement and national security agencies as part of Global Crossing's acquisition by Singapore Technologies Telemedia.

The agreement required Global Crossing to implement additional safeguards to support the U.S. government's law enforcement and national security interests. The Security Committee of the Board of Directors provides governance and support for security at the highest level within the corporation. This committee is responsible for over-

seeing security in the same manner that an audit committee is responsible for overseeing the integrity of a company's financial statements. The establishment of the committee eliminated the silo approach and unified how security was defined and measured throughout the corporation.

Global Crossing's Security Organization identifies and assesses risks to its facilities, personnel and information systems. It then evaluates options for managing these risks, working with departments throughout the corporation to decide upon and implement appropriate controls.

Mike Miller, VP Global Security & Services

Keep the Money Together

In addition to centralizing security functions, Global Crossing centralized security budgetary control, allowing the organization to get a complete picture of who was spending on security, where, and how much. This provided an opportunity to leverage their investments, consolidate like projects and to make strategic investments, shifting resources from traditional security roles like manned guarding to leading-edge measures, such as intelligent security systems and real-time event notification. Global Crossing was then able to reduce its overall operating costs, focusing on the use of technology to help address their security needs.

While all this centralization allows for improved budgetary and policy control, it does not preclude some local security functions. Certain functions can be performed more effectively at a local level, and a good security program must recognize these. It's therefore critical to build relationships with other departments, including human resources, legal and real estate. These teams are the eyes and ears for security, providing critical local information and real-time intelligence.

For example, when gang-related crime started to increase outside of Fortaleza, Brazil, the local facilities manager approached the security organization about the increased risks to one of its critical network facilities. Together, the security, real estate and network operations teams evaluated the risks and discussed the different types of countermeasures that could be implemented to minimize the threat. It was agreed that the most effective solution was to increase the size of the perimeter wall and add an electronic fence to the top of it. The local support of in-country personnel was critical to recognizing the threat and to providing a timely implementation of these preventive measures.

One Policy for All

The Security Organization is also responsible for developing security policies, processes and standards that apply to the entire corporation. As the focal point for all matters related to security, the Security Organization is ultimately responsible for all company endeavors that seek to avoid, prevent,

By using the same technology, systems and devices at locations around the world, Global Crossing is able to project a consistent security model throughout the organization.

From left: John Heaney, Head of Physical Security; Mike Miller; Jim Lippard, Director of Information Security Operations; Paul Kouroupas, VP and Security Officer; Robert Hagen, Director of Security Architecture.

detect, correct or recover from threats to corporate facilities, personnel or information systems. The centralized security approach ensures consistency throughout the organization and helps avoid incomplete application of company-wide security remedies.

Again, while the goal is to provide a consistent approach to security globally, it is of course necessary to understand local conditions and risks. This is extremely challenging for global organizations, since they do not always have security resources in every location, and since each country has its own domestic and foreign security policies.

A converged security organization must take into account local laws and regulations, regional objectives, legal requirements, employee privacy issues and governmental oversight. Global Crossing uses a combination of in-house and outside counsel to assist in understanding the multitude of legal and regulatory requirements by region.

It's also important to build and maintain a strong partnership between the security and legal departments and to establish a level of trust. This opens up the lines of communication, prevents misunderstanding, and reduces a company's exposure and risk. In addition, the security organization should conduct risk assessments that cohesively mesh domestic and global security policies with the ability to track incidents around the globe.

Uniform Use of Technology

Perhaps the most critical aspect of a converged approach to security is the uniform use of technology. By using the same technology, systems and devices at locations around the world, Global Crossing is able to project a consistent security model throughout the organization. In addition, the uniform use of technology maximizes purchasing power, simplifies training requirements and allows for central operation of many of the systems and devices, thus maximizing the personnel budget.

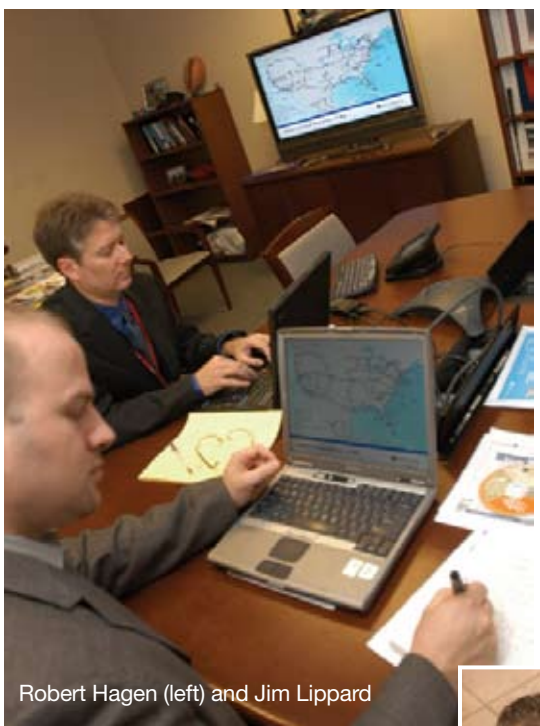
More than 35 local DVR systems at Global Crossing facilities in four countries use the same technology all linked together and accessible through the management console. This allows the local facility managers to have access to critical information while the systems are controlled and monitored centrally by security over the internal data network. The DVRs connect surveillance cameras through the facility. By using uniform technology, Global Crossing has reduced its manned-guarding expense by almost half without impacting the number of reported incidents.

The unified use of technology is dependent on the processes that are implemented to respond to incidents. Global Crossing's intelligent security systems are event driven and do not require constant physical monitoring by the Security Organization. The company's logical intrusion detection system (IDS), physical access control system and DVR systems send real-time event notification through e-mail to the incident response team. By standardizing the process and receiving alerts in real time from security systems, the Security Organization is able to focus its resources on critical events. The process for identifying critical events is iterative and time consuming. It involves tuning the security systems to reduce the number of false alarms and to ensure that critical events are not being excluded. The same methodology is applied to both the logical and physical security systems.

Once the systems are tuned, any unusual or inappropriate network activity or physical incident that is detected is investigated to determine whether it

is an isolated incident or the beginning of a large-scale attack or outbreak on the network. Global Crossing works with its customers to mitigate and stop distributed denial-of-services attacks and other malicious activity by establishing security arrangements and notification procedures. If illegal activity is detected, the Security Organization notifies the appropriate law enforcement authorities and assists in the investigation.

Employee identification and facility access are also approached with uniform technology. Global Crossing adopted a single access card format and style globally, which means the same access card can work on multiple access control systems. This has reduced the number of cards in circulation by almost a third. Not only does this improve the manageability of the systems, but it improves the overall security. Consistency builds awareness throughout the organization and reduces the possibility of multiple cards being misplaced, lost or stolen.



Robert Hagen (left) and Jim Lippard

Standards and Reviews

Every security program must have a standard against which it can be measured. Global Crossing developed its Enterprise Security Program Plan (ESPP) to be compliant with international standard ISO/IEC 17799, as well as the standards established by Global Crossing's unprecedented Network Security Agreement in the United States and other specific security requirements from the government of the United Kingdom. In addition, the Sarbanes-Oxley Act and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) provide critical standards against which Global Crossing's security can be measured.

Under the company's Network Security Agreement, an independent third-party auditor conducts a comprehensive annual security evaluation and risk assessment to evaluate Global Crossing's implementation of and compliance with the Network Security Agreement. Separately, in the United Kingdom, the company undergoes rigorous penetration and vulnerability tests annually to maintain security accreditation.

By adhering to standards and conducting periodic reviews, Global Crossing is able to continually test and improve its security position.

For industries with less clearly defined standards, the ISO/IEC 17799 "Information Technology—Security Techniques—Code of Practice for Information Security Management" can be very beneficial for providing a framework for developing standards. In addition, many industries have their own published list of best practices that can be used as assessment tools. It is important to fully understand objective standards against which you can be measured. It is equally important to understand what is required for compliance to industry standards and government regulations. Often the details are in the implementation of the standards and the checks and balances that are in place to detect violations and/or flaws in the process.

Disparate Functions Not Enough

It's no longer enough to focus on the security of assets, facilities and personnel within an organization. What's required now is security throughout the world adapting measures that address and mitigate the threats and risks around the globe.

Global Crossing's convergence strategy is effective in meeting the needs of a multinational corporation while being flexible enough to address security concerns at a local level. Security is a partnership between multiple functional groups both in and outside of the company.

It is important to build strong partnerships in both the public and private sectors, leveraging information from multiple sources to truly understand the security landscape and the threats against your company. Be proactive and flexible, looking at a combination of physical, personnel and logical security measures to secure your assets and the success of your business. STD

Michael Miller (above right) is vice president of global security and Paul Kouroupas is a security officer for Global Crossing.