WHITE PAPER

Importance of Cabinet-Level Electronic Access Control for Data Security and Regulatory Compliance

By David Knapp
Product Marketing Manager
Chatsworth Products (CPI)

Ashish Moondra
Senior Product Manager, Power, Electronics & Software
Chatsworth Products (CPI)

Raissa Carey
Public Relations Specialist and Technical Writer
Chatsworth Products (CPI)

Published: January 2019

US & Canada
+1-800-834-4969
Toronto, Ontario, Canada
+905-850-7770
chatsworth.com

techsupport@chatsworth.com

Latin America
+52-55-5203-7525
Toll Free within Mexico
01-800-01-7592
chatsworth.com.co

Europe
+44-1628-524-834
chatsworth.com

Middle East & Africa
Dubai, UAE
+971-4-2602125
chatsworth.ae

Asia Pacific
+86 21 6880-0266
chatsworth.com.cn

CHATSWORTH PRODUCTS

Introduction

The importance of physical security for protecting data is generally well understood, but how often does your organization assess the level of physical security for protecting data? And, are you compliant with regulations that address data security?

This white paper, by Chatsworth Products (CPI), presents an overview of data security regulations and compliance requirements, makes an argument for extending physical security to the rack level, recommends the use of electronic locking and access control systems at the rack level, and explains how CPI's cabinet ecosystem (Figure 1) provides a solution that is more cost effective and easier to deploy and operate than others in the market.

Fast Fact

CPI's Electronic Access Control (EAC) solutions have Secure Array® IP Consolidation technology. Secure Array reduces networking costs and requirements by linking up to 32 EACs through one IP address. Try the CPI eConnect® Secure Array Savings Estimator (www.chatsworth.com/eConnect-Secure-Array-Savings-Estimator) to see how much you could save.

Figure 1: CPI's Cabinet Ecosystem provides a more cost-effective solution for extending physical security to the rack level.

The Regulations, Standards and Compliance

What are the data privacy (security) regulations and standards, and what do they require? 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 senstive data privacy concerns, certain segments of our 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.

A few notable regulations and standards include the Health Insurance Portability and Accountability Act (HIPAA)[1], Federal Information Security Management Act (FISMA)[2], General Data Protection Regulation (GDPR)[3], Payment Card Industry Data Security Standard (PCI-DSS)[4] and the AICPA System and Organization Control (SOC-2)[5] framework. The regulations and access-control-related requirements are described below.

HIPPA Health Insurance Portability and Accountability Act

FISMA Federal Information Security Management Act

GDPR General Data Protection Regulation

PCI-DSS Payment Card Industry Data Security Standard

HIPAA - Health Insurance Portability and Accountability Act

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."

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 data base.

HIPAA affects organizations that handle individual health care records including pharmacy, dental, vision and medical service providers, insurance, billing, wellness programs, health tracking apps and even gymnasiums.

HIPAA 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.

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 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.

GDPR - General Data Protection Regulation

GDPR is part of the European Union's (EU) 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."

PCI DSS - Payment Card Industry Data Security Standard

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 provider.

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

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.

Saas SOC 2®– System and Organization Control (SOC-2) Framework

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:

- 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

Looking at the compliance requirements mentioned above, the general requirements related to security are as follows:

- You must have a method to physically secure data processing and storage equipment.
- You must have a method for identifying and managing authorized accessors.
- You must have a method of managing access to the physically secure space.
- You must keep records of access to the physically secure space.

The Role of Physical Security at the Rack Level

Most data centers and computer rooms are physically secure. In a purpose-built facility, there is perimeter security, a robust front door access control, and controlled access to data halls. In enterprise-owned facilities, access to data halls is typically limited above standard building access. So, why extend security to the rack level?

It is important to remember that the intent of data privacy and security regulations is to prevent a data breach. So, preventing a data breach should drive your decisions about physical security. Recognize that the last line of defense in physical security between data processing and storage equipment and access by unauthorized users is a secure server cabinet.

Most data breaches are perpetrated through software or network exploitation by outsiders, right? Most data breaches are but, according to the 2017 IBM X-Force Threat Intelligence Index[6], between 1-percent and 25-percent of attempts to steal data originate from malicious insiders. The 2018 IBM X-Force Threat Intelligence Index[7] further notes that included in the mix of attacks surveyed between 2015 and 2017, most of which originated through software or network exploitations, 19 successful security incidents originated through physical access to data.

For an enterprise-owned, single-tenant site, room-level security is probably sufficient. But for multitenant sites and remote sites, it is best to control access at the rack level—to control access to your assets and the data they store. This is the most granular level of physical security and is best controlled by the IT Systems Administrators and Facility Managers that manage the equipment.

Reasons to use a Rack level Electronic Locking and Access Control System

You probably agree and would argue that you already comply with privacy regulations. After all, most data center cabinets have keyed locks and the keys are carefully controlled. Well, how do you ensure doors are secured? How do you document access to cabinets? How do you recover keys from users? What is your 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. Consider the following:

The Three Levels of Security

Electronic lock and access control systems can use three types of keys: access cards, keypad codes or a biometric. These provide progressive levels of security and recovery over keyed locks with something you have, something you know, and something you are (Figure 2). The access card is something you have. Although it can still be stolen like a physical key, it provides the benefit of assigning and changing credentials quickly without the need to recover the credential or change the lock. A keypad code is something you know. It is more difficult to steal but can be guessed. A biometric is something you are. Other than rare instances of duress or fraud, it uniquely associates access with an individual.

Figure 2: Electronic lock and access control systems introduce three levels of security: something you have, something you know or something you are.

Single-Factor vs. Dual-Factor or Multi-Factor Authentication

Factor refers to the number of unique keys required to access the cabinet (Figure 3). Single-factor authentication systems utilize one key. Keyed locks are strictly a single-factor system. Used individually, access cards, keypad codes or a biometric are also single-factor. However, electronic lock keys are easier to use in dual- and multifactor combinations. Dual- and multifactor keys reduce the probability of access by an unauthorized user. Dual- and multifactor systems may require an upgrade at the electronic lock to include an additional reader, but there are alternatives that encode the second or third key onto an existing credential.

Figure 3: Locks with multifactor capabilities combine multiple key types to enhance security and connect credentials to specific authorized users.

Key Management

If you use keyed locks to secure equipment cabinets, then you 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. Conversely, electronic locking can be reprogrammed quickly with new access codes and you do not need to modify the hardware.

Rights Management

Keyed locks provide limited rights management. Typically, all cabinets are keyed alike. You can 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 or for key management.

In contrast, electronic locking can be reprogrammed quickly with new access codes and you do not need to modify the hardware. You can 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).

Logging Reports and Auditing

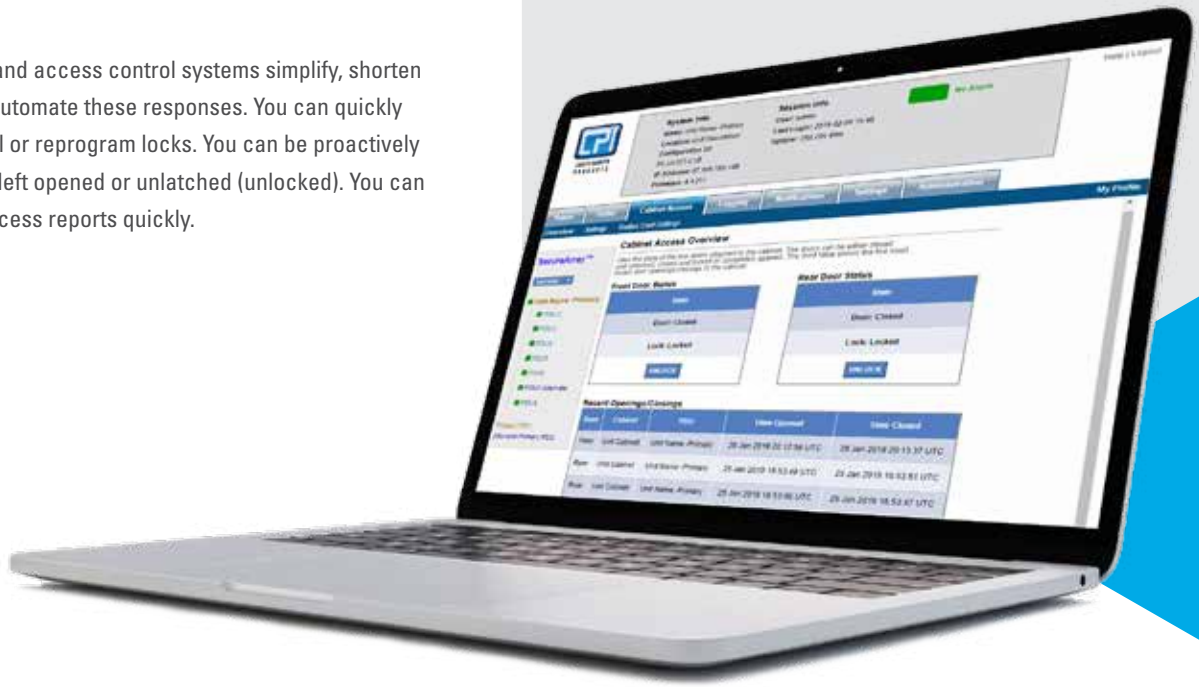
Having users sign in at the controlled front building access documents the person's presence in the building, but not their access to individual cabinets. To create a report of access to individual cabinets, you could review security video footage and annotate dates and times, or you could assign escorts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

However, 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.

Event Response

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

Electronic locking and access control systems simplify, shorten and in some case automate these responses. You can quickly disable a credential or reprogram locks. You can be proactively notified if a door is left opened or unlatched (unlocked). You can filter and create access reports quickly.



The Basics of Rack-Level Electronic Locking and Access Control Systems

At the rack level, electronic locking and access control systems have five basic components:

1. The electronic locks
2. Door sensors
3. Wiring and network connections
4. Monitoring software
5. Keys

The diagram below (Figure 4) shows how these components connect. The following section provides more details on each of these components.

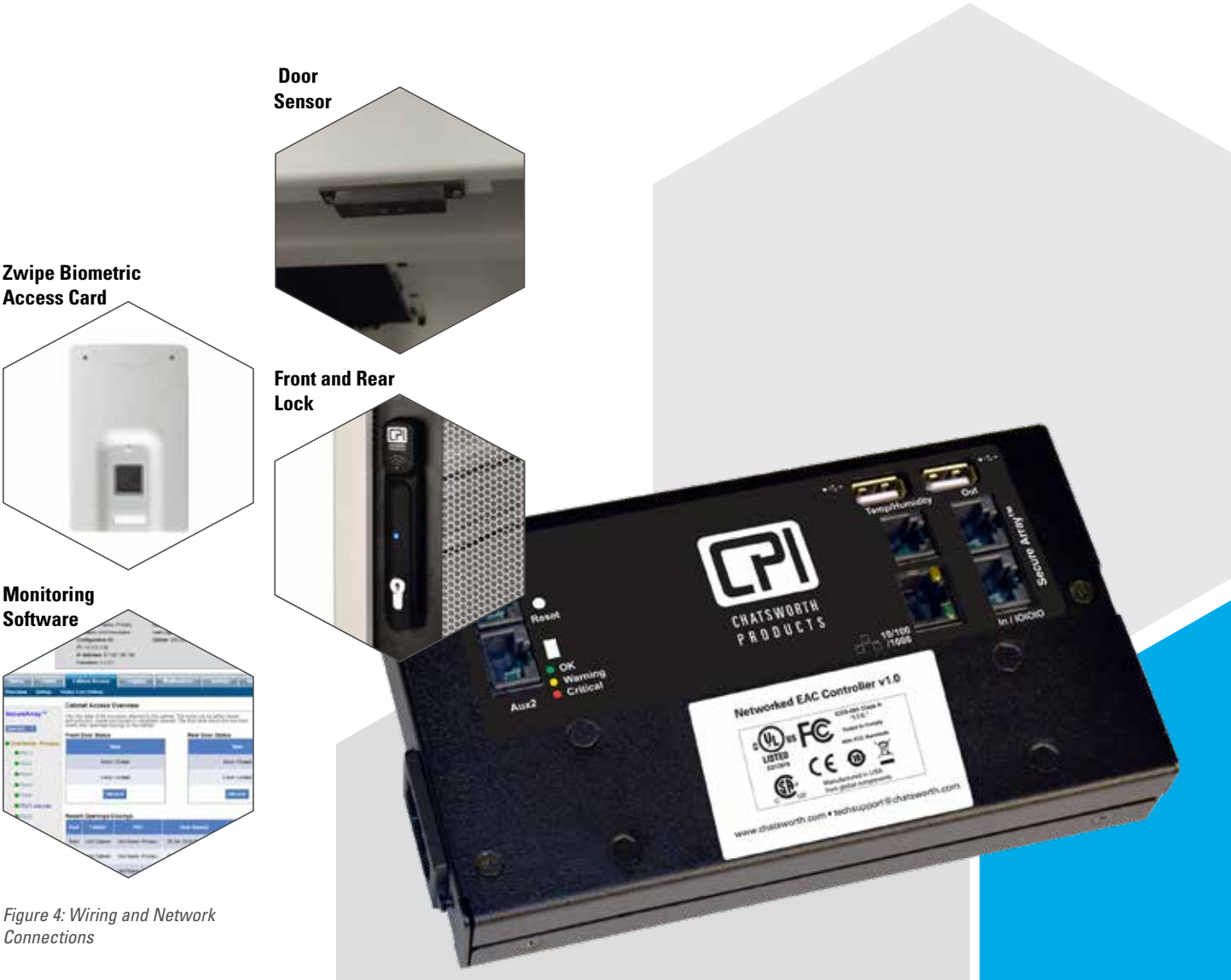


Figure 4: Wiring and Network Connections

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 swing handle 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. Some models may also include an integrated keypad or biometric reader (Figure 5).

Figure 5: Various styles of electronic locks integrated with cabinet swing handles. Photos are Southco® locking solutions: www.southco.com.

Unlike mechanical locks, networked electronic locks can indicate an unlatched (unlocked) condition, will record every access attempt (authorized or unauthorized), can be unlatched (unlocked) remotely by systems administrators, can be latched (locked) automatically after a set period of opened time, can measure the length of time unlatched (unlocked), and will indicate if the latch has been tampered (forced mechanically or opened with a physical key override).

Door Sensors

Door Sensors indicate cabinet door opened or closed condition. They are a separate proximity sensor located on the cabinet door frame and threshold typically on latching side of the door (Figure 6).

Door sensors can be used to prompt a warning notification if the door is opened and to determine the length of time that the door is opened.

Wiring or Network Connection with a Controller Module

There are two options: attach to your existing building access control system (BACS) or wire as a separate networked system. The BACS attachment requires wiring from 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.

Wiring as a separate networked system involves connecting the electronic locks and door sensors to a small, rack-mounted controller module (Figure 7). The controller module has a network connection and power connection. It attaches to a network switch with standard network patch cord. This system can be installed by site staff or preinstalled in the cabinet and requires a network port and IP address for each controller module.

To ensure the controller module has the widest range of compatibility and security for the network, ensure that it supports the IPv4 and IPv6 protocols for TCP/IP addressing with static or dynamic address assignments, and SNMP v1, v2c and v3 protocols for third-party Data Center Infrastructure Management (DCIM) software integration. The web interface should support HTTP or HTTPs sessions with definable ports. Network connections should support encryption and certificates. Email server connection should be outbound only with 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.

Figure 6: Door sensor installed on a cabinet door.

Figure 7: Controller module and wiring harness.

Monitoring Software

Monitoring software will be specific to the locking system selected, and in separate networked systems, it may be integrated into the controller module firmware. It should provide strong login security, separate administrator and user roles, individual user accounts, easy administration of user access rights to allow quick assignment and removal of user rights, event logging, notifications for events, and log export or access reports.

Access should be password-protected with separate user rights levels for administrators and users. It should support user authentication from an internal database, LDAP database or RADIUS database. Administrators should be able to assign individual user-specific electronic lock (cabinet door) access rights; should be able to unlatch (unlock) electronic locks (cabinet doors) remotely and set a specific time for the locks (doors) to remain unlatched (unlocked).

The software interface should clearly indicate opened and closed conditions; log each access attempt and associate the attempt to a specific key and user; and alarm opened, unlocked and tampered conditions (Figure 8). Ideally, reporting should provide a per-user or per-cabinet access report for any defined event log period.

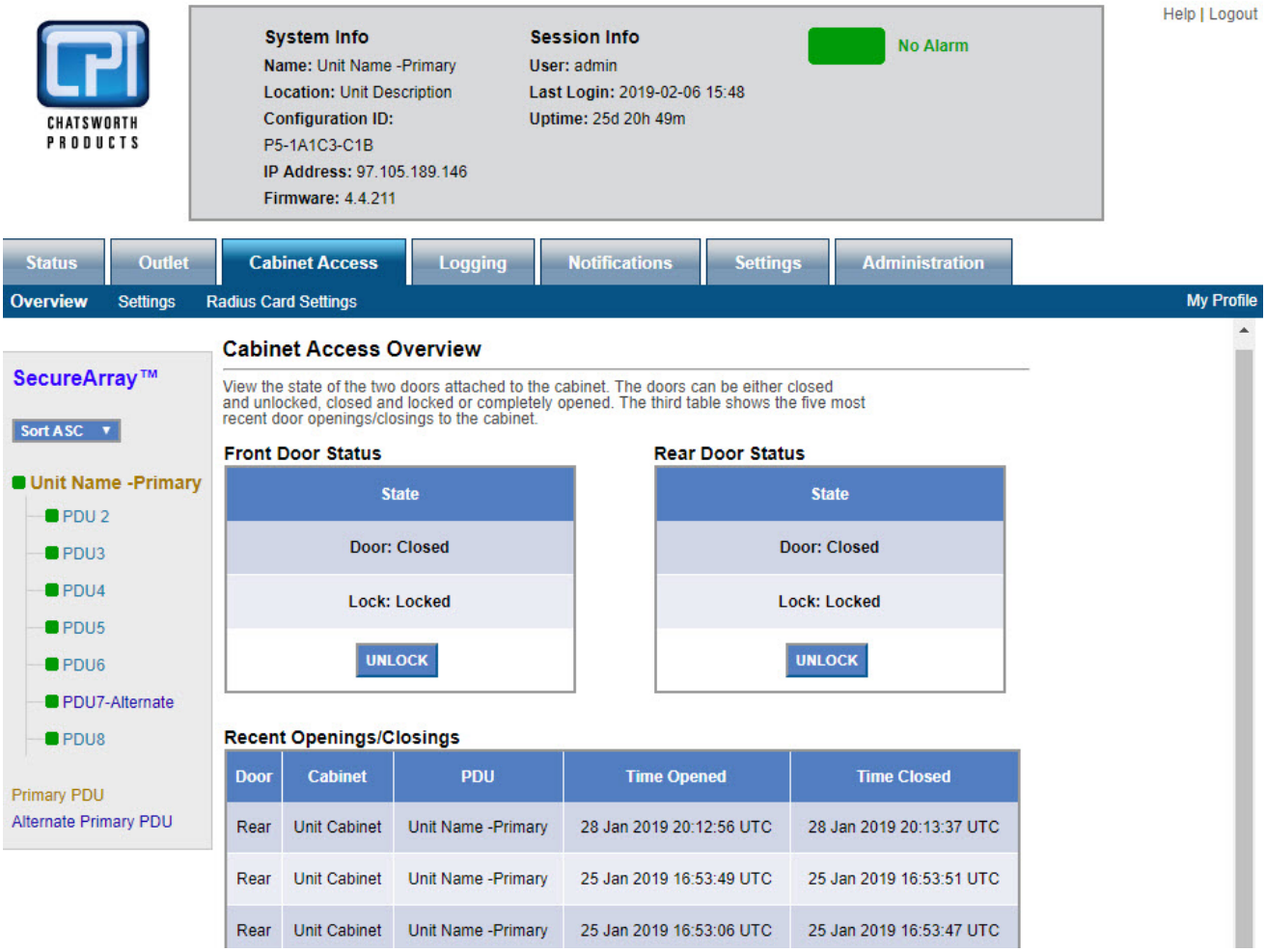


Figure 8: Screenshot from CPI Networked EAC showing latch and door conditions.

Keys

There are three types of keys for electronic locking and access control systems: access cards, keypad and code, and a biometric. There is no mechanical interface between the key and the lock. All rights are assigned in the software. Some systems use multiple keys to provide enhanced security.

For access card and biometric systems, the electronic lock must have a compatible reader (Figure 9). The software must support assignment of the key codes. If you wish to use an existing access card, like a company-issued employee badge, you will need to confirm these compatibilities. Otherwise, you may need to assign a second credential to those employees who should have access to ICT cabinets.

Figure 9: Access card used with electronic lock with integrated proximity card reader.

The Main Challenges of Deploying Electronic Locking at the Rack Level

Organizations that have studied the deployment of electronic locking at the rack level often encounter two main challenges: hardware and implementation cost. Additionally, there may be some organizational concerns if IT elects a separate system outside of direct control to the security department. Finally, retrofitting the system may be difficult.

The Challenge of Hardware Cost

There can be a significant initial hardware cost to deploy racks with electronic locking. First, each door handle (latch) needs to be upgraded with an electronic lock. Second, the locks need to be wired to a central panel or to controller modules in each rack. If using controller modules, the modules would need to be connected to the IT network, which may require additional network switches. Controller modules will also need to be powered in each rack. There may also be a separate software, license and maintenance contract.

The Challenge of Implementation Cost

The system will need to be configured and then managed. If connected to the IT network, then each controller module will use a network port and IP address. These ports are in addition to other ports and addresses used to monitor an intelligent power distribution unit (PDU) and environmental monitoring system at the rack level. A server(s) may be required to run the software and to store logged data. These represent ongoing costs for power, networking and system administration.

The Challenge of Organizational Ownership

The system may be a separate system from the main building security system. Will the security department or IT own the system and manage authorizing access to users? It makes more sense for IT to own rack-level access control, even if it needs to be a separate system. IT is responsible for the equipment and data protected by the cabinets and maintenance to those systems. Additionally, cabinet access should be tightly integrated with enterprise systems such as RADIUS and LDAP for user authentication.

The Challenge of Retrofitting Hardware

The system hardware and wiring harnesses may not fit well in existing cabinets. Electronic locks typically come in a swinghandle handle design and the cutout in the cabinet door may or may not match the retrofit electronic lock. Additionally, the handles will need to wire to a controller module or to a BACS panel. It may be difficult to route wires through a populated cabinet.

The CPI Solution

The CPI solution addresses both challenges reducing both hardware and implementation costs, and delivering an easy to configure, use and maintain system. The CPI Solution has three components: eConnect® PDUs with eConnect Electronic Access Control (EAC) and Environmental Probes; Power IQ® for eConnect DCIM software, and Zwipe® Biometric Access Cards.

eConnect PDU with EAC and Environmental Probes

The eConnect PDU with EAC and Environmental Probes address hardware cost by consolidating the power monitoring and control system from a PDU with an environmental monitoring system and an electronic locking and access control system into a single hardware solution. This solution uses a single firmware, web interface and network connection. The CPI eConnect solution reduces the number of network ports required to monitor power, environmental and access control in a single rack from three to one. The electronic locking and environmental sensors connect to and are powered by the PDU. There is one web interface to access, configure, monitor and report all rack level conditions.

eConnect PDU with EAC addresses implementation cost with the integrated Secure Array IP Consolidation technology. This allows up to 32 PDUs with all attached locks and environmental sensors to share a single network connection or two network connections for redundancy (Figure 10). This greatly reduces the number of network ports, IP addresses and associated network switches required to support the system. Like the individual eConnect PDU, each Secure Array can be viewed from a single web interface.

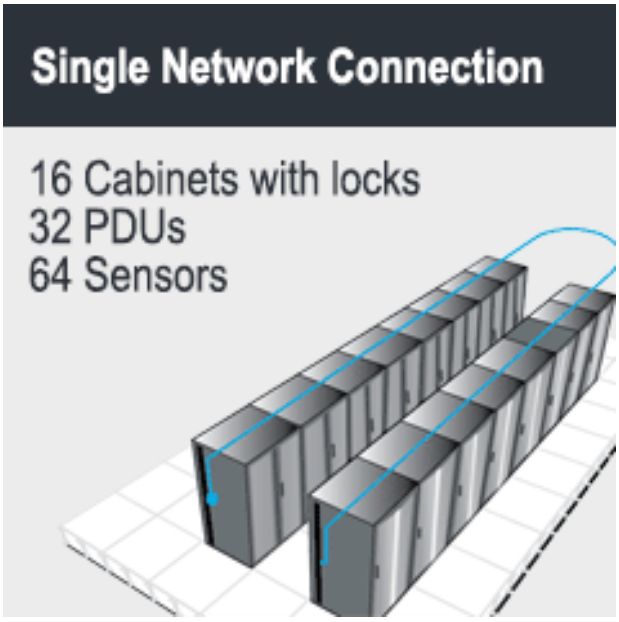


Figure 10: CPI eConnect PDU integrates power monitoring, environmental monitoring and access control into a single system. Integrated Secure Array IP Consolidation technology allows up to 32 PDUs and all attached sensors and locks to share a single network connection.

Fast Fact

If you are retrofitting an existing solution and do not need to upgrade your PDUs, you can still reduce hardware and implementation costs with CPI Networked Electronic Access Control (EAC) (www.chatsworth.com/econnect-electronic-access-control/), which combines electronic locking and environmental monitoring into a single solution and supports CPI Secure Array IP Consolidation technology.

Power IQ for eConnect PDU DCIM software

Power IQ for eConnect PDU is a DCIM software that allows you to monitor all eConnect PDUs with EAC in your room, site or multiple sites from a single screen. Power IQ recognizes the Secure Array IP Consolidation technology and identifies all devices on the network, so you gain the benefit of fewer network connections, but still see each individual device in the software interface.

Power IQ uses graphic dashboards to show immediate conditions in the racks, helping you quickly identify issues that need to be addressed (Figure 11). It trends power and environmental data to help you monitor and optimize capacity. It provides one place to assign access rights across all cabinets in your network, and it also produces reports for access attempts by cabinet and user.

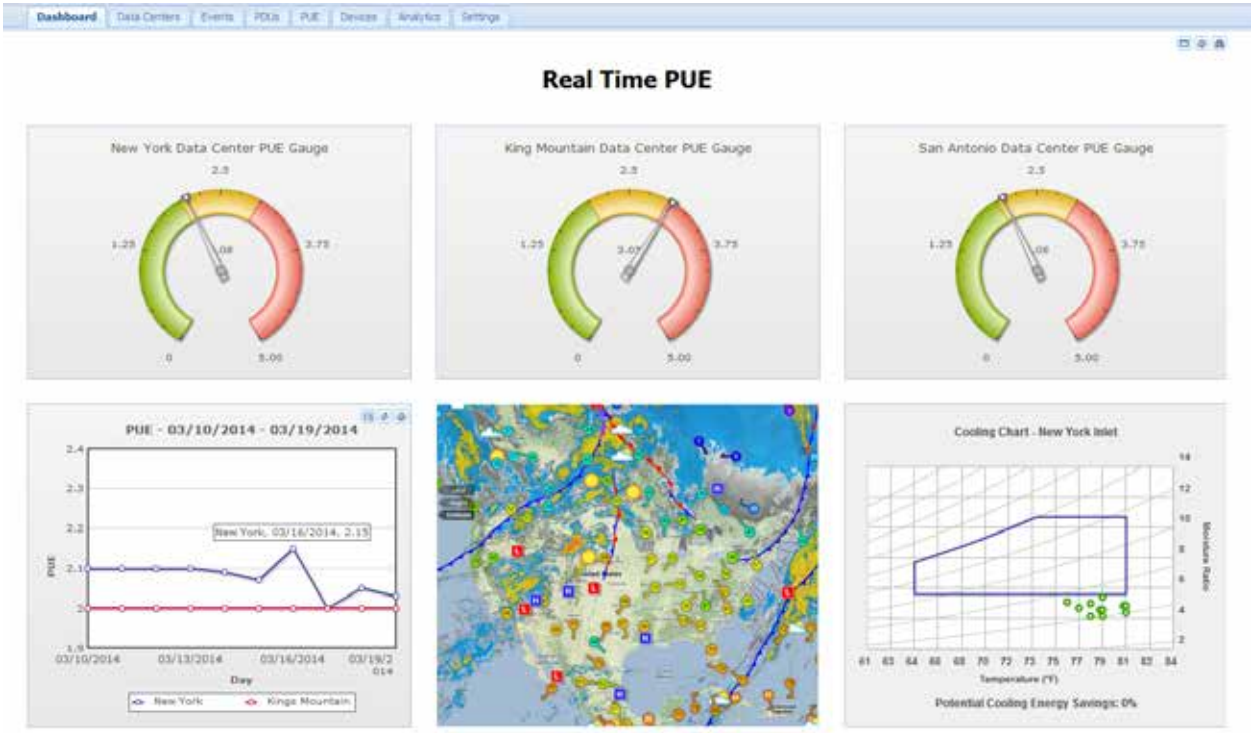


Figure 11: Power IQ for eConnect PDU provides a single screen to monitor site conditions. Easy-to-read dials and charts help you identify issues and trends quickly.

Zwipe® Biometric Access Cards

Zwipe® Biometric Access Cards provide a simple way to upgrade your access control system to include a dual-factor, biometric authentication. The Zwipe Biometric Access Card is an access card with an integrated fingerprint reader that encodes the user's fingerprint when issued, and will only function when the user's fingerprint is used to activate the card (Figure 12). No changes to electronic locking or access control software are required. Zwipe absolutely associates an access card with an individual user.

Figure 12: Zwipe Biometric Access Card has an integrated fingerprint reader allowing you to add dual-factor biometrics to an existing access card system at minimal cost.

Comparison of CPI Solution to the Traditional Solution

The (Table 1) below compares estimated costs of a traditional solution and the CPI ecosystem solution for a complete rack-level monitoring solution. The traditional solution has two intelligent PDUs for power monitoring, a separate environmental monitoring system, and a separate electronic access control system. Each has a separate network connection and monitoring software. The CPI ecosystem solution is the eConnect PDU with EAC and environmental probes.

Estimated Cost Comparison of a NEW Monitoring System for 16 Cabinets							
	Traditional System Separate PDU, Environmental, and Electronic Access Control (EAC)			CPI Ecosystem Integrated PDU, Environmental, and Electronic Access Control (EAC)			Savings with CPI
Component (estimates)	**QTY**	**Each**	**Total**	**QTY**	**Each**	**Total**	
Cabinet Handle Kit	16	$1,000.00	$16,000.00	16	$300.00	$4,800.00	$11,200.00
Power Supply for Handle Kit	16	$25.00	$400.00	0	$-	$-	$400.00
Access Card	5	$5.00	$25.00	5	$5.00	$25.00	$-
Access Control Software	1	$1,000.00	$1,000.00	0	$-	$-	$1,000.00
Environmental Monitoring Appliance	16	$750.00	$12,000.00	0	$-	$-	$12,000.00
Power Supply for Appliance	16	$25.00	$400.00	0	$-	$-	$400.00
Environmental Sensors	32	$5.00	$160.00	32	$5.00	$160.00	$-
Environmental Monitoring Software	1	$1,000.00	$1,000.00	0	$-	$-	$1,000.00
Intelligent PDU	32	$1,000.00	$32,000.00	32	$1,000.00	$32,000.00	$-
PDU Monitoring Software	1	$1,000.00	$1,000.00	0	$-	$-	$1,000.00
DCIM Software	1	$5,000.00	$5,000.00	1	$5,000.00	$5,000.00	$-
Subtotals			**$68,985.00**			**$41,985.00**	**$27,000.00**
Service (estimates)	**QTY**	**Each**	**Total**	**QTY**	**Each**	**Total**	
Handle Installation	16	$25.00	$400.00	16	$25.00	$400.00	$-
Environmental Installation	16	$25.00	$400.00	16	$25.00	$400.00	$-
Intelligent PDU Installation	32	$25.00	$800.00	32	$25.00	$800.00	$-
New Network Connection	64	$250.00	$16,000.00	1	$250.00	$250.00	$15,750.00
New Power Connection	64	$250.00	$16,000.00	32	$250.00	$8,000.00	$8,000.00
IT Administration, System Setup	4	$500.00	$2,000.00	1	$500.00	$500.00	$1,500.00
Software Maintenance Contract	4	$100.00	$400.00	1	$100.00	$100.00	$300.00
Subtotals			**$36,000.00**			**$10,450.00**	**$25,550.00**
Total			**$104,985.00**			**$52,435.00**	**$52,550.00**
Estimated Savings with CPI EAC*					**50%**	**$(52,550.00)**	

Table 1: Comparison of estimated costs for components and installation a complete cabinet-level monitoring solution including intelligent PDUs, environmental monitoring and Cabinet Ecosystem. The traditional system uses separate hardware systems, network connections and monitoring software. The CPI ecosystem uses integrated hardware and firmware and Secure Array IP Consolidation technology.

Note: Pricing is strictly an estimate. Comparison shows the relative differences in component and service quantities for the given systems, but actual unit prices will vary depending on systems selected.

The CPI Cabinet Ecosystem solution consolidates the power monitoring and control system (PDU), environmental monitoring system and electronic locking and access control system into a single hardware platform with a single network connection. So, you only need one network connection per rack versus four with a standard solution. Additionally, CPI's Secure Array IP Consolidation technology allows 32 PDUs and all associated electronic locks and environmental probes to be connected through a single network connection. The result is significant reduction of network ports required to deploy rack level monitoring and access control, and corresponding reduced networking cost (Figure 13).

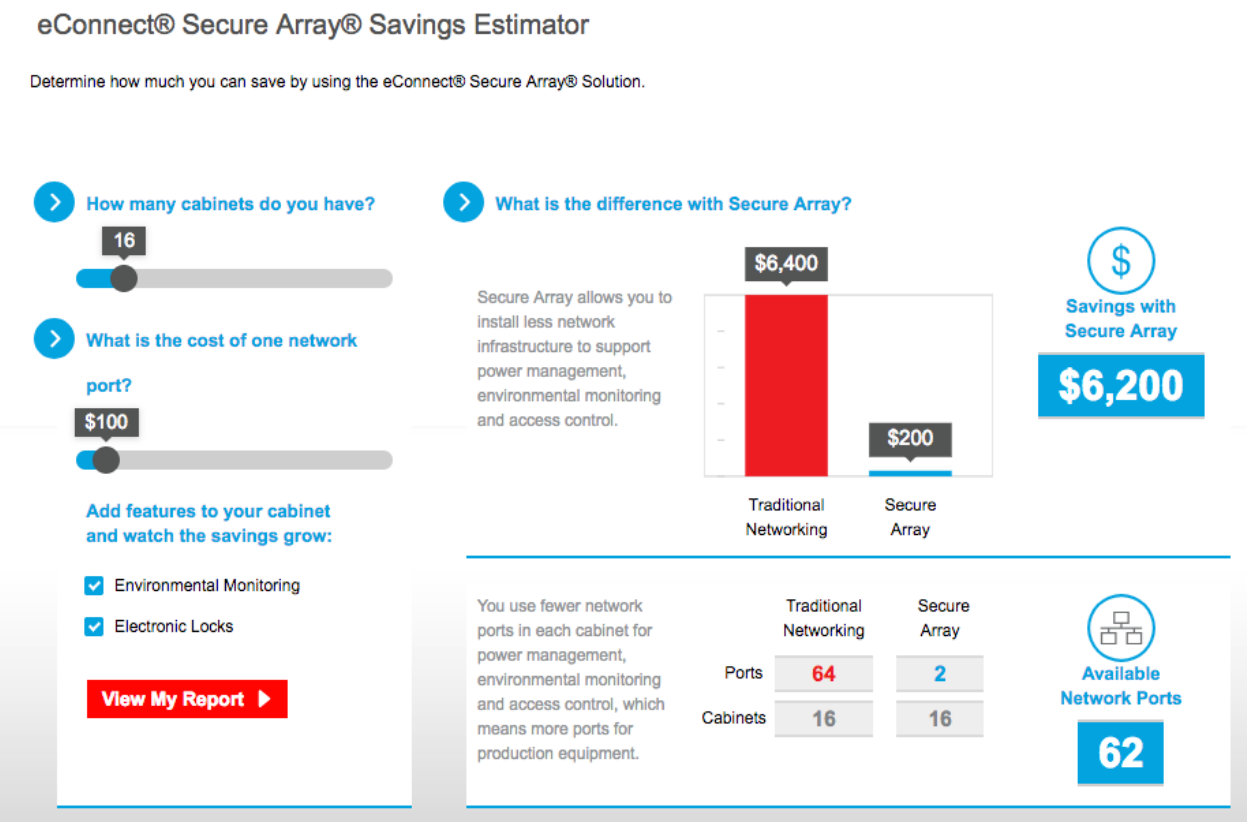


Figure 13: Screenshot from CPI's online eConnect Secure Array Savings Estimator tool, which allows you to compare the relative networking cost of a traditional system versus a CPI system with Secure Array.

Fast Fact

Try the CPI eConnect Secure Array Savings Estimator (www.chatsworth.com/eConnect-Secure-Array-Savings-Estimator) to see how much the CPI eConnect PDU with EAC and Secure Array can save you.

What about retrofitting?

If you are upgrading an existing site and already have intelligent PDUs deployed, eConnect Secure Array IP Consolidation will still reduce the cost versus a traditional system, but there is less benefit from consolidated hardware because you are deploying separate hardware. The (Table 2) below compares estimated costs of a traditional solution and the CPI Cabinet Ecosystem solution for an electronic locking and access control system retrofit solution.

Estimated Cost Comparison of a NEW Access Control System for 16 Cabinets							
	Traditional System Electronic Access Control (EAC)			CPI Networked Electronic Access Control (EAC)			Savings with CPI
Component (estimates)	**QTY**	**Each**	**Total**	**QTY**	**Each**	**Total**	
Cabinet Handle Kit	16	$1,000.00	$16,000.00	16	$1,000.00	$16,000.00	$-
Power Supply for Handle Kit	16	$25.00	$400.00	16	$25.00	$400.00	$-
Access Card	5	$5.00	$25.00	5	$5.00	$25.00	$-
Access Control Software	1	$1,000.00	$1,000.00	0	$-	$-	$1,000.00
Subtotals			**$17,425.00**			**$16,425.00**	**$1,000.00**
Service (estimates)	**QTY**	**Each**	**Total**	**QTY**	**Each**	**Total**	
Handle Installation	16	$25.00	$400.00	16	$25.00	$400.00	$-
New Network Connection	16	$250.00	$4,000.00	2	$250.00	$500.00	$3,500.00
New Power Connection	16	$250.00	$4,000.00	16	$250.00	$4,000.00	$-
IT Administration, System Setup	1	$500.00	$500.00	1	$500.00	$500.00	$-
Software Maintenance Contract	1	$100.00	$100.00	0	$-	$-	$100.00
Subtotals			**$9,000.00**			**$5,400.00**	**$3,600.00**
Total			**$26,425.00**			**$21,825.00**	**$4,600.00**
Estimated Savings with CPI Networked EAC					**17%**	**$(4,600.00)**	

Table 2: Comparison of estimated costs for components and installation a retrofit rack-level electronic locking and access control system. Both systems require a controller module in each cabinet and power supply for the module (handle kit), but the CPI Cabinet Ecosystem has integrated firmware (software) and Secure Array IP Consolidation technology, which reduces the networking costs.

Note: Pricing is strictly an estimate. Comparison shows the relative differences in component and service quantities for the given systems, but actual unit prices will vary depending on systems selected.

Conclusion

Extending physical security to the rack level with an electronic locking and access control system provides the most physically secure solution for data protection. This approach places monitoring and recording of each access attempt at the point closest to equipment. It simplifies key and credential management, automatically documents each access attempt, provides IT with immediate notification of door opened conditions and allows much quicker event response.

However, organizations considering adoption of these systems have often found them to have high hardware and implementation costs. CPI addresses both concerns with the eConnect PDU with Electronic Access Control system. CPI eConnect PDU with EAC combines the rack level power monitoring and control system, environmental monitoring system and electronic lock and access control system into a single solution, reducing hardware costs and networking requirements.

Additionally, CPI can be your single source for your cabinet, electronic locking, intelligent PDUs, environmental monitoring and DCIM software, and will preinstall the locks and PDUs into your cabinets, speeding your deployment. We call it the CPI cabinet ecosystem. Please contact a CPI Technical Support (techsupport@chatsworth.com) for more details.

References

[1]1104th United States Congress. Public Law 104-191. 110 Statute 1936. Health Insurance Portability and Accountability Act (HIPAA). Enacted August 21, 1996. www.congress.gov/bill/104th-congress/house-bill/3103?s=10&r=68
[1]Related legislation. United States Department of Health and Human Services (HHS). Health Information Technology for Economic and Clinical Health Act (HITECH act) of 2009. www.healthit.gov/topic/laws-regulation-and-policy/health-it-legislation.

[2]113th United States Congress. Public Law 113-283. 113 Statute 2521. Federal Information Security Modernization Act (FISMA) of 2014. Enacted December 14, 2014. www.congress.gov/bill/113th-congress/senate-bill/2521?q=%7B%22search%22%3A%5B%22FISMA%22%5D%7D&s=7&r=2.
www.dhs.gov/fisma.

[3]European Union. European Parliament. Regulation (EU) 2016/679. General Data Protection Regulation (GDPR). Enacted April 27, 2016. eur-lex.europa.eu/eli/reg/2016/679/oj.

[4]Payment Card Industry Security Standards Council. Payment Card Industry Data Security Standard (PCI-DSS v3.2.1). Published May 2018. www.pcisecuritystandards.org/document_library.

[5]American Institute of Certified Public Accountants (AICPA). System and Organization Controls (SOC-2), Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy Guide. Published 2011.
www.aicpa.org/interestareas/frc/assuranceadvisoryservices/sorhome.html
www.aicpa.org/interestareas/frc/assuranceadvisoryservices/cybersecurityforcpas.html.

[5]American Institute of Certified Public Accountants (AICPA). Assurance Services Executive Committee (ASEC). Trust Services Criteria. Published 2017. www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/trust-services-criteria.pdf.

[6]IBM. IBM Security. 2017 IBM X-Force Threat Intelligence Index. Published March 2017. www.ibm.com/security/data-breach/threat-intelligence.

[7]IBM. IBM Security. 2018 IBM X-Force Threat Intelligence Index. Published March 2018. www.ibm.com/security/data-breach/threat-intelligence.

Contributors

David Knapp | Product Marketing Manager

David Knapp is a Product Marketing Manager at Chatsworth Products (CPI), a global manufacturer of products and service solutions that optimize, store and secure technology equipment. David has 18 years of experience in the telecommunications industry as a product-application expert and technical communicator. He is currently focusing on data center, enterprise networking and power management solutions.

Ashish Moondra | Senior Product Manager, Power, Electronics & Software

Ashish Moondra is the Senior Product Manager for Power, Electronics and Software at Chatsworth Products (CPI). He has 20 years of experience developing, selling and managing rack power distribution, uninterruptible power supplies, energy storage and DCIM solutions. Ashish has previously worked with American Power Conversion, Emerson Network Power and Active Power.

Raissa Carey | Public Relations Specialist and Technical Writer

Raissa Carey is a journalist with more than 20 years of experience producing, developing and managing a variety of content marketing and news articles within several industries in the United States and internationally. Since 2013, Carey has been both creative and technical writer at Chatsworth Products, contributing to the majority of thought leadership and solution-based content globally.

CHATSWORTH PRODUCTS

While every effort has been made to ensure the accuracy of all information, CPI does not accept liability for any errors or omissions and reserves the right to change information and descriptions of listed services and products.

©2019 Chatsworth Products, Inc. All rights reserved. Chatsworth Products, Clik-Nut, CPI, CPI Passive Cooling, eConnect, Evolution, GlobalFrame, MegaFrame, Motive, OnTrac, QuadraRack, RMR, Saf-T-Grip, Secure Array, SeismicFrame, SlimFrame, TeraFrame and Velocity are federally registered trademarks of Chatsworth Products. CUBE-iT, EuroFrame and Simply Efficient are trademarks of Chatsworth Products. All other trademarks belong to their respective companies. 03/19 MKT-60020-709