COMMSCOPE®

SMART BUILDING CONNECTIVITY

Data security

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.

CommScope recently spoke with **Jason Bautista, Manager of Technical Consulting for CommScope,** to get his views on how enterprise networks can protect their data.

Q Recently, a number of very large, very high-profile companies have come under scrutiny due to massive data breaches that have placed tens of millions of records at risk. While their size and market influence make them especially attractive targets, that doesn't mean less well-known business aren't at risk. What do they need to know?

A That's a great point. We live and work in a hyper-connected environment. IT has an important seat at the table now. Any business is at risk of a data security attack.

Q What are the most attractive targets?

A The obvious ones are those with huge volumes of sensitive data. According to 2018 figures from Ponemon Institute, financial institutions and service providers are the two most targeted. Surprisingly, industrial manufacturing is next.

Q Are hackers typically going after the data center?

A To some extent; but, more and more, they're going after the building's LAN environment. The enterprise ITC infrastructure is growing so fast—with in-building wireless, IoT networks, and building management systems all connected—it provides a huge number of entry points for a would-be intruder. Once inside, you'd be amazed at how easy it is to move around undetected.

Q Are these the remote "basement hackers" most people think about when they read about attacks?

A Definitely not. According to the Ponemon Institute study, nearly half of all security breaches occur from inside the building by authorized users trying to gain access to unauthorized data or by visitors who are able to quietly slip into an empty office and plug into an Ethernet port.

Q So, when enterprise network managers are assessing their physical layer for data security, what should they be looking for?

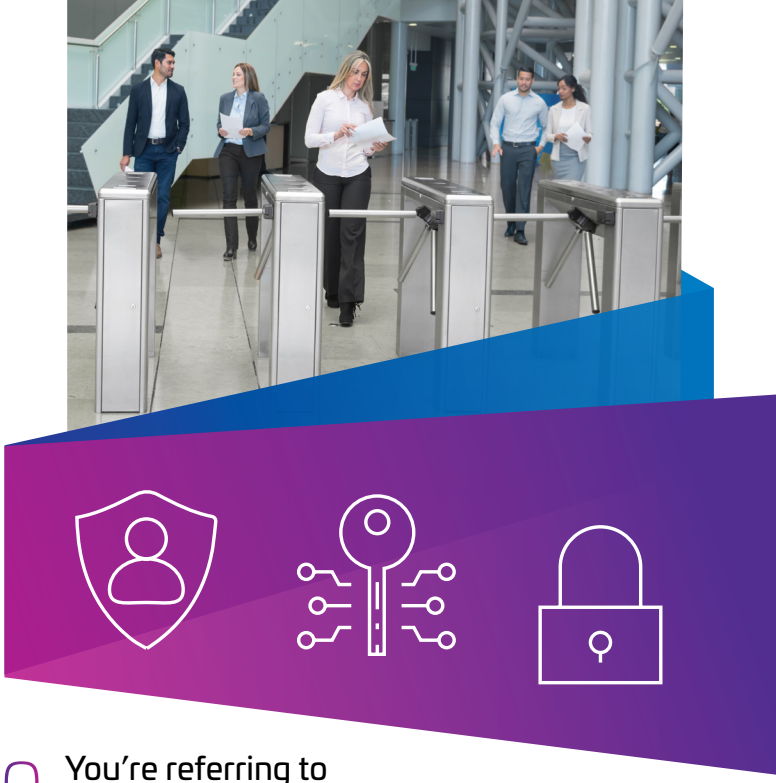
A Start with automated infrastructure security. Given the depth and complexity of the enterprise network, you have to be able to monitor and manage network connections from the inside. An automated infrastructure management (AIM) system enables you to do that. Using intelligent cabling, connectors and patch panels, it automatically detects and maps all physical layer activity at the port and device level, in real time. If an authorized user connects or disconnects a device, an AIM solution, like CommScope's imVision®, can automatically alert IT personnel.

Q Yes, but, in a large building, it could take hours to locate a rogue device.

A In the case of imVision, it knows exactly which port has been infiltrated and is able to provide the exact location of the attack. Alternatively, the AIM system can integrate with an existing intrusion detection system to identify and communicate the exact location to the intrusion detection system. There are also AIM integrations for enterprise anti-virus software that essentially do the same thing in response to virus detection.

Q Okay. So, beyond AIM, what else do you recommend?

A The next thing I'd consider is the distribution of internal security monitors throughout the building or campus.

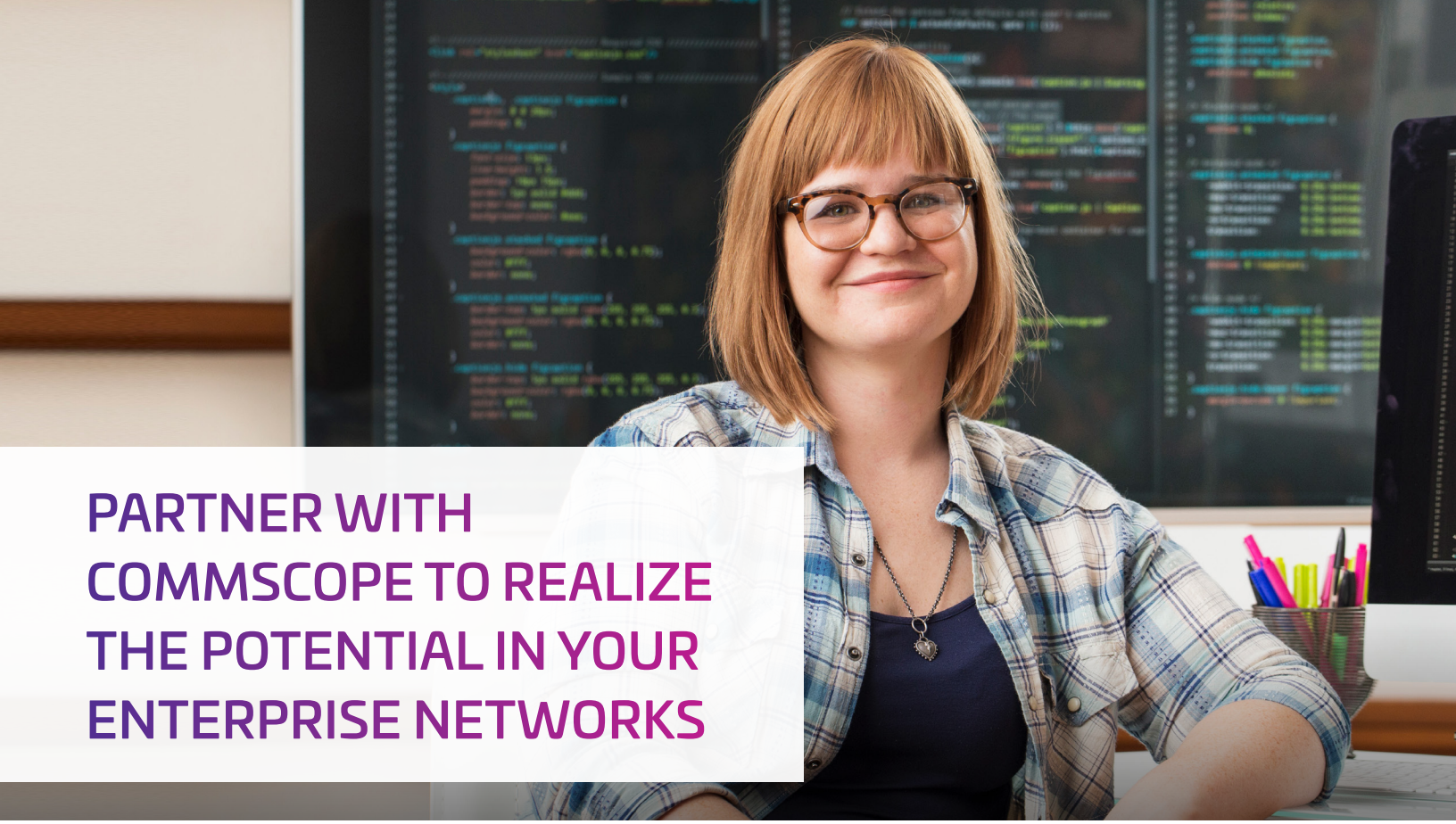


Q You're referring to closed-circuit security cameras?

A Exactly. An AIM system can only locate a would-be hacker. Cameras provide corroborating visual proof. Of course, you need cameras wherever people work, which brings us to the importance of your powered-fiber or power-over-Ethernet network. Today, most connected devices—sensors, cameras, controllers—can be supported using these low-voltage power/data networks. And, because the power is fed from the switch, which is backed up by UPS batteries, security—and anything else connected to the powered-fiber or PoE network—remains on line even if there is a power failure.

Q Anything else?

A The only other thing I'd consider is the in-building wireless system. A lot of companies and commercial building owners rely on corporate Wi-Fi. But, recently, hackers have figured out how to exploit a weakness in the WPA2 security protocol used by most Wi-Fi systems. In June 2018, WPA3 for Enterprise was released, offering the equivalent of 192-bit cryptographic strength. I think the jury is still out on its effectiveness. If you're not sure, you may want to consider a cellular or mobile network, powered by a dedicated DAS. The benefit is that security is administered and managed centrally by the service providers and may be a bit more robust and responsive than a legacy Wi-Fi.



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_QA