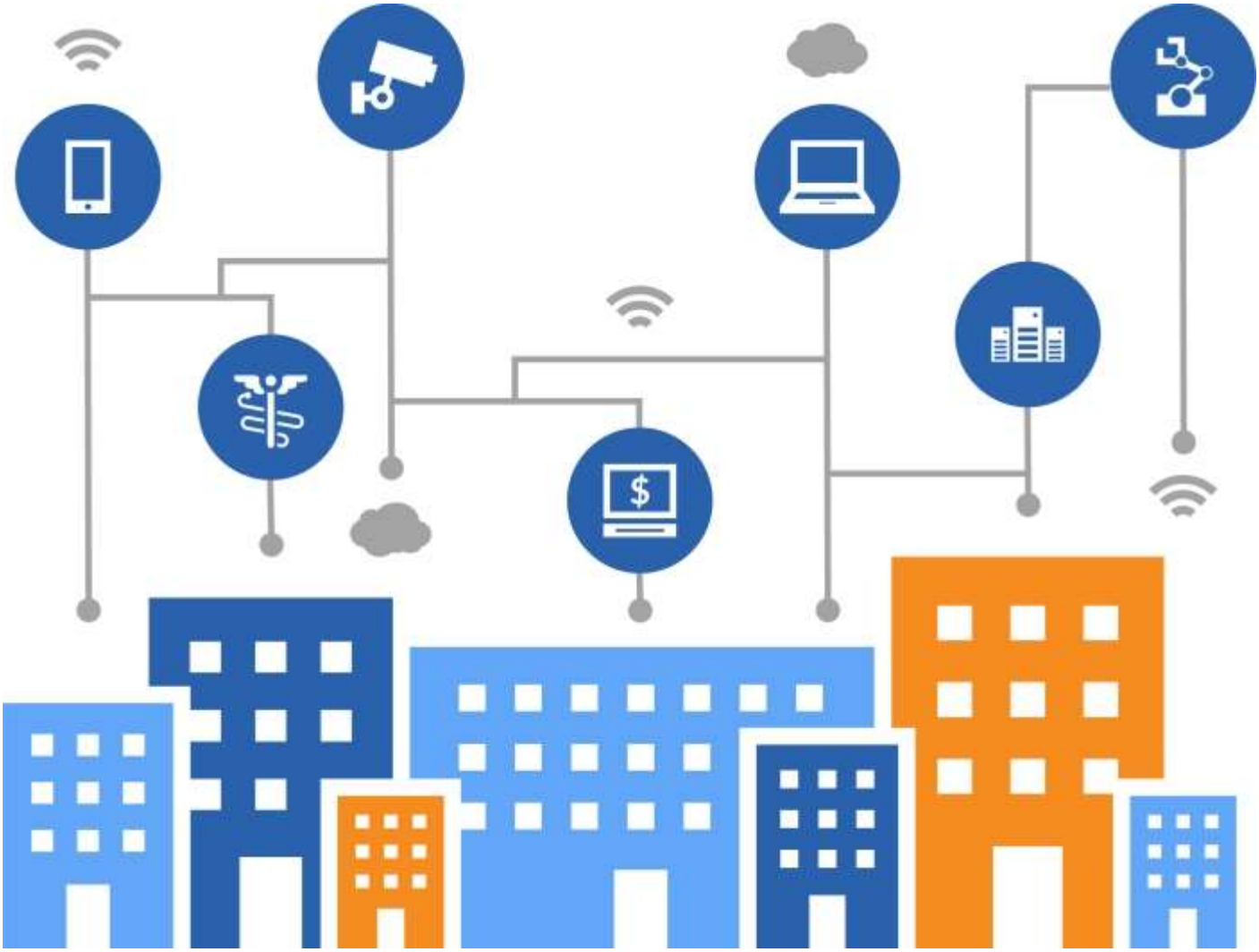
VOL. 18 NO. 9 – 3/1/2018

Smart Buildings Need Smarter Cybersecurity

JEFF HUSSEY, PRESIDENT & CEO, TEMPERED NETWORKS



Smart building technologies are shaping the future of our cities, driven by the need for energy-efficiency, wide-spread adoption of Internet of Things (IoT) platforms, and government initiatives. Seeking to reduce costs through increased operational efficiency and streamlined processes across IT, maintenance, facilities, distribution, and more, business are integrating these smart systems – such as Building Automation Systems (BAS) – across the organization on an ever-expanding scale.

Connectivity and Control Often Outweigh Security

One of the biggest concerns for network security practitioners is connected devices and systems that cannot protect themselves. This includes aging legacy systems, devices running un-patchable operating systems (e.g. Windows XP), and vulnerable systems often used in Industrial Control System (ICS) deployments. ICS, SCADA, and components such as HVAC systems, remote sensors, and IP cameras, have a single common denominator: **inherent vulnerability.** The primary goals of smart building technology are typically connectivity, control and monitoring, meaning security is often overlooked despite constant reminders from ICS-Certifying bodies and the Department of Homeland Security.

Most organizations maintain a relatively flat Layer 2 network. That means security, fire suppression, building access controls, HVAC systems, and other building-specific protocols are often on the same flat network as other systems, like HR servers, Finance, etc. Vulnerable devices and machines – like those mentioned above – are the weakest link and, when they operate on a shared network, it puts the entire organization at risk.

What's more, these security shortcomings present attackers with a way to move laterally within the network and compromise machines that could impact reliability and availability of entire systems – which could lead to service interruption, safety issues, loss of brand prestige and a negative impact to the bottom line.

The Root Cause of Networking Complexity

What many people don't understand is, despite all the layers of security in place and in the roadmap, most building automation systems remain vulnerable because they connect via TCP/IP: an inherently insecure protocol.

But why is TCP/IP insecure? Because it serves as a device's location and identity on a network. This exposes those devices to numerous attack vectors, such as IP spoofing. This fundamental flaw of TCP/IP is the root cause of virtually all networking and security challenges.

To combat this, network segmentation and device isolation are considered industry best practices. Most organizations turn to traditional segmentation tools like VLANs or leverage firewalls, managing certificates, ACLs, VPNs, etc. to accomplish this initiative.

These systems, however, often require new routing rules for certain traffic as

well as custom-configured policies for each system or location. This often results in high costs and only modest improvements in network security posture.

Firewalls can help limit traffic in and out of designated areas, but most firewalls enforce rules based on arbitrary (dynamic and spoofable) IP addresses. Furthermore, inside the protection of a firewall, devices are still able to communicate laterally and are often visible to the rest of the network. And, any slight misconfiguration of either the device or the firewall can be catastrophic.

Thankfully, with recent advancements in technology, this problem can be easily resolved. Rather than using ephemeral IP addresses for device identity, we can now use a unique host identifier that provides a more reliable attribute of identity. One such implementation is the Host Identity Protocol (HIP), an open IETF standard that adds a "host identifier" in the form of a cryptographic public key associated with the host. With HIP-based solutions, two parties must share a cryptographic binding before being able to see each other on the network; effectively hiding (cloaking) portions of the network that are not allowed to communicate with each other.

With HIP, IP resources can move anywhere in the world and maintain connectivity, regardless of whether they're in a static or dynamic IP environment. Now mobility and migration between buildings, remote offices, datacenters, shared networks, and multiple cloud providers is not only possible, but simple.

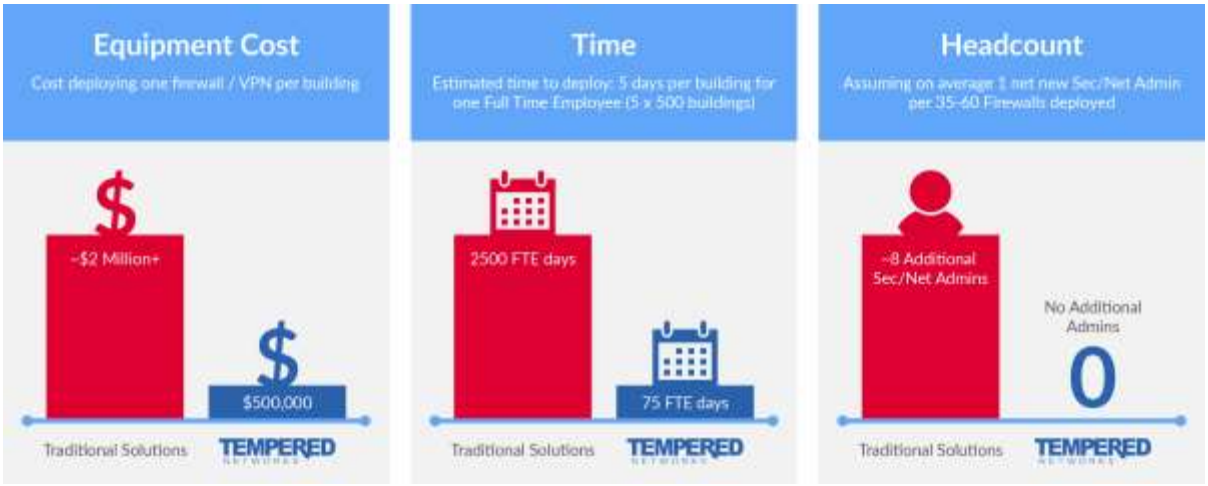
Smart Building Challenges – Beyond Cybersecurity

When we work with facilities and operations teams on building automation projects, they're also trying to optimize network performance and resiliency. For example, pervasive Building Automation and Control Networks (BACnet) systems can create broadcast storms that might cripple network performance. These traffic storms can cause problems for network administrators due to high signal-to-noise ratios and interference that can disrupt other IP traffic on the network. It can happen without warning and take down critical building services. Today, with proper micro-segmentation, you can improve overall network performance by restricting noisy traffic to encrypted network segments.

Successful BACnet Segmentation for a Leading University

We recently worked with Penn State University and its Facility Automation

Services team who was tasked with segmenting and centralizing the university's expansive BACnet system. In this case, the BACnet system-controlled HVAC, lighting controls, and access controls for classrooms, high-value research labs, and more. Over 640 buildings are spread across dozens of state-wide campuses. Their network attack surface was large due to many rogue access switches and wireless access points. With BACnet communications openly traversing Penn State's flat network, orders were to get the BACnet traffic segmented.



Tempered Networks' Identity Defined Network (IDN) solution enabled the facilities staff to rapidly segment their expansive BACnet system with centralized management across their entire deployment. The cost comparison was an eye opener for the facilities team.

"Alternative solutions would have taken us two to three years and require hiring net new technical staff to deploy and manage," according to Tom Walker, Systems Design Specialist at Penn State University.

In short, Tempered Networks' secure networking solution enables Facilities and Operations teams to remove the traditional networking obstacles and:

- Easily connect, control, and secure building automation systems to optimize efficiency
- Enhance risk posture by reducing the network attack surface across the enterprise
- Improve overall network performance by isolating specific network segments
- Experience significant OpEx savings through simplified point-and-click management – no advanced IT skills required

Jeff Hussey, President & CEO, Tempered Networks

Jeff Hussey is the President and CEO of Tempered Networks, the pioneer of the Identity-Defined Networking market. He is an accomplished entrepreneur and business leader with a proven track record in the networking and security markets.