VANDERBILT

News

What’s Worrying Today’s CSO?

BY ERIC WIDLITZ

I spend a lot of time talking with security leaders and integrators serving clients across enterprises about the challenges they face. Many require a tailored approach to building a security solution, but the same challenges pop up time and time again in conversation. Today's Chief Security Officers (CSOs) are worried about their investment, but more than that, they're worried about preserving employee safety, the safety of their data and the ability of their systems to integrate fully.

Employee Safety

It's not a secret that workplace violence is on the rise in North America – and across the world – and security leaders are tasked with keeping this in mind while also protecting

visitors and assets at the same time. More than once per day, on average, someone is killed in a workplace violence incident. The Bureau of Labor Statistics found 417 incidents of workplace violence in 2015, up from 403 the year before. And those are the lethal incidents. Around 2 million non-lethal attacks occur each year at workplaces, according to the Occupational Safety and Health Administration. That's a staggering number.

The balance of keeping employees, visitors and assets safe is a tough one, and in many instances this must be carried out while delivering an open and welcoming environment. One way this can be accomplished is by integrating multiple security systems together, including access control and video, so that security officials can keep a close eye on exits and entrances for suspicious behavior from a former employee or known harasser.

Another critical component of implementing these strategies comes from providing extensive training for employees on internal processes and procedures for dealing with potential threats. Access control through automatically locking doors, for example, can only go so far if the same doors are propped open for anyone to come in and out of a building. Training employees of the danger this can present is paramount to a comprehensive safety and security plan for an organization.

Cybersecurity

Upgrading or investing in new security solutions can be a costly endeavor for many

organizations, so making sure the solutions in place are secure is imperative. Cybersecurity and keeping networked systems safe is top-of-mind for today's security managers, since one attack on an organization can bring a company to its knees and shut down business altogether. With the rise in cloud technology and increased connectivity of devices, encrypting communications between devices is paramount – and it starts with manufacturers. Especially when legacy, new and different technologies are used together, a single insecure system or poor deployment can make the entire system vulnerable. This is where a strong relationship with IT professionals throughout the process of a security system upgrade can be invaluable.

With technology continuing to embed itself into our everyday life, it's important that the security industry proves its agility, adaptability and dependability in keeping up with remote and instant access to security solutions, but this must be weighted with the ability to keep data safe and secure from threats.

Integration

We use this term a lot in our business, but its frequent use doesn't lessen its need. Integrating systems together allows today's enterprise organizations to more easily manage risk with fewer resources, thereby maximizing investment. For a long time, manufacturers concentrated on providing products that worked well with other products within their own

lines, but those days are long behind us as open platform technology has emerged as a game changer. Open platforms allow integrators to better tailor a solution in accordance with an end user's needs and allow legacy systems to work seamlessly with new investments.

Going even further, many manufacturers have software in place that will bridge two systems together to allow disconnected systems to talk to and share data with one another. For example, some software programs will allow programs that manage human resources or event management to communicate with access control systems to streamline access at specific times of day or automatically update when an employee is terminated.

The CSO within most organizations is tasked with managing a wealth of challenges, but these three stand out consistently as the main focus for many of them. Using open platform technology that communicates by using encrypted communication protocols, as well as supplying employees with training and proper procedures for dealing with security in their day-to-day lives are all a part of meeting these challenges for enterprise organizations.

This article appeared in Security Magazine