IT-OT-Physical Security Convergence is Key to Delivering Holistic Security across the Enterprise

Most action and technology movie buffs will remember the Bruce Willis film "Live Free or Die Hard." Willis plays a New York City detective ordered to take custody of a computer hacker who has unknowingly aided an evil genius in triggering a three-stage coordinated attack on U.S telecommunications, transportation, electric power and financial infrastructure. The attack is referred to as a "fire sale," because "everything must go." Fortunately, the resourceful Bruce Willis stands between the evil doer and catastrophe.

Unfortunately, the fire-sale is not fiction. The Federal government plans for it in war game scenarios. Regrettably, the security professionals charged with protecting our critical infrastructure have neither the time nor the budget to engage in war game scenarios and prepare for simultaneous physical and digital sabotage. Their typically segregated operational, physical and logical security systems will fail to deliver the coordination required for early detection, prevention or fast remediation. Regardless, of this critical vulnerability, senior security executives are rarely and unfortunately not included in high level strategic planning and budget allocation.

A painful, and too often ignored, fact is that millions of dollars are being spent on halfway security measures, while breaches continue unabated. Current expenditures on regulatory compliance and network security too often miss a structural vulnerability: security is imprisoned in corporate silos.

IT security personnel focus on virus and malware attacks, hacker penetration of network perimeters and employee access and authorization. Corporate security personnel focus on physical access to buildings, zones and remote facilities and, often, environmental systems. Operators of critical assets like pipelines, power plants, chemical plants and airports, focus on whether assets are functioning within established parameters. The monitoring systems for these functions are rarely integrated and even more rarely correlated for contextual understanding of an evolving security event. Everyone is isolated. It is the very definition of halfway security and corporate irresponsibility.

Determined attackers have a more holistic view of security. They attack the enterprise. They understand that security silos represent vulnerability. Segregation means each silo is real-time blind to breaches in the others. Communications gaps between silos mean time delays. Time delays mean opportunities for attackers. The failure to integrate physical security with IT security and operational technology – regardless of budget – is the moral equivalent of aiding and abetting thieves and saboteurs.

Time is passing – enough time for an intruder or an incorrectly calibrated device to do a lot of damage. The operator is monitoring an increasingly unstable situation and someone must be dispatched to mitigate the damage and reconfigure or replace the equipment. The urgent question is whether they send the guy with the wrench or the guy with the gun? The problem with that question is that none of the silos, alone, has enough information to make that decision on a timely basis. A related question is:

what are the economic, health and safety costs of delayed action in preventing or mitigating the effects of a power outage whether due to equipment failure, sabotage or error? The irrefutable answer is obvious: more than the cost of a security system that combines multiple signals from IT security systems, operational technology systems and physical security systems with cross-enterprise data to give operators the contextual information necessary to act decisively and prevent or mitigate the outage.

Convergence of physical and logical systems is necessary for comprehensive security and fail-safe incident management. Real-time risk analysis that combines continuous monitoring and geospatial and environmental data with rule-based threat detection and real-time remedial action scripts can deliver contextual understanding and fast, informed action – regardless of the size of the data sets.

The Need for Security Convergence Drives Structural and Operational Changes

Tectonic Shift in the Organization: Departments like Corporate Security and Plant Operations at one time had little or no need to collaborate with IT. Times have changed. Today's badge access control systems for facility admission, as well as digital camera systems for surveillance and real-time plant performance analytics now operate on IP-based networks. The silos must work together for security and reliability. Many organizations are viewing the CSO as the chief of both IT Security and Physical Security, and, as time progresses, Plant Security. In the PwC State of Information Security Study, published with CIO and CSO magazines, survey respondents in the Utilities industry reported exploring the notion of the senior security executive reporting to the "Top of the House". This reflects the evolving role of the security leader as accountable for enterprise-wide security functions – IT, physical and operations security.

Active Enforcement of Operational Compliance Strengthens Security and Reliability: It is widely accepted that compliance alone cannot ensure security. However, active policy enforcement of operational compliance requirements extends beyond documentary compliance to rigorous application of security processes, standards and regulations. This is fundamental to competent governance.

Standards and regulations like NERC CIP, CFATS, PHMSA, MTSA, NEI 08-09 / 10CFR 73.54 (Nuclear) are incorporating IT Controls, Physical Controls, and where appropriate, the monitoring of SCADA / Plant Controls. To get the most comprehensive and informed view of risk in these environments, it is important to monitor the situational context in which events and activities are taking place. Knowing who (employee, contractor or visitor) is accessing what information, zone and equipment, with what authorization and privileges, under what circumstances and with what impact on systems and end-points in real-time is fundamental to securing the organization and the reliability of its services to the community. The ability to sense, alert, respond and mitigate on a timely basis must be among the highest priorities of critical infrastructure companies.

Security has bubbled to the Top of the Executive Agenda: In a recent study conducted by accounting firm Eisner Amper (EA), directors of boards are most concerned about cyber security risk (70 percent), reputational risk (66 percent), regulatory compliance risk (64 percent), and senior management succession planning (51 percent). The definition of cybersecurity has expanded to include IT, OT and Physical Security as well as IoT (Internet of Things).

A Simple Example of the Need for IT, OT and Physical Security Convergence Do you know who is running your plant? It may seem like a ridiculous question, but in real-life this is a question that needs to be asked or a control that needs to be tested with every event and transaction throughout every minute of every day. Consider the control room operator who is able to log into the operator console for the power plant, despite having followed someone into the building without swiping his own access card. This may be an innocent occurrence when seen as an isolated event. However, when correlated with HR data, staff schedules and system transactions, it may reveal something much more sinister. Was he scheduled to be on duty? Was he supposed to be on vacation? Was he on disciplinary probation? Was he altering system configurations? Disabling alerts? Was he attempting to access systems he was not authorized to engage?

Simply logging into the console without badging into the facility or control room should trigger automated checks to answer these questions and alert security to investigate a physical breach – innocent or not. With the right technology, a single unified Security Operations Center (SOC) can handle a wide range of incidents and threats – from cyber and physical threats to insider threats, advanced persistent threats (APTs) from hostile entities, accidents and natural disasters.

Innovations – Delivering IT, OT and Physical Security Convergence

The technology to accomplish real-time, cross-enterprise security convergence is in operation in mission critical circumstances today. An integrated security convergence platform can analyze and correlate data across thousands of events and hundreds of locations to expose risks and deliver more informed and actionable situational intelligence in real-time, every minute of every day. This eliminates both the vulnerabilities and inefficiencies of managing security and risk across silos. It enables fast and informed responses to IT, physical and operational threats, thereby reducing cost and liability while increasing safety and reliability.

Linking the HR systems to conduct risk analysis on an on-going basis and automate the on-boarding and off-boarding process can insure that only the intended individuals get access to the most critical systems. Insider threats and hostile intrusions are managed by integrating across multiple card access systems, video surveillance systems and sensor networks. This enables monitoring of employee, contractor and hostile agent access to critical assets across the energy value chain.

Security convergence can be applied to Utilities, Oil & Gas, Chemicals, Transportation, Nuclear IT and even Financial Services. Capabilities can include visual risk analysis and remediation, risk-led access control across multiple domains, incident management and response, continuous controls monitoring, compliance automation, user access certification, privileged access monitoring and audit support and reporting.

Blended threats occur in the white spaces between silos of automation represented by IT Security, Industrial Control Security and Physical Access Security. AlertEnterprise is the only software that can uncover security threats across the IT systems, physical access controls and industrial controls without adversely impacting the performance or reliability of the industrial process.

Finally, security convergence solves the inability to link events across the domains of physical, cyber and SCADA / OT domains. Just as important it becomes a key factor in helping address compliance requirements like NERC CIP and CFATS. A holistic approach to security has been proven to be more

effective in safeguarding these assets. Being able to connect the dots when complex events like physical intrusion and cyber-attacks occur simultaneously, delivers split-second response to mitigate the impact.

- Jasvir Gill, Founder & CEO, AlertEnterprise, Inc.