PHYSICAL VULNERABILITIES SEMICONDUCTOR COMPANY DATA CENTERS AND TESTING MEASURES

CRISTOPHER GUIPOC

University of the Cordilleras, Baguio City, Philippines
E-mail: cguipoc@yahoo.com

Abstract - Data centers represent a key technology in an increasingly digitized world. They house the servers and storage systems with their associated network components so that applications are present with the agreed availability and the required performance. Equally important is the physical infrastructure that provides the power and cooling for these components, as well as permitting the monitoring of all the operating parameters. Increasing importance is being given to all aspects of security. This starts with well-known anti-virus protection and firewall systems, although protection against physical threats also calls for increasing attention. Besides defense against such very real threats as burglary and theft, it also involves avoiding "traditional" potential dangers of fire, smoke, water and dust, to only name but a few. This research uses the data gathered from various semiconductor companies in South East Asiato explore each of these Data Center threats and identifies the measures that can be used to counter physical hazards.

Keywords - Data Center, IT Security, Physical Security, Physical Hazards

I. INTRODUCTION

A data center is the epicenter of any online infrastructure. A data center's size can vary widely, depending on an organization's needs. Commonly, a data center consists of large groups of interconnected computers and servers that are responsible for remote storage and/or processing of data. Even though most potential intruders or hackers target the network of an infrastructure to get in, their eventual goal is to get access to data. In addition, there is a need to pay more attention to the physical security in data centers with the ever-increasing sophistication of social engineering and hacking methodologies [1].

Data centers should guard against physical threats such as fire, water damage, burglary and theft. Protection against these risks is becoming increasingly important due to the world's constantly advancing digitization and dependency to data centers [2].

According to the Cost of a Data Breach Survey,[3] in which 49 U.S. companies in 14 different industry sectors participated, they noticed that 39% of companies say negligence was the primary cause of data breaches, Malicious or criminal attacks account for 37 percent of total breaches, and the average cost of a breach is $5.5 million.

Some industries in particular, such as financial and healthcare, are responsible for mass amounts of highly sensitive data, such as social security numbers, medical records and credit card accounts.Multitenant data centers must also be extremely vigilant in order to protect their customers' data. There's no doubt that data breaches are here to stay, and the threat will only grow worse. Every CIO and IT manager will have to grapple with these challenges and make data center security a priority. In fact, as digital data continue to flood into data centers via cloud computing, tablets and smart phones, those charged with securing these valuable facilities must assess their risk, including the threat of physical breaches from outside and within.

Physical security is needed to protect the value of the hardware and the information inside the data center [4].

The cost of a breach of security can have severe consequences on both the company managing the data center and on the customers whose data are copied. The 2012 breach at Global Payments, a processing vendor for Visa, where 1.5 million credit card numbers were stolen, highlights the risks of storing and managing valuable and confidential data [5]. As a result, Global Payments' partnership with Visa was terminated, it was estimated that they lost over $100 million [6].

The protection of data centers from physical hazards must begin on several levels, because the threats also act through different vectors, including everything from "Acts of God" (force majeure), organizational defects and technical failures to intentional action [7]. Some years ago, a few days of downtime per year were perfectly acceptable, but because industry's increasing dependence on digital systems, it has led to far tighter requirements. This is because IT failures are very costly for semiconductor companies, and other digitalized organizations. Medium-sized firms alone have to cope with the loss of business-critical IT systems worth up to $432,800 per company and year on average. This has emerged from a survey carried out in 2013 by the market research company Techconsult involving 300 companies with 200 to 4,999 employees [8]. A survey by EMC also revealed there had been either data losses or downtimes at 56% of companies in the US during the previous twelve months [9].

An all-round approach always helps when it comes to protecting complex systems. A data center consists of a large number of systems: climate control, power supply and distribution, network connectivity, access control, and last but not least the structural shell, designed as a conventionally built room or as a modular "room-in-room" system. Climate control, power supply, data connection – all of these elements need to be optimally integrated into the data center concept and their management needs to be coupled to data center administration [10].

II. METHODOLOGY

There are various gathering techniques that were used during this research. The first is to review published literatures related to IT Security. The primary data sources however, were the interviews, physical inspections, and observations conducted to several semiconductor companies in South East Asia.

Qualitative research methods used on this research includes one-on-one interview

The researcher travelled to the physical location of several semiconductor companies and inspected their Data Centers, to explore the physical threats, and their counter measures in place. This gathered information will be published so other companies relying heavily on Data Centers can use it to improve their overall IT Security procedures and processes. This will be the contribution of the researcher to the body of knowledge.

III. RESULTS AND DISCUSSIONS

3.1. Layering Approach

As observed one of the visited sites, Data Center Physical Security measures can be categorized into four layers, the Perimeter security, Facility controls, Computer room controls, and Cabinet controls. Addressing each of these layers provides comprehensive and integrated protection from the facility's perimeter to the cabinets in the data center

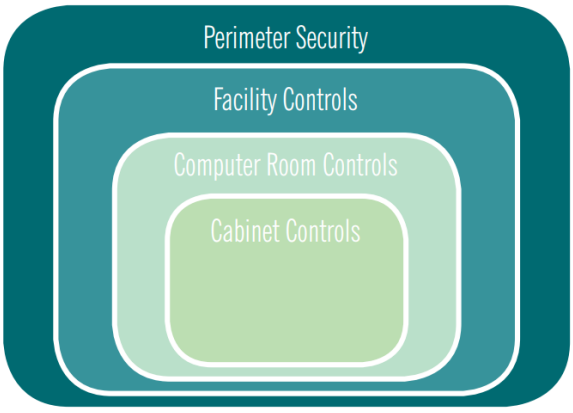


Figure 1: The Four Layers of Data Center Physical Security

The most sound and strategic way to reach optimum physical security is to design and manage your data center in terms of layers. Layering creates depth in your physical protection structure, helping to confirm failure of one element in the system will not create vulnerability in the whole system. The inner layers also help prevent malicious or even unintended data breaches from employees.

Even though the concept of physical security layering obviously makes unwanted entry originating from outside a data center facility more and more difficult, inner layers also help mitigate insider threats, which are often ignored. One of the sites visited by the researcher in China provided the result of their internal survey on how often employees breach data security.

IT Security Breach / Incident	Percentage
Employees admit to knowing that downloading corporate information from their employer is illegal	85%
Employees say they would take the data anyway, regardless of penalties	25%
Employees admit to having taken sensitive data with them to a new position	41%
Employees say they would pass on company	26%
Employers are moderately to extremely concerned that laid off or disgruntled employees will destroy company property	72%
Employers are moderately to extremely concerned that laid off or disgruntled employees will destroy company property	69%

Table 1: Survey results of employees in one of the visited semiconductor companies illustrating their IT security breach incidents

To minimize the IT Security breach on the company, their IT security team deployed various technology and security assets to track people, limit unauthorized employee access to high-priority areas, provide an audit trail of personnel access, integrate with video to provide a record of an attempted breach.

3.2Physical Vulnerabilities and Counter Measures

These are the commonly observed physical threats on the data center the researchers visited, and the corresponding counter measures placed by various companies.

1. Fire - Fire is the one threat to data centers and server rooms that administrators fear most. Even small fires can cause severe damage to IT equipment and infrastructure due to the aggressive gases that are given off. Testing for fire resistance is thus very intensive.

Prevention Approach - Individual elements such as walls, doors and building materials are subjected to flame treatment in accordance with a uniform temperature curve. One of the companies the researcher inspected conducts testing at more than 1,100°C for 90 minutes. During testing, the temperature on the side away from the fire must not increase by more than 140 K (up to 180 K on occasions). Relative air humidity is not measured during this test. Depending on the building material concerned, humidity may rise to 100% after a very short time, which would be dangerous for the server and the infrastructure in the data center.

Real protection is only guaranteed by a system test in which the complete data center and all its components such as doors, as well as bulkheads for cables and pipes are tested under conditions similar to those in an emergency. A system test requires that flames are applied for 60 minutes. This is followed by a 24-hour cooling-off period in the closed fire furnace. This time is referred to as a "post-heating period". The test piece remains in the fire area until the highest temperature in the specimen is reached after a few hours. Particular attention is paid to structurally weak points such as doors, doorframes and cable and pipe entry systems. In order to pass the test, the internal temperature must not exceed the starting temperature by more than 50 Kelvin, and – equally important – the relative humidity must not exceed 85%.

These tests can also be applied by other companies on their data center to confirm if their current setup can withstand fire incident.

2. Corrosive gases and smoke - Gas-tightness and resistance to smoke are important requirements that data centers and server rooms have to meet. The factor of tightness matters when it comes to keeping the smoke from a fire within the server room and not spreading to other parts of the building.

As observed on all the visited sites in South East Asia, fires in IT environments are not extinguished with water but with inert gases or by oxygen deprivation. This only functions reliably if the gases remain within the room and do not reach the rest of the building through leakage. Similarly, fire prevention by oxygen deprivation is bound to fail if fresh air is drawn into the room through doors, windows or structural defects. Tightness of seal plays an equally important role if there is a fire outside the data center. The IT components in the data center have to be protected from aggressive gases because the circuit boards in the servers, switches and other hardware could corrode.

A test procedure and the corresponding test conditions for determining the leakage of hot and cold smoke from one side of a seal to the other side needs to be conducted by companies in their data centers. This "leakage rate" is measured for each test condition investigated. For data centers, tests are conducted on doors and pressure relief valves and flaps because these usually represent the only movable openings into the room. Due to the fire, a pressure of up to 50 Pa builds up on the side exposed to the smoke; the pressure difference between the two sides drives the smoke through all the gaps and openings that are present. A door that functions as part of the fire safety system must hinder the passage of smoke to ensure that the conditions on the other side of the door remain bearable.

According to the IT Security Team, tests are carried out in a test chamber; the test piece is installed in the front of it. A blower system provides the necessary pressure while a heater generates temperatures of around 200°C to recreate the temperature of the smoke. Gaps due to the nature of the system, such as door thresholds or gaps between door wings are measured and recorded. Automatic closing mechanisms also have to be tried out a few times before the test. But this short test does not replace endurance testing of the mechanisms – it is simply aimed at making sure that the door can be properly closed. The real test for smoke resistance is performed at different pressure levels of up to 50 Pa and at room temperatures of 20°C and at 200°C. Successfully tested specimens must not exceed an air change rate between the inside and the outside as defined in the standard. During the tests, it is also important to record if (and which) elements of the door are deformed by the heat, and whether the door can still be opened after the test has been completed.

These tests can also be applied by other companies on their data center to confirm if their current setup can withstand corrosive gases and smoke.

3. Falling debris - The dangers caused by falling debris also have to be considered. The forces so released can wreak great destruction on the hardware and infrastructure. In addition to the fire tests for the security rooms and safes, the researcher also observed that some IT Security teams also conduct impact and drop tests.

The test is conducted after the room has already been exposed to flames for 45 minutes. A wall must be able to withstand a defined impact stress after exposure to flame. If the wall is a load-bearing one, compressive stress is also applied to the test piece.

Five loads are carried out per area (evenly distributed, oscillating or free fall). The test piece must be mounted on a rigid frame and must not give way. Exposed areas such as hinges or locks are also subjected to stress. After testing, the test piece must

be fully functional and, in particular, must not exhibit any adverse effects on its protection class.

4. Protection against unauthorized access - Normally, data centers inside buildings need to be well protected against intruders, because these first have to overcome all the other obstacles such as doors, reception area, cameras and observant staff. Nevertheless, it is important that a room containing expensive hardware and important data can resist even an attempted burglary. One of the visited sites uses what they called The Resistance Class (RC) test. The "RC" has a six-stage classification system is used.

A distinction is made, based on the capabilities of the offenders and the tools they are equipped with. The spectrum ranges from inexperienced offenders and vandals without tools through to experienced, highly motivated perpetrators, who have access to a large number of high-performance power tools. In each case, there are limits to the time that the test piece must withstand the attack for in order to pass the test.
For the category "RC 1", the components must have a limited-to-low level of basic protection against attempted burglaries involving physical force such as kicking, being jumped on, being shoulder-charged, or being pushed up and pulled out. In addition, a non-destructive manipulation test lasting up to three minutes is carried out to dismantle any screwed-on components that can be detached from outside with small tools. The duration of the attack applies for each point attacked. If, for example a complete safe is being tested, there are a number of points that may be attacked, such as the door (hinge side), door (frame side) and cable entry points. The total time is derived from the sum of all the points of attack. The remaining categories are summarized in the following table.

Code	Duration	Experience	Description / implements
RC 2	3 min	Occasional, inexperienced offender	Simple tools: screwdrivers, pliers and wedges
RC 3	5 min	Repeat offender	Additionally: second screwdriver and a crowbar
RC 4	10 min	Experienced offender	Additionally: Sawing and impact tools such as an axe, a crowbar, hammer and chisel, and a cordless drill
RC 5/ RC6	10 min	Experienced offender	Other hand-operated tools, up to and including a drill, jigsaw or reciprocating saw and an angle grinder with a wheel diameter of up to 250 mm.

Table 2: RC classification system – protection against unauthorized access

5. Electromagnetic Protection - Electromagnetic fields are an inevitable consequence when current flows. The energy that is irradiated, the electromagnetic radiation, is undesirable and in some cases harmful. Strong fields can have a negative effect on other electronic devices and make information accessible to unwanted eavesdroppers.
If they are planned and fitted out correctly, IT security rooms will protect hardware and data from the negative consequences of EM radiation. On the one hand, EMC describes how such devices can be protected against harmful interference from external sources.

According to the interviewed IT security personnel, a security room, in its basic state, does not offer any continuous and defined level of protection. However, EMC also involves preventing electromagnetic radiation from which unauthorized persons can tap valuable and sensitive information.

The EMC characteristics of IT security rooms have to fulfil two tasks. On the one hand, they must prevent IT facilities being intentionally or unintentionally hampered by radiated electromagnetic fields while on the other hand, they have to reduce the emission of safety-relevant information from the IT device. The shielding effect of the device housing and the enclosures in which the devices are accommodated can be increased considerably by adding extra room shielding. However, there are no normative requirements regarding this.

Based from the observation, the ideal situation would be a slot-free, electrically conductive shell that neither lets signals in nor out. However, this is impossible in practice according to one of the interviewed IT Support. This is because IT security rooms and data safes are composed of wall segments made of sheet steel, which enable a slot-free, conductive basic shell over wide-area, conductive connections. Openings or gaps must be shielded by suitable media, which involves a significant design effort, particularly with access doors. One basic principle applies: the larger a poorly shielded opening (for rectangular openings/joints: the longest side; for round openings: diameter), the more likely there will be a loss in shielding effectiveness for the relevant frequency range.



Figure 2: Sample design of EMC protected Data Center

The higher the frequency of the incident electromagnetic field, the more negative the effect of any openings in the shell. Therefore, some points such as the use of special gaskets and cable glands or the use of filter connectors must be observed. Basically speaking, the structural design of the sealing system largely determines the effectiveness of the shielding attenuation. The more attachment points

for walls and hinges there are, as well as closure pressure points for doors, and the more uniform the contact pressure and the contact (low impedance) of shell and door/lid are along the seals, the closer we will get to the ideal.

Conductive special seals made of metal fabric on a foam body, as combination seals for EMC and IP protection categories, achieve high shielding attenuation values in the frequency range up to 1 GHz and beyond. They connect the bare metal interior surfaces of doors and removable side panels, roof and gland plates to the bare metal sealing edges of the enclosure body or frame.

With reasonable measures, shielding attenuation values of up to 60 dB can be implemented for security rooms in the frequency range of 30 MHz to 3 (10) GHz. The design effort required to increase shield attenuation above 60 dB for the relevant frequency range would be exceptionally high.
These tests can also be applied by other companies on their data center to confirm if their current setup can withstand EMC breach incidents.

IV. CONCLUSION

Various companies, including the sites visited by the researcher, deploy various technologies, processes, and security measures to physically protect their data center from hazards and physical breaches, whether it be intentional or caused by nature.

In this research, the data center hazards and threats of the visited sites have been identified, and their corresponding counter measures were also documented. In addition, how they test and validate the effectiveness of their counter measures, including the specific parameters, were also captured on this research.

ACKNOWLEDGEMENT

The researchers would like to express his gratitude to the eight semiconductor companies visited in south East Asia for opening their doors for this research. The researcher specifically thank theirIT security team, IT Audit team, and Data Center maintenance team teams for their time, for providing the needed information. We thank all the participants in our research, our mentor and our university who have willingly shared their time during the process of establishing business requirements and conducting visitations on semiconductor companies despite their busy schedule. We thank our loved ones, who have supported us throughout the entire process, for their unconditional support, both financially and emotionally throughout our study and for by keeping us harmonious and helping us putting pieces together. Above all, we thank the Almighty God for providing us the wisdom and strength to complete this research. We will forever be grateful.

REFERENCES

[1] Craig Wolff (December 13, 1989). "Report Finds Fault With E.M.S. Computers". The New York Times. too many E.M.S. employees have access to ...
[2] Maurizio Portolani, Mauricio Arregoces(2004). Data Center Fundamentals. Publishers, Cisco Press, 800 East 96th Street Indianapolis, IN 46240 USA, Chap.5
[3] The Four Layers of Data Center Physical Security for a comprehensive and integrated Approach [1]
[4] "Data center robbery leads to new thinking on security".
[5] Jessica Silver-Greenberg (April 2, 2012). "After a Data Breach, Visa Removes a Service Provider". The New York Times.
[6] Robin Sidel (April 2, 2012). "Card Processor: Hackers Stole Account Numbers". The Wall Street Journal (WSJ). Visa yanked its seal of approval
[7] 2003 CSI/FBI report "Computer Crime and Security Survey."
[8] David Moore; Colleen Shannon (2001). "The Spread of the Code-Red Worm (CRv2)". Retrieved 2006-10-03.
[9] "Net-Worm: W32/Nimda Description". F-secure.com (F-Secure Labs).
[10] John Leyden (February 6, 2003). "Slammer: Why security benefits from proof of concept code".
[11] "Port Scan attacks and its detection methodologies".
[12] Vitaly Shmatikov; Ming-Hsiu Wang. "Security Against Probe-Response Attacks in Collaborative Intrusion Detection" (PDF). The University of Texas at Austin.
[13] "Understanding Denial-of-Service Attacks". US-CERT. February 6, 2013. Retrieved May 26, 2016.
[14] Khalifeh,, Soltanian, Mohammad Reza. Theoretical and experimental methods for defending against DDoS attacks. Amiri, Iraj Sadegh, 1977-. Waltham, MA. ISBN 0128053992. OCLC 930795667.
[15] GIAC Certifications. Global Information Assurance Certification Paper.

★★★