THREE TRENDS SHAPING THE SECURITY SECTOR

ASIS INTERNATIONAL®

There’s only so much time security managers can devote to planning for the future and ensure the present day risk, safety, and security needs are being addressed. That time likely dwindled significantly as the COVID-19 pandemic unfolded.

Despite the near-term need to deal with organizational changes brought on by the pandemic, there remains a need for security managers to consider how their organizational environment is changing, and how that will affect risk management and security. *Security Management* recently caught up with David Feeney, CPP, CISSP, PMP, to discuss emerging trends impacting the security sector.

Feeney, a Deloitte risk and financial advisory manager in cyber and strategic risk, serves on the ASIS Standards & Guidelines Commission and has previously chaired the ASIS Physical Security Community and the ASIS ESRM Guideline Committee. He also led the The New NIST Privacy Framework session at GSX+ on Thursday, 24 September. A recap of our trends conversation is below.

Foresight and Preparation

Security professionals should ask themselves which type of security professional they want to be:

- The reactive type: The person who waits until her or she is asked about something new only to then scramble to get an answer for use in later follow-up. (Don’t be this person!)
- The prepared type: The person who is ready with an answer before an inevitable question is asked about something new. (Better.)
- The proactive type: The person who learns something new and brings it to stakeholders before questions are ever asked. (Bingo!)

The earlier security professionals learn about emerging trends, the further along that spectrum they can operate and the more value they can bring to their stakeholders.

1. Automation

One emerging trend is the next generation of automation, which includes robotic process automation, artificial intelligence, and machine learning. It is important for security professionals to understand these concepts and how they differ because each provides significant security value if used properly.

- Robotic process automation (RPA) is basic automation that repeats a scripted process. It is ideal for repetitive processes that require no logic or decision making but involve the same multi-step process being repeated cyclically. RPA adds value when it essentially scripts labor-intensive, repetitious processes to enable security professionals to use their time for more strategic efforts. Think “enter URL, scroll down, click button, click another button, close page, and repeat” – over and over. Such processes are ripe for RPA.
- Artificial intelligence (AI) adds logic. It is “smarter” than RPA in that it relies on logic to determine next steps. Unlike RPA, AI does involve decision making based on that logic. Also, unlike RPA, there is more than one possible series of tasks to be completed. It is the logic that determines those tasks.
- Machine learning (ML) adds the ability to learn. It is an even “smarter” type of AI that enables its logic to evolve based on lessons that it essentially “learns” through experience.

All three of these tools provide value by allowing security professionals to spend more time on cognitive work of strategic value to the organization. The further along the RPA-to-ML spectrum an organization goes, the more tasks it can automate, and the more human talent is made available for other work.

2. Data Privacy and Protection

Another emerging trend that security professionals should understand—yes, even physical security folks—is data privacy and protection. There are many aspects to this, but one that has dominated headlines is protection of personally identifiable information (PII). The rapid increase in number and severity of private and public sector data breaches has given rise to a rapid increase in data privacy laws from various global regions, countries, and states. The European Union’s General Data Protection Regulation (GDPR) and the U.S. California Consumer Privacy Act (CCPA) may be among the most well-known, but other laws and regulations are affecting how organizations host consumer and other data. As new ones hit the books, the complexity of reconciling sometimes conflicting guidance only increases.

To try and offset that complexity, the U.S. National Institute of Standards and Technology (NIST) has released its Privacy Framework this year. The framework helps an organization document its current privacy risk posture and identify a path to its desired future state through a gap analysis and roadmap creation. It doesn’t directly provide an understanding of privacy laws, but it does map out what a comprehensive data privacy and protection should include.

Finally, facial recognition software has recently been put under the microscope due to concerns with privacy. While we may sometimes think security and privacy are always complementary, they can be at odds with each other. Balancing these will become a narrower path as time goes on and privacy incidents continue to increase.

3. Security Convergence

One other trend that is continuing to emerge is security convergence. Specifically, two specific changes are gaining popularity:

1. Integrating physical access control systems with security incident and event management (SIEM) systems. SIEMs act as central hubs to many integrated subsystems, though these subsystems have traditionally been other cyber systems. In recent months and years things have changed, most recently the integration of physical access control data. Part of the credit for the increase in popularity is disruption caused by the COVID-19 pandemic, as access control data gives cyber analysts an indication of how many people are walking through specific areas. Pairing this data with other data sets from Wi-Fi access points and other sources can help identify overcrowded in-person gatherings or physical locations.

2. Reorganizing security silos so that the CSO/physical security lead reports to the CISO/information security lead. While a role reversal from what some of our tenured security folks may have experienced shortly after 9/11, this organizational alignment of physical and cybersecurity under information security has been making sense for an increasing number of organizations lately. If your organization follows this path, it will be important to understand the priorities, strategy, and language of both physical and cyber security.