THOUGHT LEADERSHIP INTERVIEW

Bridging the Gap: The Convergence of Physical & Cyber Security in Crisis

IA FORUM MEMBER
Harris D. Schwartz, *Former CISO,* **AON** & *Consulting CISO*

What are organizations' most significant challenges when merging physical and cyber security during a threat incident?

Often, an organization will have physical security and threat intelligence separate from the cyber/information security department and their threat intelligence. Think about threat intelligence for physical security (executive protection, events, travel, buildings, et cetera). The purpose is monitoring for hazards, weather, protests, unrest, geo-political issues, travel by-country events, government alerts, and other resources. Essentially, the physical concentrates on the human individual, the employee, the executive, or the board member. On the cyber side of the house, threat intelligence monitors system and infrastructure vulnerabilities, exploits, threats, possible risks to the organization, threat actors, tactics, modus operandi, techniques, etc. The industry trends point to a combined threat intelligence offering that includes physical and cyber-related intelligence. It's more common for an incident to start as a physical one and merge or morph into a cyber one. We often see this with activists and protests, staging a sit-in or demonstration at the biotech lab of a pharmaceutical company that then escalates into a cyber hacking campaign targeting systems, users, and the like.

How do you create a unified security strategy that addresses physical and cyber vulnerabilities?

Most organizations of the more significant enterprise kind will likely have two separate departments, one for physical and the other for cyber/information security. In this realm, close collaboration and shared work products will be important for success, so the finished product, or actionable alerts or threat profiles, is ever encompassing all security facets. In those organizations that are ahead of the curve and have both physical and cyber security reporting to the same head of department, again, you'll likely have separate teams, and again, close collaboration will be necessary. Strategies are important and understanding the needs of the business and what factors can impact the business is important to assess annually and as needed. Building a strategy that is a "one voice, one team" mindset will help support this initiative.

Can you share an example where physical and cyber security teams worked together to mitigate a significant threat?

A perfect example of this was during my time leading cyber security at Levi Strauss, and in support of Super Bowl 50 (2016), Levis Stadium was the host stadium for the event. My team, along with our physical security team and Stadium physical security, collaborated on overall security efforts in alignment with the NFL and government organizations. In addition to the actual game, corresponding events were being held in San Francisco, including retail operations and other departments participating. The coordination and collaboration across teams made the events successful, having no issues that turned major.

What role does IoT and OT play in the convergence of physical and cyber security?

This is a great question because this subject has started to gain a lot of visibility in the last couple of years. I compare IoT/OT as a concern to IT in the 1990s. IT has generally been solved in terms of best practices, industry standards, etc. IoT, especially OT, which has been around for a while, has yet to be focused on for some parts, especially in private industry manufacturing and production spaces. Anything critical infrastructure, like oil and gas, has had more attention per se. From a cyber security point of view, in looking at the various security and compliance frameworks, like NIST 800-53, NIST CSF (Cyber Security Framework), or ISO 27001, while all of these are focused on cyber and information security, there are included parts that cover physical security as well.

How can organizations prepare their security operations to handle hybrid threats effectively?

This comes down to the scope of the threat. Security operations need to be focused and encompass all facets of security, both physical and cyber (be in the same room), and work closely together; otherwise, time gaps become an issue, and your output on threat advisories and actionable threats becomes slow, mismanaged and lost, with a greater chance for the target of the threats to be negatively affected, harmed or killed. Hybrid threats can morph, change, shift, and escalate quickly. Governmental “hybrid threats,” like interference in election processes, could have and contain the same or similar actions of a Corporate “Hybrid Threat,” like the targeting of an executive because an animal rights organization didn’t like the tactics of animal clinical testing. In managing security operations effectively, your threat analysts need to understand the target in great detail, whether a congressman or a Chief Executive Officer. Understanding where there might be a vulnerability with that individual target or breaks in physical security protection of a building that might be a target, and even the computer systems that target may have access to, that could be compromised somehow. Conducting assessments at regular intervals is always important, and conducting “advanced” security assessments for traveling individuals is also important. Plan, Plan, and more Planning is necessary. Then, a good threat intelligence program will have a deep understanding of the various known threats and groups or individuals behind those threats or could potentially become a threat based on other events if we take, for example, the animal rights movement. There are layers of groups that play a part in a threat campaign. This typically starts with a low-level organization that conducts peaceful protests and writes letters of opposition and other similar activities. Very low level, First Amendment protected activities and usually no arrests. Then, secondary groups come into the picture. These are typically anarchist groups or groups of individuals that push the line by conducting sit-ins or locking themselves to plant operation equipment or other objects. These groups use physical actions to apply pressure and essentially advocate for violence over voice. The destruction of public property, such as retail stores, corporate offices, and vehicles, is a common target. I will say the anarchist groups in the United States, while they can be extreme, their counterparts in Europe can be 1000x worse. Then, the next group is your extremists, who often fall under domestic terrorism and carry out physical harm, kidnappings, bombings, and other extreme activities. The bottom line is that knowing your adversaries and groups targeting your organization is key, as well as understanding the levels of activity that could be taken or used during an event and strategizing on the best mitigation plans as we advance.

What are the key indicators of a well-integrated physical and cyber security program?

The two most important aspects of any security program involve the detection of threats and quick response to those corresponding threats. With an integrated physical and cybersecurity program, success would be defined by improved threat detection and response capabilities through both teams' close working collaborative integration. With an integrated effort, there should be an improved and comprehensive understanding of potential threats, a better understanding of those threat actors, and improved response times. All of this results in mitigating these threats so they don't become risks for the organization. Additional key indicators should include reduced response time from the original event detection, reduction in incident severity, and improved risk strategies.

Many organizations also face the issue of protecting sensitive data they may possess. This is where an integrated physical and cyber security program also intersects, as physical security focuses on measures and policies to safeguard and secure access to server rooms and data centers, and cyber security addresses logical access control by users and reduces which users have access to the sensitive data. Insider threats are another area that bodes well with an integrated physical and cyber security program, as both groups would be responsible for these cases. In this instance, insider threats are criminal and malicious cases that might result in an arrest, prosecution, or other actions. Physical security handles cameras, badge access, and other physical security measures, which often play an integral part in an insider threat case.

How do you balance immediate incident response with long-term business-risk mitigation strategies?

Incident Response should be a collaborative and centrally managed program, especially in a large enterprise with multiple business units and countries. Some business units may have IT or security staff who will participate in the response activities, but your incident commander should be within your global security department. In risk management, and again looking at most security or compliance frameworks, incident response is integral within those frameworks. Breaches are a huge deal nowadays, and companies and customers want to ensure that the proper plans, policies, SOPs, and playbooks are in place in the event of an incident. How do we mitigate risks effectively in an organization? We plan, are proactive, have measures to detect events promptly and educate the workforce on how to recognize an event and report it timely. An event that becomes an incident should be handled promptly to prevent missed opportunities, downed systems, loss of sensitive data, etc. Planning and testing your incident response program is crucial to keep technical and executive teams up to date on your incident response plan and the cyber threat landscape.

In summary, what are your key lessons learned and what advice would you share with others tackling similar objectives or challenges?

- If your physical security and cyber security groups aren't currently aligned, start now and have meaningful discussions among the groups to determine how you can work closer, more collaboratively, and proactively. If there are "egos" in the way, it's time to put them aside and work together.

- Organizations should make strides to move from a "reactive security" stance to a "proactive security" stance. Think about security and privacy by design; bake security into everything from the beginning instead of making it an afterthought.

- Collaboration is your new friend. You should already be building relationships with your internal stakeholders and key partners in the organization where collaboration is important, in areas like HR-IT, Internal Audit, Risk Management, Travel, and PR/Communications. Oh yeah, and physical security, too.

- Be early, be aware, educate your workforce, and be Proactive in all you do. Talk to your Board, your executives, and your audit committee. Bring awareness of issues, key performance indicators or metrics, the maturity of your program, and fight for budget. Influence those responsible for budgets or approvals through thought leadership, demonstrate real examples of what ifs and what could happen, and build a strategy over 3-5 years.