ICT TODAY
THE OFFICIAL TRADE JOURNAL OF BICSI

July/August/September 2020
Volume 41, Number 3

Bicsi®

AV OVER IP AND COMPLEX ENTERPRISE NETWORKS

PLUS:

+ Simple AV Control Concepts
+ Overcoming Challenges at Carnegie Mellon University
+ Wireless Communication: The First Line of Defense for Schools and First Responders

Access Control at the Cabinet Level: The First Line of Defense in the Cybersecurity Roadmap

By Ashish Moondra

In a reality where data has become the world's most valued asset, cybersecurity has quickly taken on a new meaning within every IT budget. Privacy and ethical management of data are not only priorities but also law.

Within the many layers of cybersecurity, physical security is generally well understood in ICT, but when it comes to executing a simple and effective strategy, there are different opinions of what that strategy should be and how it should be deployed.

How often do enterprise organizations assess the required level of physical security for protecting data? Are they compliant with regulations that address data security? More importantly, how is their IT team applying physical security and complying with privacy laws within a hybrid data center architecture, where the data center, colocation, cloud and edge sites coexist?

When it comes to physical security, there are a few basic guidelines that should be part of a cybersecurity roadmap. But first, it is useful to know the applicable law within each vertical.

REGULATORY COMPLIANCE

The number of breached records in business organizations jumped significantly in 2019 with over 8.5 billion records exposed—that is more than three times greater than 2018 year-over-year—according to the *2020 IBM X-Force Threat Intelligence Index*. The report goes on to cite that the over 8.5 billion records that were compromised in 2019 was more than a 200 percent increase than those lost in 2018 and "The inadvertent insider can largely be held responsible for the significant rise."

Another report, *The Cost of Insider Threats: A Global Report 2020* published by IBM and the Ponemon Institute, states that insider security threats have increased significantly in frequency and cost. In fact, from 2016 to 2019 the frequency of incidents per company has tripled from an average of 1 to 3.2 and the average cost has almost doubled. Insider security threats mean that serious data breaches can be caused internally by disgruntled or malicious employees, contractors, those engaged in competitive espionage or other criminally-minded insiders within an organization. These statistics do not even account for the inadvertent insiders who may cause data breaches via human error and non-malicious intent.

The global average cost of a data breach in 2019 was $3.92 million, and the most expensive country in terms of average total cost of a data breach was the U.S. at $8.19 million, more than twice the global average, according to a study by Security Intelligence.[1] With each data breach costing businesses millions of dollars, regulatory compliance and strict cybersecurity measures are no longer a choice; they are part of the cost of doing business and must be closely watched.

All data privacy standards and regulations require physical access control measures for data processing and storage equipment, but with most regulations, it is up to organizations to decide which specific method or technology to use. Because of sensitive data privacy concerns, certain segments of the industry—particularly health care and financials—look at cabinet access control more strictly, requiring a detailed report of who, when and why the cabinet is accessed.

Regulations and access-control-related requirements ICT designers and installers should know include:

Health Insurance Portability and Accountability Act (HIPAA)

The Centers for Medicare & 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."

Under HIPPA, companies 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. The HIPAA rules affect organizations that handle individual health care records, such as pharmacy, dental, vision and medical service providers, insurance, billing, wellness programs, health tracking apps and even gymnasiums.

The Health Insurance Portability and Accountability Act access-control-related requirements include:

- Limit physical access to electronic information systems and the facility or facilities in which they are housed.
- Document access attempts, dates and reason for access.

The U.S. Department of Health and Human Services Breach Portal indicated more than a dozen organizations were being investigated from January-April 2020 for unauthorized access breaches with millions of dollars of expected fines.

Federal Information Security Modernization Act (FISMA)

Based on a 2013 presidential 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 framework's core function (Protect) which recommends:

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

General Data Protection Regulation (GDPR)

The GDPR is part of the European Union's (EU's) data protection reform and is a strict set of regulations that gives data protection and security policies a new level of priority. Although GDPR is an EU regulation, any organization collecting or processing data for individuals within the EU should also have a compliance strategy.

Data centers 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."

In the United States, the same concept was developed in California with the California Consumer Privacy Act, enacted in June of 2018. However, the new regulation does not include requirements for physical access control.

Payment Card Industry Data Security Standard (PCI DSS)

The PCI Security Standards 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-sales devices, wireless hotspots, e-commerce, and the transmission of cardholder data to service providers.

The PCI DSS compliancy affects organizations that handle financial transactional information, including financial institutions, merchants and service providers, software developers of payment systems, and manufacturers of PIN devices.

The PCI DSS access-control-related requirements include:

- 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.

All data privacy standards and regulations require physical access control measures for data processing and storage equipment, but with most regulations, it is up to organizations to decide which specific method or technology to use.

System and Organization Control Framework—Saas SOC 2

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 SOC 2 criteria include several considerations to ensure the prevention of intentional or unintentional security events, including:

- 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.

Summarizing Requirements

In general, compliance to regulations requires a method to:

- Physically secure data processing and storage equipment.
- Identify and manage authorized accessors.
- Manage access to the physically secure space.
- Keep records of access to the physically secure space.

FIVE CONSIDERATIONS WHEN BUILDING AN ACCESS CONTROL SYSTEM

1. Physical Security: First Line of Defense

Because most of the privacy breaches happen in the network, little attention is typically paid to physical security. It is important to remember that the intent of data privacy and security regulations is to prevent a data breach. Therefore, preventing a data breach should drive the decisions about physical security. Recognize that the final straw in physical security between data processing and storage equipment and access by unauthorized users is a secure server cabinet.

For an enterprise-owned, single-tenant site, for example, room-level security could be considered sufficient. Particularly in multitenant data centers (MTDCs) and remote sites, physical access control at the cabinet level simplifies management and prevents unauthorized users to access the servers and switches in which data is stored (Figure 1).

Many enterprises would probably argue that they already comply with privacy regulations. After all, most data center cabinets have keyed locks and the keys are carefully controlled. Well, how do they ensure that doors

FIGURE 1: To prevent unauthorized users to access the servers and switches in which data is stored, physical access control at the cabinet level is crucial.

are secured? How do they document access to cabinets? How do they recover keys from users? What is the response when a key is lost or stolen?

Electronic lock and access control systems automate monitoring, documenting and control of access and allow fast reprogramming if access rights change or if a credential is lost or stolen. These types of control systems support three levels of access:

1. Something a person has – Access card
   - Assign and change credentials quickly without the need for changing the locks, but an access card can still be lost or stolen
2. Something a person knows – Keypad password
   - A password is more difficult to steal, but it can be guessed or reprogrammed
3. Something a person is – Biometrics
   - Biometric authentication is uniquely associated with an individual digital print and is only allowed for rare instances of fraud (Figure 2).

Additionally, it is important to consider the levels of security for each type of access: single-factor or multi-factor authentication. Factor refers to the number of unique keys required to access the cabinet. Used individually, access cards, keypad codes or biometrics are also single-factor. However, electronic lock keys are easier to use in dual and multi-factor combinations. Dual and multi-factor keys reduce the probability of access by an unauthorized user (Figure 3). Dual and multi-factor systems may require an upgrade at the electronic lock to include an additional reader.

2. Key and Rights Management

When keyed locks are used to secure equipment cabinets, companies must have a strong and completely effective key management program. This requires escort of visitors and/or recovery of keys when users enter and exit the facility, recovery of keys from any exiting employees and rekeying of cabinets when keys are lost or stolen.

FIGURE 2: Electronic lock and access control systems introduce three levels of security: something a person has, something a person knows or something a person is.

FIGURE 3: Locks with multi-factor capabilities combine multiple key types to enhance security and connect credentials to specific authorized users.

Keyed locks provide limited rights management. Typically, all cabinets are keyed alike. It is possible to use combination locks or have groups of cabinets keyed differently to limit access for cabinets to groups or individual users, but this requires a strong system for documenting assigned combinations for key management.

In contrast, electronic locking can be reprogrammed quickly with new access codes, and no hardware modification is required. With electronic locking, it is possible to assign individual users and individual cabinet access rights. Each user can have different and specific access rights. The setup of rights in the software is simultaneously documenting the assigned access codes (keys).

3. Logging Reports and Auditing

Having users sign in at a controlled front building access documents the person's presence in the building but not their access to individual cabinets. To create a report of access to individual cabinets, the IT team could review security video footage and annotate dates and times or assign escorts and keep manual records, then generate reports of access from those records.

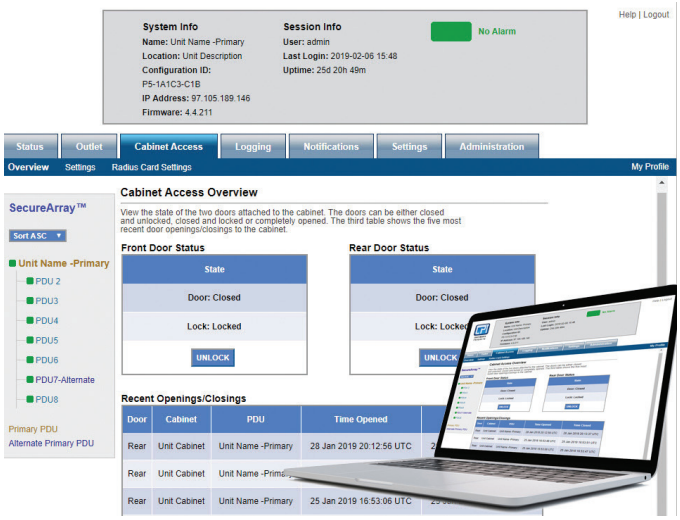

FIGURE 4: Remote visualization and control of the status of the cabinet doors help IT and cybersecurity teams to be aware of any access attempt, and then take the necessary proactive measures to remain compliant with privacy regulations.

Electronic locking and access control systems automate the logging of access at the cabinet level and enable automated reporting by user or cabinet. This speeds preparation for an audit and helps narrow the scope of event investigations.

4. Event Response

When a data breach occurs, immediate event response is critical. With a keyed lock system, IT must manually check the condition of doors and locks. If a key is lost or stolen, they must rekey the lock. Reporting requires manual collection, review and preparation of records.

Electronic locking and access control systems simplify, shorten and, in some cases, automate these responses (Figure 4). The IT department can quickly disable a credential or reprogram locks, and it can be proactively notified if a door is left opened or unlatched (unlocked).

5. Jurisdiction: IT or Facilities Management?

In most data center facilities, security is deployed via a building management system platform, owned and managed by facilities management. However, when it comes to data center cabinets and systems, security is most often controlled by IT, given it is the IT department that oversees data protection and the controls applications that reside in the equipment. It would be wise for IT managers to obtain an understanding of the building management system and the ICT connectivity infrastructure supporting it. Likewise, it behooves facilities management to understand better the responsibilities and functions of IT for a unified team approach.

Electronic lock and access control systems automate monitoring, documenting, and control of access and allow fast reprogramming if access rights change or if a credential is lost or stolen.

ESSENTIAL CONSIDERATIONS FOR RACK-LEVEL ELECTRONIC LOCK SOLUTION

Given the five considerations discussed, there are essential capabilities to look for when selecting a rack-level electronic lock solution:

Electronic Locks

Electronic locks secure the doors on cabinets, sense access attempts and indicate door latch (lock) opened or closed condition. They are typically a swinghandle with an integrated solenoid that operates the latch to opened or closed condition, a proximity sensor that indicates condition of the latch opened or closed, and an access card reader that senses and reads values from presented keys. The lock also carries a mechanical key override to handle door openings during a power outage.

Access card readers need to be compatible with the card types provided to individuals within an organization. Types of access cards can vary from 125 kHz proximity cards to simple 13.5 MHz smart cards, to next-generation smart cards with one-time passwords. With access card technologies changing very rapidly, it is ideal if the swinghandle and the reader are separate integrated modules. Some models may also include an integrated keypad or biometric reader.

FIGURE 5: Networking the electronic lock through the PDU provides a more cost-effective solution for extending physical security to the rack level, since there is full integration with environmental sensors, power distribution and access control into a single platform.

Single-Factor or Multi-Factor Authentication

Depending on the level of security required, multiple levels of authentication may be preferred. Some electronic locks may include an additional keypad for a unique PIN entry. More advanced solutions may include a biometric reader. If using biometric authentication, privacy laws need to be considered. It is best if it is used alongside an RFID card where the biometric imprint is stored on an individual's badge rather than a centralized database.

Door Sensors

An electronic locking solution for the cabinets needs to monitor not just the cabinet lock status but also status of the door itself. It is critical that an effective locking solution be able to collect input from multiple doors on the cabinet. In the event a door is opened, a warning notification should be provided immediately, followed by additional warnings if the door is left open for an extended duration.

Wiring and Network Connections

There are three types of network connections. The first is through rack intelligent power distribution units (PDUs), the second via a separate networked controller module and the third in which the locks are connected to a building's security access panel. In the first two scenarios, the locks are managed by IT through a data center infrastructure management (DCIM) software solution while the latter is managed through the building security system, which is also used to manage access within the entire campus.

Networking Through PDUs

Advanced rack PDUs can now integrate with environmental monitoring sensors and access control. This means power management, environmental monitoring and access control can be handled at once, via a straightforward, easy-to-use web interface, all networked under one IP address (Figure 5).

With an integrated PDU system, there is no need for a dedicated controller for the electronic locks. The locks also get powered up through auxiliary ports on the PDU. Operators can monitor, manage and authorize each cabinet access attempt wherever the cabinet is situated through remote management to the PDU, which is already part of the data center cabinet ecosystem. This significantly reduces the initial cost of deployment of cabinet-level locks as well as ongoing operating costs. Using this integrated, intuitive interface, data center operators are easily able to provide log reports for critical audit trails for regulatory compliance. It also reduces the need for wiring the electronic access systems to security panels, eliminating another unnecessary expense (Figure 6).

Card IDs can be stored within the PDU web interface. The PDU firmware should support either a standalone list of authorized users or integrate with third-party databases that control user access and rights management. For centralized authentication, either enterprise authentication services (i.e., those supporting networking protocols RADIUS, LDAP, Active Directory) or a DCIM solution can be used.

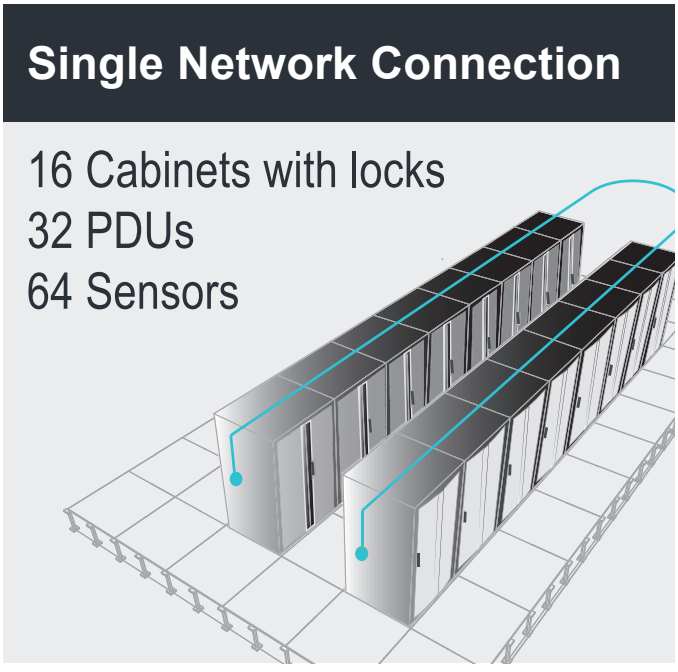

FIGURE 6: Linking all integrated PDUs in a secure array allows up to 32 devices and all attached sensors and locks to share a single network via the IP consolidation connection, potentially saving companies thousands in networking costs.

Networking Through a Separate Controller Module

Electronic locks can also be managed through a dedicated controller module located in every cabinet. While this does increase the initial hardware cost, ongoing operational costs can still be significantly reduced by networking several locks through advanced IP consolidation technology. The PDUs that support IP consolidation allow multiple PDUs to connect through a single physical network connection, IP address and interface, thereby reducing network overhead to monitor at the rack level. For example, some IP consolidation solutions allow up to 32 controllers to be networked under only one IP address

FIGURE 7: In cases where the PDUs are already installed, the best option is to deploy networked locks. In this application, the devices integrate with environmental sensors and can be deployed in a secure array, securing several cabinets under one IP connection.

with an alternate second connection for failover capability. This means MTDCs and colocation providers do not have to pass on unnecessary networking costs to their tenants (Figure 7).

Like the PDU-integrated system, authentication and management could be provided through interfaces that IT organizations already use. For the widest range of compatibility and security for the network, ensure that the PDU or the dedicated controller supports the IPv4 and IPv6 protocols for TCP/IP addressing with static or dynamic address assignments. Simple network management protocol (SNMP) v1, v2c and v3 protocols should be used for third-party DCIM software integration. The web interface should support HTTP or HTTPS sessions with definable ports. Network connections should support encryption and certificates. The email server connection should be outbound only with transport layer security (TLS) and definable ports. For ease of maintenance, the controller module should support bulk configuration and firmware upgrades. The firmware should log every system change.

Networking Through Security Access Panels

With this approach, cabinet-level electronic locks get connected to a Wiegand technology-based security access panel that in turn communicates with a building access control solution (Figure 8). The security panels provide power to the locks. The advantage of this approach is that it leverages the same access control system that is used for campus security. On the flip side, it requires wiring from

FIGURE 8: In cases where communication with the entire building system is preferred or required, there are controller modules that can be installed in the cabinet. These devices connect any cabinet access attempt to the security panels, allowing building security managers to have more control of equipment access.

There are three types of network connections. The first is through rack intelligent power distribution units (PDUs), the second via a separate networked controller module and the third in which the locks are connected to a building's security access panel.

each electronic lock and door sensor to a centralized panel. This typically involves an electrician to wire the handles, including installation of conduit or a pathway structure to secure or isolate the electronic lock wiring from network and power cables. Given the high number of cabinets on a data center floor, this solution requires installation of additional access control panels for connecting the handles on the cabinets. It is powered and controlled from that system and that system's software.

CONCLUSION

To summarize, as higher amounts of confidential data get stored in the cloud, physical access control at the cabinet level needs to become a norm rather than an exception. A myriad of solutions that vary based on the level of security, management modes and budgets are available for organizations to consider.

Technology media company International Data Group (IDG) predicts 50 ZB of data will be created worldwide this year. It is safe to say that enterprise businesses that inspire trust and know how to ethically address risk, security, and compliance will excel in a big way.

AUTHOR BIOGRAPHY: Ashish Moondra is Sr. product manager of Power, Electronics and Software for Chatsworth Products. He has over 20 years of experience developing and managing rack power distribution, uninterruptible power supply (UPS), energy storage and data center infrastructure management (DCIM) solutions. Ashish has previously worked with American Power Conversion, Emerson Network Power and Active Power. He has been an expert speaker at various data center forums. He is currently contributing in the security working subgroup of the Telecommunications Industry Association's (TIA's) Edge Data Center Standard Working Group. He can be reached at amoondra@chatsworth.com

REFERENCES:

1. Ponemon, Larry. "What's New in the 2019 Cost of a Data Breach Report," *Security Intelligence*, 23 July 2019.