Integrating IT and Physical Security

Two worlds need to converge in the security system sphere. While IT systems are poised to counter or prevent any credible digital attack, physical teams continue to focus on threats such as fire, flood, and physical intrusions. In some cases, these physical systems are monitored by multiple teams, making the process even more splintered.

```
 + 1 ) % $columns == 0 )
classes[] = 'last';
_link = wp_get_attachment_url( $attachment_id );
 $image_link )
continue;
                = wp_get_attachment_image( $attachment_id,
_class = esc_attr( implode( ' ', $classes ) );
_title = esc_attr( get_the_title( $attachment_id ) );
 '<div class="slide easyzoom"><a href=
 , wp_get_attachment_url( $attachment_id )
 _size', 'shop_single' ) ) );
loop++;
```

Friction Between Physical and IT Security

Some of the most frustrating inefficiencies in your physical and IT protection system are the overlapping areas and blind spots. An overlapping area occurs when two or more teams and systems are focused on a single threat. Blind spots occur when no part of your comprehensive system is focused on a potential threat.

Infrastructure, Software and Monitoring Dissonance

If your safety system is monitored or installed by more than one team, then you could have dissonance between the infrastructure, software, and monitoring services. An alarm installation company may install the physical alarms and cameras in particular areas, but the monitoring team is looking for additional information from other areas.

Physical access concerns were shared by 73% of respondents to a recent security survey, but many IT monitoring teams continue to treat IT threats as more important or more necessary to monitor. This can cause friction between CIOs and monitoring teams.

Repetitive or Unnecessary Information Concerning Safety Breaches

When a monitoring team has an issue it wishes to bring up to other departments, it's crucial to have streamlined communication channels. One major pitfall in safety monitoring is the way in which information is processed and sent to relevant parties.

A tendency among monitoring teams is to overcommunicate about safety concerns. This can lead to burnout or losing the general survey amidst the minutiae. It's sometimes necessary to educate teams about the proper way to bring up safety concerns and the amount of information that's necessary to determine whether the threat is credible.

Alternative Responses to Safety Concerns

When a physical security hears about a cyber attack, they'll likely pass clients over to an IT team. Similarly, a hardware problem may then be sent to the installation team. Bouncing between teams and professionals is an inefficient way to deal with a risk or a blind spot in the safety system. Synchronizing communication of these various areas can streamline responses. This doesn't need to involve hardware, software, or team replacement, but it can be effectively managed using your legacy system.

How To Align Systems and Departments

Aligning goals and streamlining communication can not only improve the total security system but can also save money. Whether working through a central monitoring system or contracting with various teams, start moving in these directions to mitigate safety concerns and reduce your expenses.

In some cases, friction between teams is too much and you may need a new hardware or software approach. For most situations, however, the key issues relate to goals and communication. These issues can be targeted with improved education and goal realignment, which is more cost-effective than a total security system retrofit.

Align Goals Between Teams

IT and physical monitoring may seem to go hand in hand, but there can be fundamental goal differences between separate teams or professionals. It's estimated that 30% of network and security ops will have aligned goals by 2022. This is a drastic improvement from the approximately 1% of ops that were aligned in 2019. Stay ahead of the curve by moving in this direction quickly.

Improve Communication Among Security Professionals

Once your teams have aligned goals, it's time to improve communication channels. There are a stunning number of communication channels that need to be open and available to create a secure facility. Here are just a few examples of lines of communication that may be used during a threat:

- IT team to physical team
- IT safety to IT ops
- Monitoring professionals to CIO
- Safety teams to other business teams

Increasing directions and volume of communication result in increasing risk of miscommunication or other risks. By improving the volume and proper lines of information, a safety department can improve reaction times and reduce the risk of a serious threat.

Steps Toward IT and Physical Integration

Alignment of goals, integration of teams and streamlining communication are essential steps to improve a safety system and strategy. At Security Information Systems, we offer custom integration services to help you make the most of your security systems – legacy and new. Request a custom integration service to see how we can help you hit your targets and align goals among your safety professionals.