brivo®

REDUCE RISK:

UNDERSTANDING CYBERSECURITY IN YOUR PHYSICAL SPACES. EXPERT ROUND UP ADVICE

Stay Secure...

According to a recent poll, 63% of security professionals believe cybersecurity is of high importance to their organization. However, this same poll revealed 40% of security professionals believe their systems are only somewhat secure against cyber vulnerabilities. It's easy to ignore the scale of cyber crimes if you haven't felt a personal impact yet. Did you know this year the GDP of cyber crime will hit $1.5 trillion, making it the 13th largest economy in the world?

WE PUT TOGETHER THIS ROUNDUP OF ADVICE

AND EXPERIENCES FROM EXPERTS IN THE FIELD TO HELP YOU:

1. Understand cybersecurity and its relationship with physical security systems
2. Work more closely and improve relations with your IT department
3. Prepare yourself and organization for potential breaches

YOU CANNOT PROVIDE GOOD CYBERSECURITY WITHOUT GOOD BUILDING SECURITY.

The reality is understanding cybersecurity and its relationship with physical security systems is important. Clifford F. Franklin, Owner & CEO of Sabre Integrated Security Systems says, "Any money you spend on cybersecurity will be wasted without having your physical security under control. To achieve good cybersecurity, you must first control the perimeter of your assets, whether physical or logical. Some important questions to ask yourself are - Do you have an audit trail with visual verification of personnel entering your office? If you don't - do you have these controls in vital network infrastructures like server rooms? If you can't protect your entire perimeter, at least start with your network infrastructure.

I urge you to get your company's security, facilities and IT teams working on a coordinated security plan. You can't have good cybersecurity without good building security and if both of those groups aren't working together, you most likely can't have either."

WORKING TOGETHER WITH YOUR IT DEPARTMENT IMPROVES YOUR ORGANIZATION'S OVERALL CYBERSECURITY.

Rueben Orr, President & GM, Security Install Solutions, explains, "About 10 years ago, there was a push for physical security to catch up with IT organizations. As a result, most manufacturers developed products to communicate across networks. This almost immediately drew lines between security and IT practitioners causing a lack of control and communication. What started as a disconnect resulted in animosity between these two organizations, ultimately forgetting about the common goal of storing and protecting an organization's data. This created havoc for both the physical security integrator and the IT organization.

When a physical security integrator and IT can work together, it reduces cost and can also reduce the amount of system downtime. IT departments, without working in coordination with physical security, have their own policies to adopt including network scanning, looking for devices they don't recognize, and applying patches to networks that would shut down ports commonly used for physical security devices. By working together, the system has a better chance for surviving an attack."

BUILDING A BETTER RELATIONSHIP WITH YOUR IT GROUP HELPS YOU BECOME BREACH-READY.

Ron Chandler, CISSP and VP of Enterprise Solutions at Guidepost Solutions, provides some tips, tricks and methods to help you build a better relationship with your IT group:

1. Be Better Partners With IT

Understand a few things about each other to get to common ground quickly. Ease into requests to be a better partner, as they are probably scaled to meet the bare minimum of their internal responsibilities for the corporation.

2. Own and Arm IT With Relevant Information

This assists in your company's breach readiness program and helps prevent physical security and corporate production outages. It also allows them to conduct proper resource and capacity planning.

3. Rely on IT's Mature Oversight and Management

For example how they conduct discovery scanning of devices on the network that may or may not be hidden.

4. Become Breach-Ready

When a breach happens, you have to be ready with information for the incident response team. This includes a list of all IP devices, ensure vulnerability management SOPs are in place and assign a person in your staff to participate on the incident response team."

Many organizations, especially ones with multiple facilities, struggle to keep up with maintenance and updates to their servers. Time and resources are of the essence and dedicating people to this task every month can be overwhelming. That's why timely and automated updates are one of the biggest benefits that most cloud (or SaaS) providers make available. Think about your phone. Every time there's a new iOS or Android update, all you have to do is click on the update link and it's taken care of. The same experience holds true for cloud-based access control. Your internal IT and security staff don't have to keep up with the latest cyber threats; your cloud provider will do that for you.

TIP 4

THERE'S A LOT TO CONSIDER WHEN HANDLING RISKS.

Matt White, Senior Manager, Americas Region - Enterprise Risk Management & Security, TE Connectivity provides his list of questions to consider when deploying any kind of system:

- What are these threats? Why are they threats?
- Where does your physical security fit in as technology evolves?
- What's your plan for potential reputational risks to you and your profile and how would you handle potential media attention? (This is not to be underestimated as more high-profile companies are targeted)
- How are you going to stay ahead of the incident instead of waiting - which can often be disastrous?
- Do you understand the consequences in terms of data privacy as you shift to cloud services?
- Are you aware of who's coming in and out of your buildings? Do you have sufficient access control in place?
- What are you doing with the visitor management access control data you're compiling? Are you sufficiently protecting it?
- Can your manufacturer prove a pen test?
- Do you understand what your integrator is installing on your network? Do you really understand the technology?
- Do you understand the IT department's requirements? Can you understand their language?

To determine whether a manufacturer is providing good cybersecurity, look at how they build their products, deploy their products and manage their people and procedures internally. At Brivo, we build end-to-end security designed for IoT using the strongest encryption for communications. Our hardware uses embedded bot monitoring and real-time alerts to take corrective action. We deploy our applications with regular and automatic software updates and pre and post deployment scans of software and systems. We manage our business by monitoring and managing what employees can access, and conduct 3rd party audits on our software, hardware, and internal processes.

LEARN HOW BRIVO CAN HELP YOUR ORGANIZATION

SCHEDULE A DEMO

brivo®
simply better security

7700 Old Georgetown Road, Suite 300
Bethesda, MD 20814

1.866.692.7486

brivo.com