

The Convergence of Logical and Physical Security Solutions

Computer hacks aren't just about bits and bytes; they can have real, quantifiable and destructive outcomes. Nobody would contest that organizations require physical security; further, very few organizations would even consider doing business without some type of IT security.

Prudence dictates that for physical threats, physical monitoring solutions be leveraged to mitigate risk. If there are logical threats, then logical monitoring solutions should be used. And, if the threats converge, then the security solutions must converge as well. This sounds simple, but the disciplines of physical and logical security are highly disparate. As such, getting the technology and the individuals to work synergistically can be challenging.

To truly gain a holistic perspective of an organization's security posture and provide the right level of incident detection, physical and logical security solutions must converge. Here are some examples of computer hacks that had direct repercussions on the physical world.

- Armed with only a laptop and a stolen data radio, an Australian hacker broke into computerized a SCADA system (Supervisory Control And Data Acquisition) and released 264,000 gallons of sewage into waterways in 2000.
- The Davis-Besse nuclear plant in Ohio had its safety systems disabled by SQL Slammer for several hours.
- The CSX Railroad Corporation halted passenger and freight train traffic because of a worm infection in their telecommunications system.

The U.S. government has already declared that before August 2006 all indi-

viduals accessing Department of Defense (DoD) systems must possess common access cards (CAC). These cards, which replace traditional identification cards and feature an imbedded microchip, are used for physical access to DoD facilities as well as information systems – negating the use of usernames and passwords. The card is also being explored for the Guest Worker Program and for the TSA Registered Traveler Program.

Most CAC systems interact with backed LDAP solutions such as Active Directory. Access to secured networks and servers will require a CAC. Additionally, they can be used for encrypting e-mail and other logical security functions. The physical security and logical security information are synced through the CAC identifier, creating a more efficient and scalable network infrastructure. For example, if a government worker walked into a building in Virginia, then 5 minutes later also accesses a sensitive server from a remote VPN account in Germany, alarms would be raised.

ESM Solutions

One of the primary issues in the past was simply trying to find a solution that could not only collect information from both physical and logical systems, but also actually add real value beyond simple log storage. This issue has been remedied with the introduction of enterprise security management (ESM) solutions. These solutions can:

- Collect events from virtually anything that generates logs and alerts.
- Apply business context, such as physical locations; user, group and department information; asset relevance; content

sensitivity; and regulatory policy and compliance.

- Correlate information, detect anomalies and identify patterns.
- Reduce data overload and false positives.
- Render the data through useful visualization and reporting capabilities.
- Provide advanced real-time and forensics analysis.
- Facilitate integrated incident management.
- Allow rapid remediation for incident response.

As such, ESM is a core ingredient for successful convergence.

Physical security groups are often former law enforcement, secret service, security guards and individuals with like backgrounds. They often report through departments such as facilities, human resources or legal, and focus on protecting property against fire, theft, vandalism and illegal entry. At the core of their duties is observation – such as video surveillance or hallway patrols – and then reporting what they observed via a written summary of events during a shift.

Information security professionals usually have business and/or technical backgrounds. They typically report to a CIO, CSO or an executive responsible for information security. Given the bifurcation in IT and physical security backgrounds, the varied expertise in each discipline, reporting structures and responsibilities for these groups, it is plain to see why there hasn't been a lot of synergy in the past.

Collaboration is Crucial

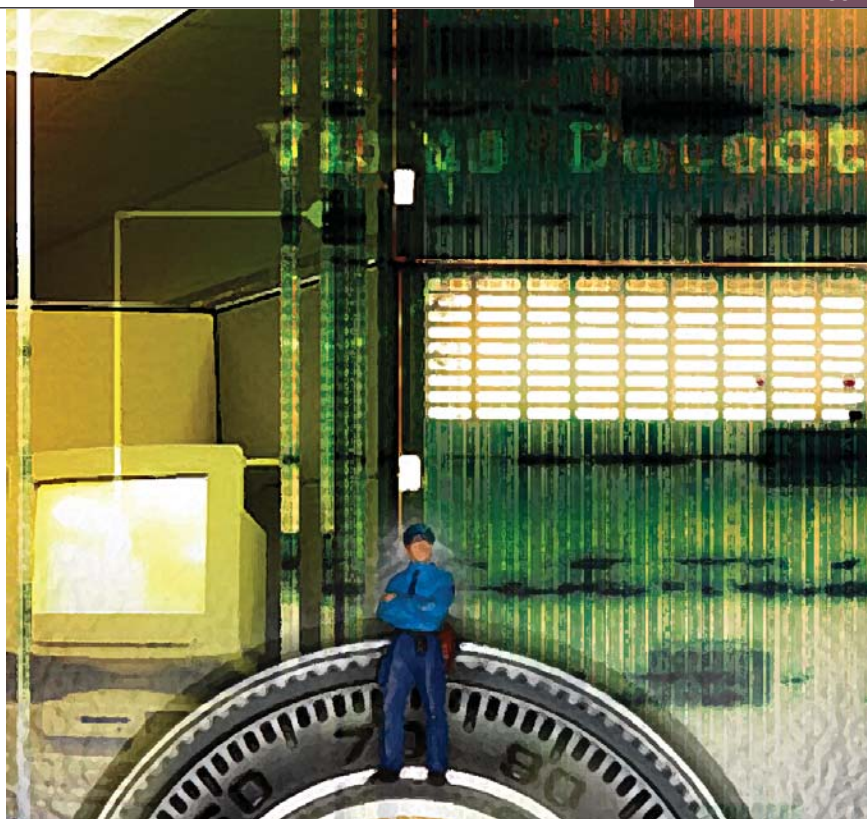
When IT and telephony began to converge several years ago, there was a lot of

resistance on both sides, but over time, most learned to co-exist. I can recall an event early in my career where I was given the responsibility of trying to track down all analog phone lines, since they could provide dial-up modem backdoors into the corporate network and bypass firewall controls. The project was called the “unauthorized modem abatement project.” It should have been called “phone guys don’t play with computer guys.”

Just the politics involved in getting IT and telephony to work together on this project took weeks of coaxing and executive intervention. Since there was no source for analog phone line data, a combination of war dialers and PBX databases were used to find which analog lines were being billed against which departments.

The telephony team had no interest in helping IT navigate the complexities of the PBX. And when it finally came time to actually start disabling the unnecessary analog lines, convincing the telephony team to break their golden rule of “cause no user disruptions” required more executive sponsorship and coaxing for each line that was disconnected. It took almost a full year to disconnect, secure or find alternatives for about 1,300 analog lines.

Not all cases are this painful, and collaboration can be quite simple. For example, there may need to be weekly meetings between physical and logical security managers. Tactically, it may encompass things such as the information security group sending an e-mail warning staffers about a fast-moving Internet virus while the physical security group posts signs around the building as a secondary reminder. Or for the IT security team to notify the physical security team



when they see anomalies in badge reader logs such as one ID card being used in two separate locations within a short time frame.

The Real World

One place where the need for these synergies became unmistakably apparent was Guangzhou, China, which is about a 2-hour train ride west of Hong Kong. While there, I was meeting with a manufacturing company that had recently experienced an attack on their facilities. Criminals had e-mailed individuals at the company stating they were representing the Chinese equivalent of the fire department and were going to be conducting tests. The message was sent to the IT team, which then forwarded it to the entire company. The employees were told to ignore any alarms and continue working. Shortly after, the building was set afire.

Fortunately, after noticing smoke, the employees were able to safely evacuate and nobody was harmed. If the IT managers had coordinated with the physical security group, they would have discovered that these types of tests are never

scheduled through e-mail, and that the message must have been a hoax. However, when it came time to investigate the incident after the fact, the teams did work closely to determine the source of the e-mails and pursue the criminals.

Another common issue is that the technology leveraged for physical and logical security can be very different. Luckily, most modern solutions will generate logs and allow some type of integration with networked systems. If they don’t, then integration will require an upgrade. Also, the two groups generally have different approaches to technology. While IT embraces new technologies, physical security personnel are usually more skeptical and standoffish about emerging technologies in favor of tried and true methods. It’s one thing if somebody can’t check e-mail; it’s a more critical matter entirely if they can’t get in the building.

Another example: A financial institution is in the midst of upgrading its physical security badge readers. The current solution generates logs; however, it does so in line printer (lpr) format. This means that while you can send the lpr output to a

syslogNG daemon instead of an actual printer, you have to deal with things not commonly associated with syslogs, such as page numbers, hash marks and dashes everywhere. Typically these issues can be overcome with mature, enterprise security monitoring solutions. Once the logs are captured and normalized, the data itself must be valuable.

Again, modern systems provide valuable data such as time, user ID, location, number of attempts, etc. As covered in the CAC example with the DoD, this ID can be further associated with logical access. With older physical security systems, the value of the logs is unclear at best. However, as industry analysts have been pointing out, because of increased efficiencies and improved security, convergence is here, and if the current physical systems can't co-exist, they'll ultimately require an upgrade.

More Synergies

Convergence doesn't stop and start with monitoring physical security access controls. There are a number of other areas where organizations have taken advantage of synergies. One organization that I worked with integrated video surveillance with traditional logical security products. They have a number of systems that allow remote user access or administration. If somebody has to log on and make changes, they must do from a local keyboard and monitor attached to the server.

This is somewhat common for mission-critical applications or devices containing highly sensitive data. These systems are under 24-hour surveillance by network-enabled cameras that are capable of not only video recording, but also taking still photographs that can be automatically stored on a web server. Based on suspicious activity derived from

There are a number of solutions that can be tied together, such as RFID, HVAC, burglar/fire alarm systems, and timesheets, as well as vertical-specific solutions such as SCADA and fraud detection.

server's OS and application logs on the targeted system, an enterprise security management (ESM) system correlating that data can trigger an event that prompts the video camera to take a snapshot. The security analyst is alerted to the event, and with a mouse click on their ESM, they can display the photo. Since the video surveillance is fed to the physical security team's CCTV system, that team can also receive an ESM alert detailing which camera feed to observe.

Another interesting video camera example comes from a retailer, which records countless hours of time-stamped video. Since it is nearly impossible to go over every second of video, its main purpose is to act as a deterrent. However, it can also assist in supporting investigations. This organization had cameras positioned above point-of-sale (POS) registers. The transaction logs were sent over the network to an ESM for processing. If suspicious register activity is detected within the ESM, the security team will receive an alert. The time-stamped video surveillance can be used to substantiate the alert and the IT security team can work with the physical security team to review video.

These examples only touch a few technologies and synergies that can be leveraged with convergence. There are a number of solutions that can be tied together, such as RFID, HVAC, burglar/fire alarm systems, and timesheets,

as well as vertical-specific solutions such as SCADA and fraud detection. Not all integration makes sense for every organization, but for almost every organization, convergence at some level can aid in risk reduction and increase in operational efficiencies.

Convergence is achieved through endurance; it's not a sprint. Executive-level sponsorship is a must, and even small victories will ultimately ensure that convergence is successful. For management, this success will increase operational efficiencies and mitigate risk, while adding to stronger ROI and enhanced ROSI. Operationally, both physical and logical security teams will benefit from broader event collection, incident detection, analysis, reporting, tracking and remediation. The integration will also facilitate tighter controls over regulatory compliance, policy and enhance security awareness. The net effect: convergence will positively amplify your organization's security posture. ■■■

Brian T. Contos, *CISSP*, is the Chief Security Officer of ArcSight.

