SMART BUILDING CONNECTIVITY

Data security

COMMSCOPE®

DATA SECURITY

Ensuring data security at the physical layer

Hackers aren't picky; give them an opening—at any level, through any device—and they'll exploit it. The results, as you well know, can be catastrophic. According to a July 2018 study by Ponemon Institute, the average cost of a data breach in the enterprise network is $3.86 million. Once hacked, the likelihood of being successfully attacked again within 24 months is 27.9 percent. The financial damage is just the beginning. Once compromised, it can take years for a business to regain trust and rebuild its reputation.

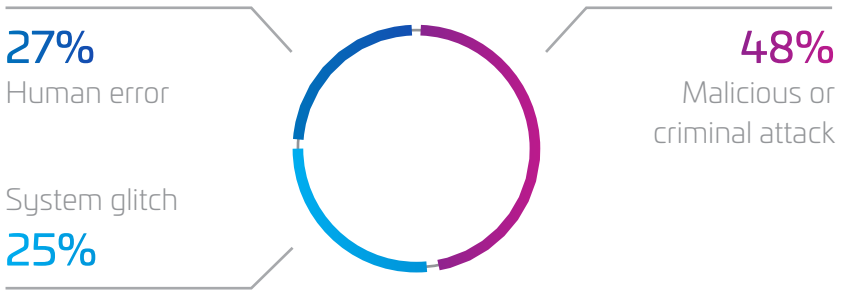
In today's hyper-connected smart buildings, every network connection is a door into your network. To avoid unauthorized access, you need to lock down every layer and secure every point of entry—from encryption at the application level, to authentication, virtual private networks (VPNs), firewalls and, finally, physical layer security. As with every element in the network, the physical layer infrastructure is a critical part of proper planning against intrusion or other worst-case scenarios.

60 percent of all data security breaches in 2015 were carried out by insiders with either malicious or inadvertent intent.

2015 Cyber Security Intelligence Index, IBM Security

Network infrastructure becomes an attractive target

Security has traditionally been implemented at the higher, logical layers of the network. As commercial building networks evolve, becoming more heavily integrated into all aspects of the enterprise, the physical layer becomes a more attractive target. Whoever controls the routing infrastructure of a network essentially controls the data flowing through the network. In industries such as healthcare and finance, the issue of network security has spawned new regulations and compliance requirements regarding data storage. Network infrastructure security concerns generally fall into two categories:



2018 Cost of a Data Breach Study, Ponemon Institute

- **Unauthorized access by an unauthorized person** can be reduced or prevented through the deployment of IP-connected cameras, occupancy sensors, access controls and other connected elements of physical security. Physical cabling security—such as keyed connectors, secure patch cords and port blockers—can be deployed to reduce the threat of unauthorized access. Similarly, automated infrastructure management (AIM) solutions can record and report any unauthorized activity on the physical layer.
- **Unauthorized access by an authorized person** can be more difficult to detect and repel since physical security may not be effective. In these cases, AIM solutions can automatically record and report the attachment of any unauthorized network device, including its physical location, and track all changes to the physical layer in real time.

Implementation Recommendations

The right connectivity strategy can go a long way to protecting your data from on-site attacks. Some important aspects to consider include the following:

Physical layer monitoring and detection

Automated infrastructure management (AIM) systems are unique in their ability to monitor and map all authorized and unauthorized changes to the physical layer in real time. Using intelligent cabling, connectors and patch panels, they automatically document all changes and alert personnel to new and non-scheduled connections, such as an intruder plugging in a laptop to gain unauthorized access. Alternatively, the AIM system can integrate with an existing intrusion detection system to identify and communicate the exact location to the intrusion detection system. Some AIM systems, like CommScope's imVision®, also can be integrated with enterprise anti-virus software to identify rogue or infected devices by physical location—minimizing the cost and damage during an attack.

In-building wireless

As hackers discover new vulnerabilities, protections once considered secure are being exploited. A good example is the WPA2 security protocol used by Wi-Fi systems. Using a weakness in the handshake between clients and WPA2 access points, intruders were able to break through encrypted connections. In a cellular or mobile network, security is administered and managed centrally by service providers. By necessity, these security measures are more robust and responsive than the legacy corporate Wi-Fi systems.

Security monitoring and sensors

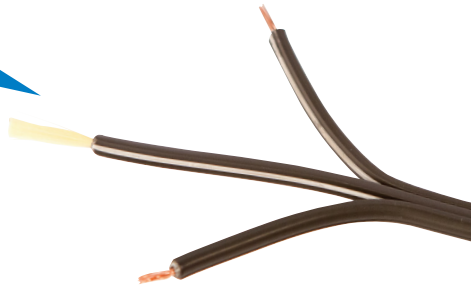
Enhanced connectivity like that found in intelligent buildings allows for networks of IP security cameras and occupancy sensors that help spot unauthorized intruders. With the right cabling infrastructure, these power-over-Ethernet (PoE) devices can be placed just about anywhere they're needed for optimal coverage.

Powered Fiber/PoE cabling

In a powered fiber or powered Ethernet network, all connected devices draw their power from the switches, which are typically backed up by UPS batteries and generators. This centralized power structure is inherently more resilient and secure. In case of a main power failure, the AIM system and all connected security devices will continue to function.

The CommScope imVision Controller X provides visibility of the entire connected environment

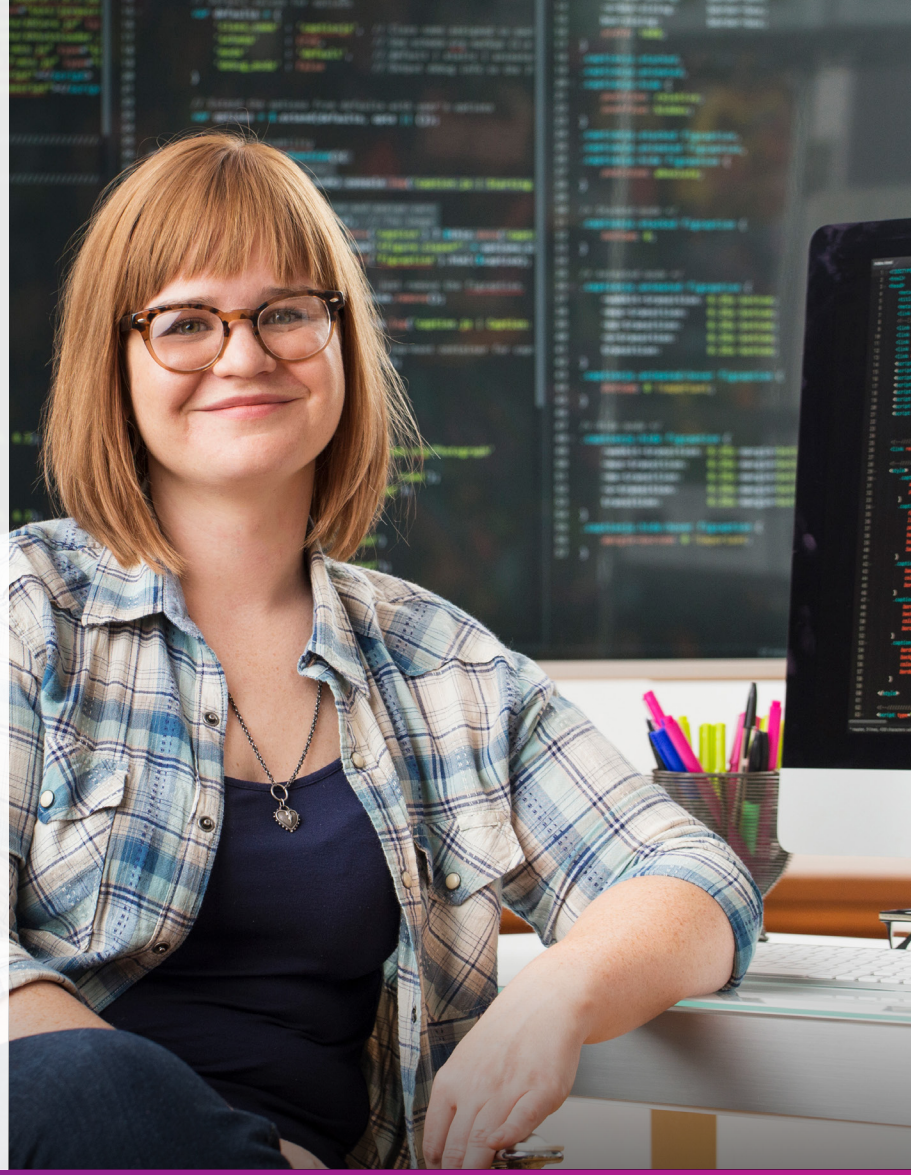
Powered fiber cable system



PARTNER WITH COMMSCOPE TO REALIZE THE POTENTIAL IN YOUR ENTERPRISE NETWORKS

As the enterprise network becomes more connected, securing sensitive data becomes more challenging. Staying one step ahead of the potential risks is a full time job. At CommScope, nobody understands your building's network infrastructure better.

For more than 40 years, CommScope has been the face of security and the driving force of innovation for commercial building networks. Our ongoing involvement in crafting industry standards and developing best practices gives us the vision and experience to help you create a smarter, more productive workspace. You know what you need—we know what's next. Together we can realize your full potential.



COMMSCOPE®

commscope.com

Visit our website or contact your local CommScope representative for more information.

MC-113149-EN_SECURITY