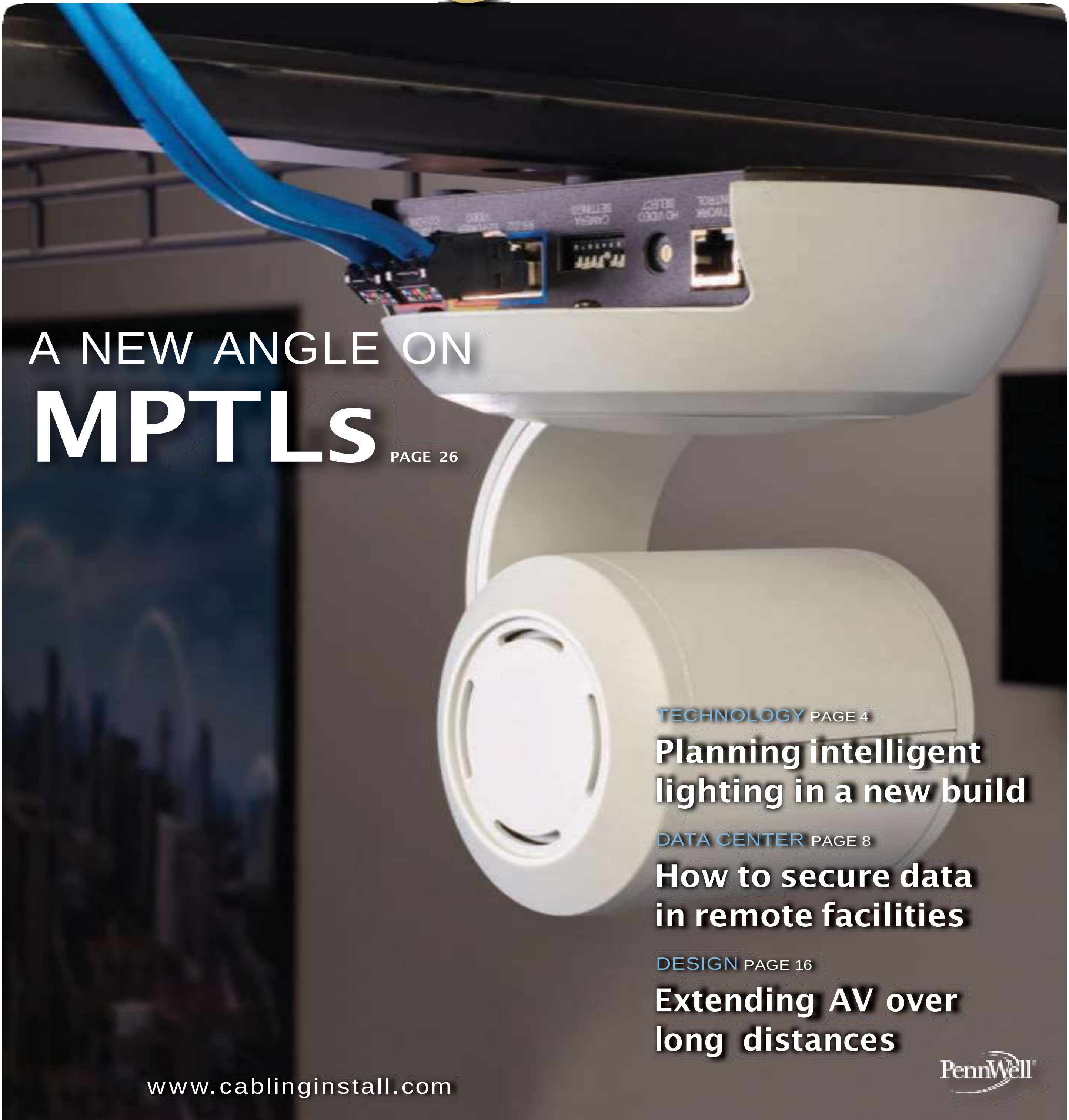
MAY 2018

FOR PROFESSIONALS MANAGING THE CABLE AND WIRELESS
SYSTEMS THAT ENABLE CRITICAL COMMUNICATIONS

Cabling Installation & Maintenance



A NEW ANGLE ON

MPTLs

PAGE 26

TECHNOLOGY PAGE 4

Planning intelligent lighting in a new build

DATA CENTER PAGE 8

How to secure data in remote facilities

DESIGN PAGE 16

Extending AV over long distances

www.cablinginstall.com

PennWell

Understanding data security concerns in remote data centers

With security breaches on the rise, compliance with regulations keeps a tight leash on enterprises.

BY RAISSA CAREY, Chatsworth Products Inc.

In 2017, recorded U.S. data breaches hit a new all-time high of 1,579, up almost 50 percent over the previous year, according to the Identity Theft Resource Center. This should come as no surprise, considering that also last year, data has taken the place of oil as the world's most valuable resource.

For data centers, privacy and physical security of servers and switches have always been a critical priority, but increased migration toward remote edge compute sites and multitenant data centers (MTDC) has made remote management and access control of the data center cabinet more complex and challenging.

Furthermore, growing data privacy regulations such as the Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI-DSS), Federal Information Security Management Act (FISMA), and the upcoming General Data Protection Regulation (GDPR) are driving the need for more-stringent cybersecurity measures, including closely controlled access to cabinets where servers and switches reside.

Regulations and physical security compliance

Certain segments of the industry—particularly healthcare and financials—look at cabinet access control more strictly, requiring a detailed report of who, when and why the cabinet was accessed. Generally though, all regulations simply require physical access control measures to be in place, but it is up to enterprises to decide which specific method or technology to use.

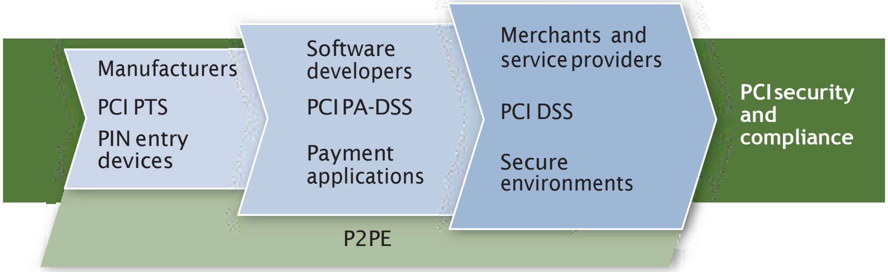
Here are a few regulations worth knowing for proper compliance.

FISMA—Federal Information Security Modernization Act. Based on the 2013 Executive Order "Improving Critical Infrastructure Cybersecurity," the National Institute of Standards and Technology (NIST) published a cybersecurity framework to guide companies' cybersecurity risk management processes. Access control is an element of the frameworks core function.

- Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions, under which:
  - Identities and credentials are managed for authorized devices and users.

Payment card industry security standards

Protection of cardholder payment data



Standards in the payment card industry incorporate an ecosystem of payment devices, applications, infrastructure and users.

- Physical access to assets is managed and protected.
- Remote access and access permissions are managed.
- Network integrity is protected, incorporating network segregation where appropriate.

HIPAA—Health Insurance Portability and Accountability Act. The Centers for Medicare and Medicaid Services (CMS) has the rule titled “Security Standards for the Protection of Electronic Protected Health Information,” which requires covered entities to “implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed. Access to hardware and software must be limited to properly authorized individuals.”

Additionally, companies under HIPAA are required to document access attempts, including dates and reason for access. These notes can vary from a simple logbook to a more-comprehensive electronic database.

PCI DSS—Payment Card Industry Data Security Standard. The PCI Security Standard Council (PCI SSC) created the PCI DSS to protect cardholder data in the digital age. Vulnerabilities appear everywhere in the card-processing sphere, including point-of-sale devices, wireless hotspots, e-commerce, transmission of cardholder data to service provider, etc.

One of the requirements of PCI is to restrict physical access to cardholder data, such as the following.

- Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.
- Develop procedures to easily distinguish between onsite personnel and visitors, such as assigning ID badges.
- Use a visitor log to maintain a physical audit trail of visitor information and activity, including visitor name, company, and the onsite personnel authorizing physical access.
- Retain the log for at least three months unless otherwise restricted by law.

Saas SOC-2—System of Organization Control (SOC) reporting for service organizations. Developed by the American Institute of Certified Public Accountants (AICPA), SOC 2 is a framework that helps service organizations put cybersecurity processes and controls in place. The criteria include several considerations to ensure the prevention of intentional or

unintentional security events, including the following.

- Protection of data whether at-rest, during processing, or in-transit
- User identification, authentication, authorization and credentials management
- Physical and logical access provisioning and deprovisioning, including remote access
- Operating location and data center physical security and environmental safeguards

GDPR—General Data Protection Regulation. GDPR is part of the European Union's data protection reform and is a strict set of regulations that gives data protection and security policies a new level of priority. While EU countries must comply, any organization collecting or processing data for individuals within the EU should also be developing their compliance strategy.

Data centers in particular will need to be able to demonstrate examples of "preventing unauthorized access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems."

GDPR is slated to take effect in May 2018.

Actionable considerations

Cabinet-level security is the first line of defense for data centers' data protection and security policies, but what has worked in the past is no longer adequate to meet the challenges of the future. When reassessing cybersecurity processes and controls, IT teams should consider these questions.

- Does IT have safeguards in place to control physical access to sensitive data?
  - The access control solution should be easy to manage remotely.
  - Consider multiple layers of security, including dual-factor, biometric authentication, as employee cards or keys can be stolen and used by unauthorized users.

This is the eConnect Electronic Access Control Swinghandle Upgrade Kit from Chatsworth Products Inc. The kit includes smart card authentication, as well as front and rear swinghandles.

- Is IT able to monitor who is accessing sensitive data both physically and remotely?
  - The access control solution should monitor swing handle and door conditions.
  - The access control solution should log and report every access attempt.
  - The access control solution should alert in real time when a door is tampered open.
- Does IT need to have an audit trail showing who has accessed sensitive data and when they accessed it?
  - At the very least, the access control solution should keep logs of access attempts, but ideally, it should be paired with data center infrastructure management (DCIM) software for more-granular reporting and trending information.

Simplified approach for immediate security in remote spaces

With concerns of data breaches on the rise, cabinet-level electronic access control with audit capabilities have taken a new direction—particularly within colocation and remote sites. Emerging trends indicate security integration within the space of intelligent power distribution, providing a simple and effective solution for physical access control, power usage and environmental monitoring. Deploying one system also nullifies the need for a separate source of power or network to the cabinet's electronic swinghandle locks.

This integrated approach provides a single view and the ability to manage power at each outlet and cabinet, monitor status of environmental conditions and control each cabinet access attempt with an audit trail report that is easily explorable via a user-friendly web interface—a documentation requirement by the key privacy regulations as described here. Further integration into DCIM software provides real insight and more-granular reporting of power and cabinet access. u

Raissa Carey *is a technical writer with Chatsworth Products Inc. (www.chatsworth.com). The topics addressed in this article can be viewed in a presentation titled "Managing Remote Sites: What to Manage and How?" which is available on Chatsworth Products Inc.'s website.*