CERT'S PODCASTS: SECURITY FOR BUSINESS LEADERS: SHOW NOTES

Convergence: Integrating Physical and IT Security

Key Message: Deploying common solutions for physical and IT security is a cost-effective way to reduce risk and save money.

Executive Summary

Given growing levels of network connectivity, convergence of physical and IT security is happening today. Integrated and interoperable solutions for video surveillance, identity management, and radio frequency identification are increasingly prevalent. In this environment, leaders need to examine organizational roles, skills, processes, and technologies to implement cost-effective solutions that reduce risk on multiple fronts.

In this podcast, Brian Contos, Chief Security Officer at ArcSight, and Bill Crowell, a member of the board of directors for several security companies and former deputy director of the National Security Agency, discuss the business and technical issues involved in bringing together physical and IT security solutions.

PART 1: WHAT IS CONVERGENCE, AND WHY IS IT IMPORTANT?

Defining Convergence

Convergence:

- brings together multiple security disciplines. It is driven by the ability to connect a wide range of security processes
- expands the context of security to include video surveillance, physical security, and logical security including network and applications security

Why is convergence relevant now? What has brought it about?

One answer is the advent of the Internet and IP (Internet Protocol)-centric business solutions. Examples include:

- the evolution of the process control industry and network-connected SCADA (Supervisory Control and Data Acquisition) systems
- Voice over IP with traditional telephone systems
- the integration of network and security operations centers

These developments, in turn, are starting to bring about convergence of the CIO, CSO, and CISO (Chief Information Officer, Chief Security Officer, and Chief Information Security Officer) roles

What are the implications?

- Traditional silos will start to disappear, for example, boundaries between network security, physical security, and human resources.

- Single user identities are starting to emerge for all business transaction authorization and access. Identity management will include physical facility access and rights as well as network and application access and rights.

- Approaches like Common Access Cards are being used today to support physical access, network access, and email encryption, as well as to provision new employees and revoke the rights of terminating employees.

- Smart video and video analytics will be used to integrate and present all sources of video surveillance and to assist with forensics analysis. We can then collect physical security events captured by video surveillance cameras and correlate these with system and network access, for example.

The CxO-level role that leads this effort will be responsible for risk, compliance, physical, and logical security.

Physical and IT security roles will still be required, but there will be much more communication among those roles and much more integration of solutions, including policies, procedures, and technologies.

PART 2: GETTING STARTED; TACKLING CHALLENGES

First Steps

So, how can companies get started in tackling convergence issues?

In this case, the U.S. federal government has led the way.

Homeland Security Presidential Directive - Number 12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors, presents a standard for combining physical access, logical access, and identity cards into a single credential.

Recognizing the Risks

Leaders need to recognize that they are equally at risk from an intruder attempting to attack their network, an insider inserting malicious code into network-accessible software, or a member of the cleaning crew stealing a server or laptop computer with sensitive customer information.

Challenges include:

- Lack of uniform, consistent standards; many exist for specific security technologies
- Historical biases, along with the need to update skills and build new skills: Physical security professionals typically have a law enforcement background, whereas those involved in logical security have an IT background.
    - Leaders need to understand the strengths and shortcomings of each skill set and find ways to bridge the skill and language gaps.
- The need to establish clear distinctions and assignment of roles and responsibilities for converged solutions
- Whether or not to outsource

Taking Action

Concrete steps to take:

- Recognize that convergence needs to happen and is happening.
- Seek opportunities to integrate solutions and roles and to save money.
- Recognize that security can be a value-added business function.
- When evaluating technology solutions for incident prevention, detection, and response, consider both physical and logical security. But do make sure the solutions produce outputs that can be used for multiple purposes.

PART 3: TRENDS AND FUTURE DIRECTIONS

What the Future Holds

The marketplace can expect to see integrated solutions such as the combining of video surveillance, RFID (radio frequency identification) tagging, identity management, information security systems, and physical security systems.

Combined or integrated solutions will be able to generate correlated data that takes all information sources into account and can present analysis results based on risk.

Getting Buy-In to Drive Innovation

It turns out that approaches and progress do not really fall along market sector boundaries as one might expect. What seems to make the most difference is the vision and drive of key decision makers in an organization.

Risk, regardless of whether it results from physical or logical security weakness, therefore needs to be expressed in terms that are meaningful to business leaders. For example, a breach, regardless of its source, leads to fraud or identity theft.

Lastly, in deploying layered security defenses, recognize that solutions at every layer can now be integrated, be interoperable, and convey a more holistic view of any given situation.

Resources

Contos, Brian; Derodeff, Colby; Crowell, William P.; Dunkel, Dan. Physical and Logical Security Convergence: Powered by Enterprise Security Management, Syngress, May 2007.

Webcasts:

Contos, Brian. "Hacking the Hallways: The Convergence of Physical and Logical Security."
https://www.sans.org/webcasts/show.php?webcastid=90687
http://searchsecurity.bitpipe.com/detail/RES/1160422178_79.html?src=wc_ssec_ArcSight_10_25_06_P&li=28156