SECURITY FOR POWER AND COOLING SYSTEMS

Jeffrey Osowski

Davenport University

Advisor: Dr. Lonnie Decker, PhD

Thursday, July 26, 2012
Contents

Abstract .................................................................................................................................................... 4

Introduction ............................................................................................................................................ 5
  Data Center Design ................................................................................................................................. 6
  Security Defined ....................................................................................................................................... 7
  Potential Threats ...................................................................................................................................... 8
  Potential Benefits ..................................................................................................................................... 10

Literature Review ................................................................................................................................. 11
  Sources for Standards and White Papers ............................................................................................ 12
    National Fire Protection Association (NFPA) ..................................................................................... 12
    Telecommunications Industry Association ....................................................................................... 13
    The Uptime Institute ............................................................................................................................ 14
    Green Grid ......................................................................................................................................... 15
    National Institute of Standards and Technology (NIST) ................................................................. 15
    Bicsi (Building Industry Consulting Services, International) ......................................................... 15
    Manufacturers .................................................................................................................................... 17
    APC .................................................................................................................................................... 17
    Raritan ................................................................................................................................................. 18
  Textbooks, Manuals, Other Sources .................................................................................................... 18
    Network Security .............................................................................................................................. 18
    Social Engineering ............................................................................................................................. 20

Research Methods ............................................................................................................................... 22
  Secondary Research ............................................................................................................................. 22
  Primary Research .................................................................................................................................. 22
  Industrial Facility .................................................................................................................................. 23
  New Data Center Construction ........................................................................................................... 24
  Major Retailer Data Center .................................................................................................................. 25
  Industry Consultant .............................................................................................................................. 27

Analysis ................................................................................................................................................... 28
  Critical Components of Data Center Design ..................................................................................... 29
  Security Design for Critical Power and Cooling Delivery Systems .................................................. 30

Conclusion and Suggestions .................................................................................................................. 31
  Support Standards Efforts .................................................................................................................... 31
  Include Security in Data Center Designs ............................................................................................... 32
  Track and Document all Breaches ......................................................................................................... 32
  Conduct Additional Research ............................................................................................................... 33
  Create a Comprehensive Security Plan ................................................................................................. 33

References ................................................................................................................................................ 34

Appendix 1: Explanation of Terms .......................................................................................................... 36
Appendix 2: TIA 942 Section F.6 ............................................................................................................. 38
Figure 1 - NEC Adoption by State (NEMA.org, Standards subheading technical) ..................... 13
Figure 2 - Data Center Layered Security Design (From ANSI/TIA 942) .................................... 26
Figure 3 - Bicsi Layered Security Diagram (Bicsi 002 Data Center Design) ......................... 29
Abstract
It is necessary to include a security component for critical power and cooling delivery systems in thorough Data Center designs. My thesis statement, Security for Critical Power and Cooling Delivery Systems is a Necessary Component of a Comprehensive Data Center Design, details a position I’ve taken on IT Infrastructure security, both through personal experience (through my position as a Systems Engineer specializing in Data Center Design for large corporations), as well as through research and communications with industry professionals. Currently the industry standards and best practices often do not fully address security for critical power and cooling systems. This thesis will illustrate the need for and best applications of security for Critical Power and Cooling Delivery Systems.
Security for Critical Power and Cooling Delivery Systems is a Necessary Component of a Comprehensive Data Center Design

Introduction

When referring to Information Technology security, the major focus has traditionally been software security – protection against hackers/crackers that breach the network to gain access to sensitive data. There is an equally important, yet often overlooked, aspect of IT security, that of the infrastructure supporting the servers, storage, and network switches that house and disseminate the applications and sensitive data. This infrastructure delivers the critical power and cooling that is vital to operations. Any interruption in power or cooling delivery may result in a complete or partial shutdown of data center operations.

Once the IT infrastructure is compromised, major damage may be inflicted on the hardware, applications, and data that compromise an organization’s information and intelligence. Yet many companies do not pay proper attention to this aspect of security, either for lack of knowledge or lack of experience. In some vast organizations, the responsibility is spread over two (2) or more departments, typically IT and Facilities, and neither fully understand the requirements or functions of the other. This creates a hole in the security of the organization, one that can be exploited to delay or halt operations in the event of a breach.

My thesis is as follows:

Security for critical power and cooling delivery systems is a necessary component of a comprehensive data center design.
The subject of security within IT operations is vast; this research paper will focus specifically on the hardware used to deliver power and cooling to data centers. The security domain (Schou and Shoemaker, 2007) will be the critical power and cooling delivery systems. This will include the electrical supply from the utility substation, which is generally the demarcation point (where the utility relinquishes responsibility for equipment and security), as well as internal cooling systems. Not included will be all gear outside of the jurisdiction of the organization, meaning demarcation point (substation) out to the utility, and any municipality provided chilled water systems (heavily populated urban/downtown areas that have chilled water loops available as a utility service). It will be noted that interruption to these services can greatly impact the operations of an organization’s IT processes; a well-designed Data Center Infrastructure system will incorporate self-sufficiency, redundancy, and security in the design.

**Data Center Design**

Exactly what is involved in designing a data center? It is a complex mix of construction, facilities (including critical power and cooling), layout, and contingencies for future growth. All of these are vital, but on top of that you must add security – security specific to the Data Center Design in question. A Data Center is like a delicate ecosystem. If one item is compromised, it can have a drastic effect on the other components.

The first item in design is a secure space of sufficient size. This would preferably be on the ground floor in the center of the building, or minimally a nominal distance with separation from an outer wall. There should not be any windows to the external environment, and all entrance/egress points require a monitored and tracked security entrance (e.g. proximity readers that gather and store historical data).
Utility delivery would be dependent upon the geographic location and building physical infrastructure. For a top tier in accordance with the Uptime Institute’s Tier Levels (Uptime Institute Tier Standard), the most safe and redundant design incorporates dual feeds from dual power grids - something that is hard to attain unless you live where grid systems overlap. Some municipalities offer chilled water delivery as a utility, which can offer efficiency as well as redundancy. In most situations, the organization must provide their own cooling, albeit with municipal water systems when water is required (BICSI 002-2010 Data Center Design).

While these items constitute the finite list of requirements for data center infrastructure, most documentation details their design and implementation but never discusses security or the implications of a security lapse. Documents such as application notes, white papers, and standards guides (as published by Green Grid, Bicsi, and Uptime Institute) are remiss in their requirements for security for the critical power and cooling delivery systems (sometimes referred to as the infrastructure or critical infrastructure).

**Security Defined**

The existing data center design guides revolve around geography, layout, structure, delivery, availability, and redundancy, but all seem to leave the security portion to the security planners. One particular manufacturer, APC by Schneider Electric, promotes their Netbotz line which is IT and Data Center Physical Threat Monitoring. They define physical threat as intrusion, unauthorized access, or environmental breach (flooding, heat, fire), but only provide monitoring. Monitoring, in this sense, can be described as gathering and tracking data in real time, but monitoring without full time human review is insufficient.
Security incorporates real time, full time analysis of all data points vital to continuous operation. For example, a security camera can monitor a Data Center, recording and storing video images. However, unless the data points are analyzed immediately, the breach is not prevented from occurring, and may not be discovered or reported until additional damages are incurred. Monitoring can point out that someone gained unauthorized access to sensitive equipment, with a time stamp and other details including the identity of the intruder. Security is real time, full time analysis that can halt and even prevent the breach from occurring.

This lack of attention to security for critical power and cooling systems is a highly likely target for future breaches and attacks.

**Potential Threats**

Much is known and documented about breaches involving the loss of organizational data (including proprietary documentation, financial data, and customer records) to hackers and internal improprieties. Breaches and attacks on the physical infrastructure are less publicized, most likely due to the lack of regulation requiring public disclosure, or the tendency to cover up shortcomings that would tarnish an organization’s reputation. Some organizations even refrain from using local law enforcement resources. There is an acceptance on defining risk management: identify a vulnerability, identify the threats that can exploit it, design and implement a countermeasure (Tipton and Krause, 2007).

Critical power and cooling delivery equipment that supports Data Center operations, including chillers, condensers, generators, substations, and in some cases UPS, are often deployed outside of their respective buildings. Due to the recent down turn in the economy and subsequent rise in value for scrap metal and copper, many of these components have
become targets for damage and loss due to theft. In major urban areas, anything outside and unsecured is subject to theft, being damaged, or both. Security is absolutely a necessity for continued operations. This type of breach will cause loss of availability along with loss of revenue and capital. Additionally, the company may be susceptible to lawsuits from overzealous family members if a vandal is hurt or killed while attempting to steal copper from high voltage power lines.

For their part, the electrical utility generally will provide a locked and secured area for their substation gear. While this level of security is not impenetrable, it does provide some level of deterrence. And while the energy delivery is important for the utility, especially in terms of meeting Service Level Agreement contract terms, it is not vital to have continuous power (as it is for the IT operations). So it is beneficial for the organization to monitor and secure the utility substation when applicable, to insure their continued operations.

Security for cooling systems is equally vital, and while less a target for theft (it generally requires a crane to move even the smallest pieces of a chiller or condenser system), vandalism to cooling systems can halt operations immediately. Cooling systems rely on a heat removal medium – refrigerant, water, or glycol solutions. If the medium is compromised, either by damage to the pipes that transport them or by contamination of the medium itself, the ability for the cooling equipment to perform can be reduced or halted.

The examples given were to illustrate breaches outside of an organization’s business model. However, breaches can be perpetrated by competitors or internal staff. If a disgruntled employee wants to interrupt service on payroll day for revenge, he might contaminate the water of an open loop chilled water system. A bucket of paint or other damaging chemical composition might turn the Data Center air conditioning system off, and
on a hot summer day in a warm climate, cause the Data Center temperature to rise uncontrollably, requiring a system shut down. If the organization does not have sufficient redundancy for cooling, this might cause temporary or permanent damage to the critical cooling delivery system. A manufacturing competitor might also conduct a similar act, albeit for a different purpose – possibly to disrupt operations during a period where competing manufacturers are pursuing the same business opportunity.

Whenever sensitive equipment is placed in the outdoor environment, it is open to breaches by any number of perpetrators. Security systems must be deployed utilizing real time full motion camera monitoring, intrusion detection for secured equipment deployment areas, monitoring of utility services provided, and fuel delivery components (i.e. natural gas or diesel fuel in storage tanks for generators).

**Potential Benefits**

The most prevalent benefit of insuring a secure and monitored data center is an increase in the factors most important to data – Accountability, Accessibility, and Availability. If there is a break in the delivery of power or cooling (in most cases chilled water as a heat removal medium) to a data center, operations will be interrupted or halted. This may be a minor inconvenience, such as in the case of research where testing might simply need to be restarted when the power and cooling are restored.

However, in some cases any loss of time could result in litigation, government sanctions, or possibly death (as in the case of a hospital). The National Fire and Protection Association, which publishes the National Electric Code (NFPA 70) allows that full power must be restored to a hospital facility within 10 seconds (in section NFPA 99). While this insures the safety of doctors, nurses, patients, and visitors, it is not sufficient for data centers
that may be controlling lifesaving and life supporting equipment that is computer based. Loss of power, even for a fraction of a second, may require minutes or hours to restore all equipment to full operational capacity. This will result in lost hours, and possibly in lost data. If an internet commerce site goes down and nobody can make purchases, every minute results in lost revenue. If a call center loses Voice over IP phones, they cannot handle support calls, and customer satisfaction and confidence is affected. So the standards for critical power and cooling systems will differ by the level of operation being supported.

**Literature Review**

There are standards published by various organizations meant to provide guidelines for the design and implementation of data centers. These published standards are used by architectural and engineering firms, consultants, designers, and end users to create data center designs that suit the needs of the IT applications. However, standards are not required.

Codes are required and enforced by the Authority Having Jurisdiction (AHJ), the building and electrical inspectors that are present during construction of new facilities. Assuming the company and its contractors follow construction law requirements, these inspectors are also involved with upgrade and remodeling projects. The standards published by National Fire Protection Association (NFPA) do not become code until the local jurisdiction (city or state government) adopt them into the legislature, at which time they become law.

Standards regarding security for IT critical power and cooling systems are not included in most of the publications considered industry best practice guidelines. Individual manufacturers, who create the security and monitoring systems for critical power and cooling delivery equipment (such as Schneider Electric, Emerson, and Eaton) publish white papers and case studies that detail the benefits and security realized by focusing on security for data center gear.
It should be noted that many white papers revolve around specific solutions created by manufacturers, and that these components may not be included in a data center design project.

Sources for Standards and White Papers

There are a number of organizations that publish standards and documentation for data center design. We will review the sources accepted for data center design in the North American market.

National Fire Protection Association (NFPA)

The NFPA publishes the most widely known and accepted standard – NFPA 70, the National Electric Code (NEC). This includes the guidelines for safe implementation of electrical systems for residential and commercial buildings. They also publish NFPA 90A: Standard for the Installation of Air-Conditioning and Ventilating Systems, and NFPA 90B: Standard for the Installation of Warm Air Heating and Air-Conditioning Systems. At this time security is not addressed in any of the NFPA standards publications. For the record, fire detection and fire suppression are included, and there are provisions made for data centers to include chemicals and methodologies that would cause the least disruption in the event they are deployed.

The NFPA standards are updated and published on a three (3) year cycle. The current published versions are 2005, 2008, and the 2011. These standards must be reviewed and adopted into legislature by each municipality that chooses to use them as codes. At time of this writing, the most widely accepted standard was 2008; only 19 states have adopted the latest version of the NEC (as illustrated in Figure 1 below). This means that even if security for critical power and cooling systems is added to the 2014 NEC, it may not be required by code until 2020 or later in the majority of the United States.
For those states denoted as “local adoption”, the report details that some municipalities still utilize the 2002 standards. The full report is available on the National Electrical Manufacturers Association web site (NEMA.org).

Figure 1 - NEC Adoption by State (NEMA.org, Standards subheading technical)

**Telecommunications Industry Association**

TIA 942-2005 Telecommunications Infrastructure Standard for Data Centers has been published in association with ANSI (American National Standards Institute). The standard is important for many elements Data Center Design, including size, layout, cable, power, and cooling infrastructure. Security is mentioned in Section F.6 Security Site Selection
Considerations (TIA 942-2005, page 82) in generic terms such as equipment situated outside should be adequately secured, and common areas should be monitored with cameras.

While this is pertinent advice, it is far from a set of standards that can be followed to provide adequate security coverage for a highly sensitive data center operation. Since the focus is on Security Site Selection Considerations, the majority of the items address geographical issues such as flood plains and proximity to military bases, nuclear operations, railroads, highways, and airports. They do stipulate that the building should not be located in a high crime area.

The TIA 942 standard is being updated to a 2012 revision that may increase the security requirements, but it has not yet been released. There are no indications that the section on Security Site Selection Considerations will be expanded to include physical security of critical power and cooling delivery systems, or that a separate section to address security will be added. It is highly doubtful that this is part of the update.

The Uptime Institute

The Uptime Institute has created a widely accepted tier format that explicitly defines four (4) levels of data center classifications. These are published in the Data Center Site Infrastructure Tier Standard: Topology and Data Center Site Infrastructure Tier Standard: Operational Sustainability standards guides (as published on the web site uptimeinstitute.com). While both mention securing areas, neither standard goes beyond saying that access must be monitored and controlled. References to the critical power and cooling delivery systems primarily deal with redundancy and performance. They do categorize natural (flood, seismic) and man-made (nuclear power, transportation, military) risks.
Green Grid

As an industry standards body that consists of leaders from government and private organizations, their primary focus is on Data Center Efficiency. Their standards define methods of measuring environmental issues. While there are implications of waste due to breaches (i.e. release of toxic elements into the environment, such as refrigerant gases that damage the ozone), the Green Grid does not address security.

National Institute of Standards and Technology (NIST)

The standards addressed by NIST are primarily for code and logical breaches, and do not address any physical intrusion. These standards are applicable for data center control software. The key is that the data center design must implement this security system to cover the network software and hardware that is being utilized to control the critical power and cooling delivery systems. With some older Building Management Systems, this may not be possible, as they may run on proprietary networks. However, in that event, those systems generally do not have internet based access and run “stand alone”, so they are less prone to external breaches.

Bicsi (Building Industry Consulting Services, International)

Bicsi has published the ANSI/BICSI 002-2011, Data Center Design and Implementation Best Practices. Bicsi is best known as the industry standards body responsible for telecommunications equipment classifications (Category 5e, Category 6A, etc.), as well as creating a certification program for telecommunications installers and designers.

Of all the standards bodies, Bicsi published the most comprehensive document for data center design, especially with regards to security. As detailed in Chapter 12 Security, they define physical barriers (fences, walls) as “not prevention and should be layered with other countermeasures like alarms, surveillance, and guards” (ANSI/BICSI 002-2011, Data Center
Design, page 126). This is just one example of the multitude of security issues addressed by the Bicsi Data Center Design standard.

While not specifically for critical power and cooling delivery systems, the Bicsi standards, if applied, would provide more than adequate security. They key issue here is who the design is being provided for – the Information Technology staff or the Buildings / Facilities Management group. If there is separation between the two (2) departments and they design to different security levels, the critical power and cooling delivery systems may not receive adequate protection. In this case, it is the responsibility of the IT Department to work with the Facilities Group to insure that a safe level of security is included in the design of critical power and cooling delivery systems that support data center operations.

Another limiting factor for the Bicsi standard is that the organization itself (Bicsi) is not universally accepted as being a de facto standards body. While they have provided telecommunications standards that have been adopted globally, their efforts to break into other telecommunications and information technology arenas have not been entirely successful. While the Bicsi Registered Communications Distribution Designer (RCDD) and Outside Plant (OSP) Designer certifications are accepted as the top level of professional achievement in their respective fields, others like the Network Transport Specialist (NTS) and Wireless Designer (WD) are considered copies of better certification programs supported by manufacturers like Cisco. For this reason, some end users and design professionals may defer to the TIA-942 standard and the Uptime Institute’s Tier Standards rather than the Bicsi standard; some consider it an attempt to benefit from training and testing for the Data Center Design Consultant (DCDC) certification. This is unfortunate as Bicsi has drafted the best Data Center Design standard, which is both comprehensive and
vendor agnostic. As the Bicsi site states “BICSI publications are standards-based, vendor-neutral, and are known for their careful research, precise writing, detailed graphics and tables, and easy-to-understand format” (Bicsi.org).

Manufacturers

The leading manufacturers in the data center equipment world, including Schneider Electric, Emerson, and Eaton, have all published white papers and case studies that detail the benefits realized by including security as a component of data center design. These organizations also publish application notes that deal with electrical and mechanical engineering in high detail, including the exact processes needed to monitor and protect critical power and cooling delivery systems.

APC

In White Paper 82 Physical Security in Mission Critical Facilities, author Suzanne Niles addresses data center security in detail. Regarding critical power and cooling delivery components, she writes: “Take note of all external plumbing, wiring, HVAC, etc., and provide appropriate protection. If left in plain site or unprotected, these infrastructure components can be used to sabotage the facility without having to disable security measures.” This statement perfectly describes an issue that many IT facilities managers never consider – IT operations can be disabled without ever breaching the facility or hacking the network. An entire operation can be halted with a simple act of vandalism on a critical power and/or cooling delivery system component that is not properly protected or monitored (Niles, S. 2004).

In APC White Paper 124 Preventive Maintenance Strategy for Data Centers, Thierry Bayle notes that performing scheduled maintenance provides an opportunity to not only
insure operational stability, but to identify possible security breach attempts due to theft or
vandalism (Bayle, T. 2010).

**Raritan**

In their white paper An Introduction to Data Center Infrastructure Management, the
need for constant monitoring and tracking of critical power and cooling delivery systems is
vital to again, insure operational stability and also identify any attempted breaches or areas
where a breach may be conducted.

**Textbooks, Manuals, Other Sources**

There are textbooks, technical manuals, and commercial books that address security in
data centers. Some address the matter peripherally – security for networks or systems, or in
general terms; others detail them in direct context to compromising the critical power and
cooling delivery systems.

**Network Security**

Network security standards are detailed in a multitude of textbooks, manuals, and
commercially available text. For data center Building Management Systems (BMS) or Data
Center Information Management Systems (DCIM) that are run on conventional networks (as
opposed to RS-485 Serial Networks detached from TCP/IP), all of the standards for network
security apply.

In Part Two of his text Network Security Essentials, William Stallings describes the
levels of authentication, transport security, WLAN and IP security required for a safe
network. Part Three of the same text describes the necessary firewalls, intrusion detection,
and malware/virus efforts needed. These elements must be applied to a data center critical
power and cooling delivery system security design (Stallings, W. 2011).
Training for all security plans and systems is absolutely vital and must be addressed. “Information security awareness programs serve a critical role in keeping an organization safe by keeping the user community vigilant against the dangers of intruders” (Tipton & Krause 2007). It begins with an attitude change that everyone needs to be aware of all dangers, both physical and logical, and not just “because the higher-ups say so”. Constant effort must be made to keep security in the front of all end users’ minds.

When developing a security plan, a security baseline must be developed and documented. While this applies to information security in general, it is also applicable to protecting against external and environmental threats. “Protecting your organization from natural or man-made disasters should be considered a primary and critical concern by any organization” (Layton, 2007). The text continues with “The scope of this control should be part of the annual risk assessment an organization undergoes to evaluate the appropriate controls and safeguards required to uphold the integrity of the security policy and associated business requirements”. This statement illustrated the importance of measurement, documentation, and scheduled review of security policies.

Safeguarding equipment is the primary purpose of physical access control measures, which establish integrity of all equipment not in a locked and secured environment. For equipment and components exposed to external access, security “may include human-based monitoring and control methods, such as security guards and badges as well as simple administrative mechanisms and visitor escort” (Schou & Shoemaker, 2007). This approach is not an option for a comprehensive security system for critical power and cooling delivery systems; it is a requirement.
Layered Security is “a fundamental element of any comprehensive security program and is absolutely vital for designing and managing security in large IT systems environments” (McCumber, 2004). This model uses a bank to illustrate the methodology: the exterior is surrounded by a parking lot with ample lighting and limited landscaping that might block the view of security cameras, which surround the entire facility. Lighting is incorporated into parking blocks and pillars that further provide protection. Secure glass is used in multiple layers, as are external walls which are manufactured with dual bricks. Once inside, the security layers continue, with surveillance cameras, security guards, and bullet proof glass surrounding locked tellers areas. All of these elements can be modeled in the design of a secure facility housing critical power and cooling delivery systems for a data center.

**Social Engineering**

The most prolific author of computer hacking books, Kevin Mitnick, addresses the issues of hacking and social engineering in his books. He has written and is the subject of a number of hacking books, being the first person to hack the telecommunications industry and (arguably) the federal government.

Mitnick describes how he has successfully obtained passwords and other information by simply asking for it (The Art of Deception, 2002). Mitnick describes The Human Factor as Security’s Weakest Link – quoting Albert Einstein: “Only two things are infinite, the universe and human stupidity, and I’m not sure about the former”. Whether being helpful or afraid that they might insult someone, many employees divulge sensitive information (or open doors) to unknown individuals daily. Therefore security is an illusion – something we think we have achieved but really have not, due to end user error.
Another issue is that hackers don’t operate on a 9 to 5 schedule like much of corporate America. If surveillance isn’t maintained around the clock, that opens up a window of opportunity for a breach. Even if a company spends excessive time and money to create a secure computer system, “a hacker who is competent enough, determined enough, and willing to spend enough time is nearly impossible to keep out” (Mitnick, The Art of Intrusion, 2005). When the night security guard comes on and goes on rounds, the diligent hacker, who knows the guard’s routine, can easily breach an outside wall while nobody is watching the security camera monitor.

Pretexting is another form of social engineering that can be used to compromise critical power and cooling delivery systems. Defined as “the act of creating an invented scenario to persuade a targeted victim to release information or perform some action” (Hadnagy, 2011), pretexting can be a dangerous and effective tool if used properly.

By creating an electrical or mechanical contractor uniform and badge, a social engineer could access the external cooling and power delivery system components at a facility without going inside and dealing with the receptionist/guard or IT / Facilities personnel who might normally approve or accompany this type of worker. Chillers, condensers, transformers, and generators that are located outdoors and not behind locked barriers (fences, walls, or enclosures) might be accessed by simply driving up in a work truck. If anyone questions their presence, all they need say is they are doing repair or maintenance, and they could compromise the equipment in a matter of moments. A foreign substance entered into a water chilling system or generator fuel tank could effectively halt operation of the equipment immediately. Only by securing the external equipment, monitoring it with
surveillance cameras, and training employees on social engineering will deter this type of attack.

**Research Methods**

Research was conducted in both a secondary and primary manner. The secondary research utilized the sources listed above in the Literature Review section (and as detailed below in Secondary Research section). Primary research consisted of discussions held with IT professionals who have exhibited detailed knowledge in their respective fields (i.e. Subject Matter Experts), along with site visits of select data center facilities.

**Secondary Research**

Secondary Research consisted of books, articles, literature, and electronic database repositories on system requirements and specifications. This will include information obtained from viable sources on the internet. These sources, as detailed above, include industry standards bodies (The Uptime Institute, Green Grid, Bicsi). Also included were white papers from various manufacturers of Critical Power and Cooling applications, as well as monitoring device hardware and software vendors.

**Primary Research**

Discussions were held with Subject Matter Experts who have direct input on data center design projects; in some cases, this discussion included a site visit. Due to the highly sensitive nature of security, especially regarding internal IT equipment and deployment, all data used from direct discussions with Subject Matter Experts will remain anonymous.

The following are summaries of the conversations held as well as descriptions of the methodologies for data center design implemented:
Industrial Facility
The TIA 942 standard, in its final statement of security site selection considerations (see Appendix 2), states the obvious: The building should not be located in high crime areas.

This was evidenced at a site visit to an automotive supplier located in the middle of an industrial area of a large urban population. All of the critical power and cooling delivery system components located outside were repeatedly vandalized and/or stolen. This included the cooling system condensers, the utility transformer, and a natural gas generator.

The transformer was the responsibility of the utility, and while the target company experienced no financial responsibility for securing the area, they did experience downtime with each incident of vandalism. In this case, the vandalism was due to cinder blocks and other items being thrown at the transformer, causing damage and shorting out the operation when the debris used was metallic. Only after repeatedly being petitioned to secure the equipment did the utility eventually build an enclosure (locked and secured) surrounding the transformer.

Because of the relatively manageable size, the cooling condenser was replaced and reinstalled on the roof. This put the unit out of site from ground level, and allowed the company to create internal pathways for the cooling medium (refrigerant) piping and electrical pipe and wire, both elements which were damaged and stolen at various times. Additionally, each time the copper was stolen from the refrigerant piping it released toxic gas into the environment, an offense that could be punishable by fines.

The generator, however, was too big to easily build a secure enclosure, and was too heavy to relocate to the roof without a structural analysis of the roof by a licensed structural engineer. It was fueled by natural gas, and extending the feed pipe may not be possible. Again, each time the unit was damaged, downtime was experienced and the time could be
extended if the gas line was damaged and the supply cut off by the utility until repairs were made.

The final solution was to replace the natural gas generator with a diesel fuel generator, and install both in an empty factory bay that had no windows. This removed the unit from visual contact with external parties, very important as the gas tank held up to 120 gallons of diesel fuel. A barrier wall had to be constructed to protect employees, and a vent system was installed in the wall which opened exhaust panels to the environment whenever the unit was operating.

**New Data Center Construction**

Another site visit was to an extensive data center construction project for a major automotive manufacturer. The building is being built as an attachment to a current facility; however, all power and cooling delivery systems are independent and will be managed as a completely separate operation.

The digital rotary UPS (DRUPS) systems will be installed behind 20’ brick walls that provide ample security and allow for maximum air flow for cooling and ventilation. Each 2.4 Megawatt unit will have its own secured area, and will be monitored with multiple surveillance cameras. The power delivery bus system will be installed 3’ below the ground surface, and will be housed in a fire and water retardant duct. This delivery system will enter the data center building below ground level, so it will never be exposed to the elements or human view, minimizing the chance of vandalism.

The cooling solution is similar in regards to security protection. There will be five (5) chilled water towers, each with its own walled off protected area. The chilled water will enter the building through a channel protected by both metal and concrete, and will not be
exposed to the elements (although the channel itself will be in plain view. In the data center operations area, multiple cooling units in an N+2 Redundancy configuration will be deployed.

There will be a Building Management System as well as a Data Center Infrastructure Management system for critical power and cooling control. The systems will have some redundant operational capacity, and the IT staff will manage the DCIM while the Facilities staff will manage the BMS. Both staffs will operate 24 hours 365 days, as now control will be allowed outside of the walls of the data center. External monitoring will be allowed only through the company VPN. The control network will be standalone from the data center production network, furthering segregation and increasing the layered model effect. No external devices will be allowed to access the control networks; only company issued computers will have access to control of the critical power and cooling systems.

Security will also include security guards internal and on the perimeter conducting patrols 24 hours 365 days. Only people with a high level of clearance will be allowed into the facility. There will be no visitors at any time, including vendors, which will only be allowed to conduct business in facilities currently in place in the existing building.

**Major Retailer Data Center**

Another example of a layered approach was witnessed at the data center of a major retailer. This facility was a dedicated building housing the POS operations of a global retailer headquartered in the Midwest. This facility was first established prior to publication of any of the current standards, but could easily have been a model for the Data Center Layered Security Design drawing which follows.
The first floor housed the diesel generators on one half of the facility, with the diesel fuel tanks directly below them in the basement. This allowed easy access to the utility feed, which was adjacent to this area in a locked and secured outbuilding. The other side of the first floor contained the air conditioning units, which were fed by a water chiller located in a secured, walled area adjacent to the building on the opposite side of the electrical feed. Critical power and cooling was delivered to the actual data center on the second floor of the facility through chases located adjacent to the building support beams in the central area of the building.

The entire first floor electrical and mechanical rooms were surrounded by service pathways which were large enough for delivery trucks and forklifts to transport gear. This created a dual

---

Figure 2 - Data Center Layered Security Design (From ANSI/TIA 942)
walled system with all gear protected from the external area by a minimum of two (2) walls. This was repeated on the second floor – a narrow hallway surrounds the entire floor, and the data center was behind the second wall. This arrangement created a secure and environmentally sound solution.

Concrete vehicle bollards (protective pillars approximately 4’ in height) surrounded the building on the first floor. These were, however, made part of a decorative brick fence, so that they did not attract attention. Both floors were surrounded with reflective glass windows on top of the brick exterior, so that it appeared to be a normal office building. This building is in a highly populated section of a large urban area, and according to the facilities director, has never been a target of a breach. The Director of Security confirmed this fact – the facility included vandal proof cameras at all corners, all entrances, and at both the utility outbuilding and the cooling tower enclosure, and there have been no breaches (other than a few minor vandalism incidents) in over 25 years of operation.

Industry Consultant

An interview was conducted with the vice-president in charge of data center design and operations for a multi-billion dollar electrical engineering and manufacturing firm. This executive made the following observations:

Training and documentation is lacking in nearly all existing data center facilities and operations. While physical security controlled through access control methods is good at most facilities, security awareness is almost never addressed. This means once an external individual enters the space, he is almost never escorted and allowed free access to areas that need to be secured. For facilities with existing policies, they are almost never enforced. Seeing as 60%-70% of the errors or incidents that affect data center operations are due to human error, this fact
is staggering in that prevention would be as simple as providing an escort who is trained on internal policies.

    No drills are ever conducted. While some companies may conduct penetration testing, this does not necessarily help with testing the availability of critical power and cooling delivery systems (unless the pen test is specifically targeted at the BMS or DCIM systems). Mock failures will identify whether panic ensues, or whether the IT, Facilities, and Security/Life Safety personnel are trained and equipped well enough to handle a breach or loss of power and cooling.

    Budget cuts have severely affected operations. Staffs of 22 cut in half leave 11 people to handle an increasing load, especially with regards to security and operations. This compounds risk, as a breach may not be discovered until a critical situation is escalating, and there may not be enough staff to react to the incident. While finance and executive decision makers are aware of the needs, they are remiss to release funding and resources without the presence of a clear and distinct threat.

**Analysis**

    As described in the Literature Review chapter, the documentation in forms of standards does not include specific security guidelines for critical power and cooling delivery systems. With exception to Bicsi 002 - Data Center Design and Implementation Best Practices the standards focus on performance and operations. The Bicsi Data Center Design standard takes the TIA 942 to a higher level of design including operational functions and monitoring/security. The TIA 942 standard is a more granular and detailed specification for design than the Uptime Institute Tier Standards, which primarily describe different levels of design based on availability and redundancy. Therefore Bicsi 002 - Data Center Design and
Implementation Best Practices is the most comprehensive of the data center design standards available to IT professionals.

When designing security for critical power and cooling delivery systems, a layered approach for both physical and logical protection must be incorporated. Once designed, a comprehensive deployment plan must be developed. This will include installation, testing, training, and commissioning.

Figure 3 - Bicsi Layered Security Diagram (Bicsi 002 Data Center Design)

As denoted above, the layered approach for physical security must be applied to all critical power and cooling delivery system components, including the TCP/IP logical components (BMS, DCIM), and the physical layer transport components (Serial RS-485), if applicable. This must be a cross functional effort and include the Information Technology, Security/Life Safety, and Facilities Management teams.

Critical Components of Data Center Design

The design of a data center begins with the geographic location of the physical structure. The building physical attributes must then be designed, including floor plan and room structuring. Once this is complete, the sizing of the critical power and cooling
delivery systems can be completed. After the layout of the utility demarcation points is established, the facility entry points are determined, the pathways for cabling and piping are designed and the placement of the power and cooling gear is finalized, a security design for the critical power and cooling delivery systems can be created.

**Security Design for Critical Power and Cooling Delivery Systems**

The security design for critical power and cooling delivery systems should include the following requirements:

- All external equipment components must be separated from public view and access.
- Surveillance for all components (via security camera) outside of data center.
- Monitoring of security camera feed, including all data center entry/egress points.
- BMS and/or DCIM software for full time monitoring of critical power and cooling delivery systems, and all data center production equipment.
- The BMS/DCIM system must be segregated from general production and/or data center network.
- All BMS/DCIM access is informational only. Access control allowing only qualified power and cooling personnel have access to system control and operation.
- If external access is granted to BMS/DCIM it should be through VPN (Virtual Private Network) and not public web based access.
- Security Training provided for proper use of monitoring software.
- Penetration testing and disaster recovery drills must be conducted.
- Periodic (semi-annual and annual) review by cross functional team on security policies, operations, and change control.
• Use of personal equipment (smartphones, tablets, non-company issued computers) is prohibited.

**Conclusion and Suggestions**

By creating a comprehensive security component as part of a Data Center Design, you insure the availability and integrity of your IT operations. Failure to do so can result in major losses of time, revenue, and capital. Most issues regarding lapse security for critical power and cooling delivery systems revolve around the lack of a coordinated effort put forth by all the functional departments – Security/Life Safety, Facilities, and Information Technology. Organizations need to increase cross functional communications – the knowledge is there, the execution is lacking. There also needs to be a trend amongst industry standards bodies to integrate security into Data Center Design, Implementation, and Operations documentation. As awareness to the issue of infrastructure security increases, funding and support from executive management will also increase. IT professionals charged with the security of critical power and cooling delivery systems must remain diligent in keeping this issue a focus of the enterprise.

**Support Standards Efforts**

Manufacturers generally drive the standards efforts; end users can push groups like NIST, the Uptime Institute, Bicsi, and the TIA to include security in their data center design standards. IT professionals directly involved in the design and operation of critical power and cooling delivery systems for data centers should work with the manufacturers to make security applications a primary focus of Research and Development.

Groups like 7X24 and ASHRAE hold regular meetings for their local chapters. IT professionals should either join or petition their organization to keep a member active and attend all meetings. Identify security as an issue you consider vital to your operations. Large
organizations can nominate qualified individuals to the standards committees for ASHRAE, Bicsi, and the NEC to provide input on future standards.

**Include Security in Data Center Designs**

Whenever involved in a data center design and/or implementation project, make sure to identify security for critical power and cooling delivery systems as a requirement for the final design. Be prepared to support your position by researching and preparing documentation on how breaches to data center infrastructure have hindered operations in your particular company or industry.

For existing facilities and operations, include security (and lack thereof) in all annual reviews and assessments. Create awareness of the need for increased security for critical power and cooling delivery systems before a man-made disaster or breach halts operations. Whenever new equipment is scheduled for deployment, make sure that sufficient critical power and cooling is available to support the new gear.

**Track and Document all Breaches**

It is important to monitor operations for all critical power and cooling delivery systems, track performance and issues, and document each and every breach or incident. This information must be communicated to cross functional teams in the enterprise, including Security/Life Safety, IT, and Facilities Management.

This includes internal and external components, as well as incidents involving internal employees, external vendor, contractors, and maintenance personnel, and vandalism and breaches by hackers or other external entities. A good example of this is the electrician working in an office area who trips a breaker that shuts down a computer closet with network distribution
equipment. First, this gear should be fed with critical backup power (generator or UPS), and must have consistent cooling. If not, separation in accordance with the layered security model must be instituted to insure that all operations are continuous.

**Conduct Additional Research**

All competent and conscientious IT professionals conduct continuous research on the technology and methodologies for their particular focus. Research can consist of participation in focus or discussion groups at local chapter meetings that deal with critical power and cooling applications (e.g. 7X24, ASHRAE, AFCOM), participation in online forums, or discussions with other IT professionals that take place while conducting business or completing normal job functions. If you are not familiar with the security standards, obtain and read copies of the standards reviewed in this paper (Bicsi, NFPA/NEC, Uptime Institute, and TIA-942).

**Create a Comprehensive Security Plan**

If the security of your company’s IT operations is your responsibility, budget sufficient resources to create and maintain a comprehensive security plan. As detailed in Bicsi 002 - Data Center Design and Implementation Best Practices, this includes all physical and logical security, 24 hour surveillance, and ongoing monitoring and change control as applied to the data center as a whole. For critical power and cooling delivery systems, it is vital to identify all those components that may be out of the domain of the controlling department, or to create a cross functional team of Information Technology, Security/Life Safety, and Facilities Management personnel so that all components are included in the security plan.
References


http://static.schneider-electric.us/assets/consultingengineer/appguidedocs/section10_0307.pdf

Indianapolis


National Electrical Code (2012). Retrieved from
http://www.nema.org/Technical/FieldReps/Pages/National-Electrical-Code.aspx


Uptime Institute. (2010). uptimeinstitute.org. Data Center Site Infrastructure Tier Standard: Operational Sustainability. The Uptime Institute, LLC

Appendix 1: Explanation of Terms

The following are terms used that are specific to the design, operation, monitoring, and maintenance of Critical Power and Cooling Delivery Systems applicable in Data Center Design:

**Building Management System (BMS)** – software that monitors and controls critical power and cooling delivery systems, including air conditioning, heat, humidity control, generators, transformers, and electrical switch gear.

**Chiller** – device used for liquid based cooling systems that transfers the heat captured in the liquid medium to the environment. The liquid might be water, coolant (i.e. anti-freeze), or a mixture of the two. Sometimes referred to as a cooling tower, dry cooler, or wet cooler.

**Condenser** – device used with refrigerant based cooling systems that transfers the heat captured in the cooling medium to the environment.

**Cooling** – device(s) that generates cool air, from 68°F to 78°F, from ambient air; any number of various forms of Air Conditioner.

**Critical Power** – power provided for data centers that is provided by the utility, generators, or an Uninterruptible Power Supply (UPS).

**Data Center** – a centralized repository of computer equipment that includes, but is not limited to, servers, telecommunications equipment, and digital media storage.

**Data Center Information Management (DCIM)** – software application that monitors and controls Information Technology centric equipment in a data center, including critical power and cooling delivery systems, environmental monitoring equipment, and computer/network hardware operations and performance.
**Fuel Cell** – a power generation device often used for short to medium length power interruptions, often using hydrogen as an alternative fuel. Best suited for high rises and brown field (retro fit) applications where batteries may be too heavy (upper floors) and access to a generator is cost or distance prohibitive.

**Generator** – device for providing power in the event of utility power interruption, utilizing alternate fuel source (Fuel Cell, diesel gasoline, gasoline, or natural gas). Can provide alternate power for time range of several hours, to several days, or indefinitely (in theory).

**Security** – uninterrupted real time surveillance of physical threats, including intrusion, espionage, vandalism, or any form of unlawful activity.

**Sub Station** – demarcation point from utility provided power to organizational entry point, termination, and distribution.

**Uninterruptible Power Supply (UPS)** – electro-mechanical device that provides interim battery or alternate source (Fuel Cell, Flywheel) of temporary power in the event of a utility power delivery interruption. Typical run times range from several seconds utilizing a flywheel with generator, up to several hours with battery technology.
Appendix 2: TIA 942 Section F.6

F.6 Security site selection considerations

- If cooling equipment, generators, fuel tanks, or access provider equipment is situated outside the customer space, then this equipment should be adequately secured.

- Also, the data center owner will need access to this space 24 hrs/day, 7 days/week.

- Common areas should be monitored by cameras, including parking lots, loading docks, and building entrances.

- The computer room should not be located directly in close proximity to a parking garage.

- The building should not be located in a 100-year flood plain, near an earthquake fault, on a hill subject to slide risk, or down stream from a dam or water tower. Additionally there should be no nearby buildings that could create falling debris during an earthquake.

- The building should not be in the flight path of any nearby airports.

- The building should be no closer than 0.8 km (½ mile) from a railroad or major interstate highway to minimize risk of chemical spills.

- The building should not be within 0.4 km (¼ mile) of an airport, research lab, chemical plant, landfill, river, coastline, or dam.

- The building should not be within 0.8 km (½ mile) of a military base.

- The building should not be within 1.6 km (1 mile) of a nuclear, munitions, or defense plant.

- The building should not be located adjacent to a foreign embassy.

- The building should not be located in high crime areas.