Data center supportive infrastructure security threats and threat mitigations

Lauri Haverinen, Jukka Pajukangas

Oulu University

2021-11-29

ArctiqDC – Arctic datacenters 2019 - 2021

ArctiqDC – Arctic Datacenters project aims to strengthen the regional data centre industry's products, services, solutions and offerings to customers (parties) outside the region, nationally or internationally. This should be done by demonstrating and proving that; Investing and operating data centres in Arctic regions have low and among the lowest investment and operating costs in the world in terms of cooling and power distribution

ICE
RI.SE SICS NORTH

UNIVERSITY OF OULU

OULUN ENERGIA

Oulun DataCenter
Northern Data Cloud

H66

Hushållnings
sällskapet

AURORA DATACENTERS

ÄLVSBYNS
KOMMUN

sftec

Business
Rovaniemi

LAPIN LIITTO

xarepo

OULU | BusinessOulu

Interreg
Pohjoinen
Euroopan aluekehitysrahasto

EUROOPAN UNIONI

Executive summary

Data center supportive infrastructure security threats and threat mitigations

Key words: building automation, cyber security, risk management, physical security

This report describes supportive infrastructure of data centers, discusses a variety of human-born security threats and possible threat mitigation and prevention measures. Data center operators can use the observations in this report to reflect on their own risk model and perform corrective actions if required. The observations can also be used in creating automation-oriented security training programs or workshops.

Various industries and organizations are utilizing and becoming more dependent on the resources that the data centers are offering. Data center demand was hitting record numbers in 2020 and future predictions foresee an increasing need for data centers.

Data centers are considered to be part of critical infrastructure that keeps the society running smoothly. Disruptions to data center operations may cause severe consequences to any functionality that relies on the availability of them. Keeping data centers online has very high priority, as outages may result in significant financial or operational capacity losses for various organizations.

Data center core consists of various computing equipment, and it requires a supportive infrastructure that keeps the equipment cooled, powered and protected from various hazards. Failure of support infrastructure can effectively cause operational disruptions, so attacks towards supportive assets may be a valid approach for attackers to reach their goals.

As data center supportive infrastructure may consist of a complex set of heterogeneous assets, multiple viewpoints must be considered when data center supportive infrastructure security is planned. Variety of physical, cyber and human related threats, and combinations of them require a comprehensive assortment of security measures, meaning that operators should not rely on just some single viewpoints of individual security disciplines.

Long lifespans of automation systems can cause challenges in keeping system environments secure. Although the security of operational systems is considered to lag behind, there are signs that the situation may be improving. The subject is being researched and new applications are being developed, but it may take some time until they are implemented in facilities. Although the adaptation of modern embedded systems can reduce the gap between information and operational technology systems, further research on building automation security is still needed.

Although this report categorizes threats to personnel related, physical security, system security, and information leakage threats, there are no countermeasures that would counter specific threats. Some can however improve the level of security regarding multiple threat categories, such as security awareness training. Implementing all of the discussed security measures might also not be the most cost-effective solution as the security budget is typically not unlimited. Instead, organizations should weigh the threats based on their risk model and make the decisions on what are the potential threats and how important it is to protect specific assets.

Oulu University

CONTENT

1 Introduction

As various industries are becoming more and more dependent on cloud services, the demand for facilities offering computing resources and infrastructure has increased strongly. At the turn of the decade, a record for data center demand was reached [1] because of the massive rise in data usage caused by a rapid shift towards virtual workplaces [2]. In their daily functioning, several fields of industry and society operations are relying either on outsourced data center services or the capabilities of their own in-house data centers. Any disruption to these services or centers could cause system outages, data loss and business losses, so it is important to keep these systems available and running.

The core of a data center consists of computing equipment, data storage systems, and networks capable of providing the processing power and various computing services to its users. To remain operational, equipment and infrastructure requires a support system providing control of sufficient air temperature and quality, uninterrupted supply of electricity, and mechanisms to prevent any possible physical damage to the hardware. As the support infrastructure is what keeps data center operations running, any malfunctions within it or attacks targeting those elements may potentially cause serious disruptions to data center operations.

As the economical and operational importance of data centers increases, motivation of different adversaries to target those facilities for economical, political or other purposes can increase as well. The support infrastructure of a data center can be a tempting target for attackers, because successful attacks could open possibilities to disrupt data center operations, extort ransom by holding support infrastructure systems hostage or gain a foothold that could be leveraged in an attempt to access additional internal systems of a data center.

Threats towards support infrastructure of data centers can take many forms: cyber threats, physical threats, human threats or some combinations of them. Consequently, securing the support infrastructure of a data center can not rely on a single viewpoint such as physical or information security, but it must contain multi-discipline approaches and multi-domain security measures. During the planning of the security of the support infrastructure of a data center, guidelines concentrating on cybersecurity, information security, building automation security, IoT security, physical security, ICS security, and human-related security issues should be appropriately considered.

This report describes different components of data center infrastructure, discusses a variety of threats towards these infrastructure components and the ways to counter or mitigate those threats. The focus of this discussion is on the support infrastructure of the data center architecture and it does not consider internal non-physical core operations of data centers, like security of software running on machines or software controlling allocation of executions, encryption or security of stored data or security of networks connecting data center core machines. These topics may be referred to when an appropriate link to them exists from the viewpoint of support infrastructure security, but any reader interested in these topics should search for specific information considering those areas. Also non-human made risks of data center supportive infrastructure are not the focus of this paper, but those will be referred to and discussed if the type of risk or security measure is relevant to securing the data center supportive infrastructure against human threats.

2 Data center support infrastructure

In addition to the computational hardware, data centers require a comprehensive support infrastructure to be able to perform their everyday operations and provide their services reliably, faultlessly and securely. In modern data centers this supportive infrastructure consists of several information systems and networks used to monitor and control not only the cooling and heating systems and the computing equipment power distribution, but also the physical security of the area, life safety systems, and data center operator office space conditions. This chapter describes the main components of this infrastructure. An overview of this environment is presented in Figure 1.

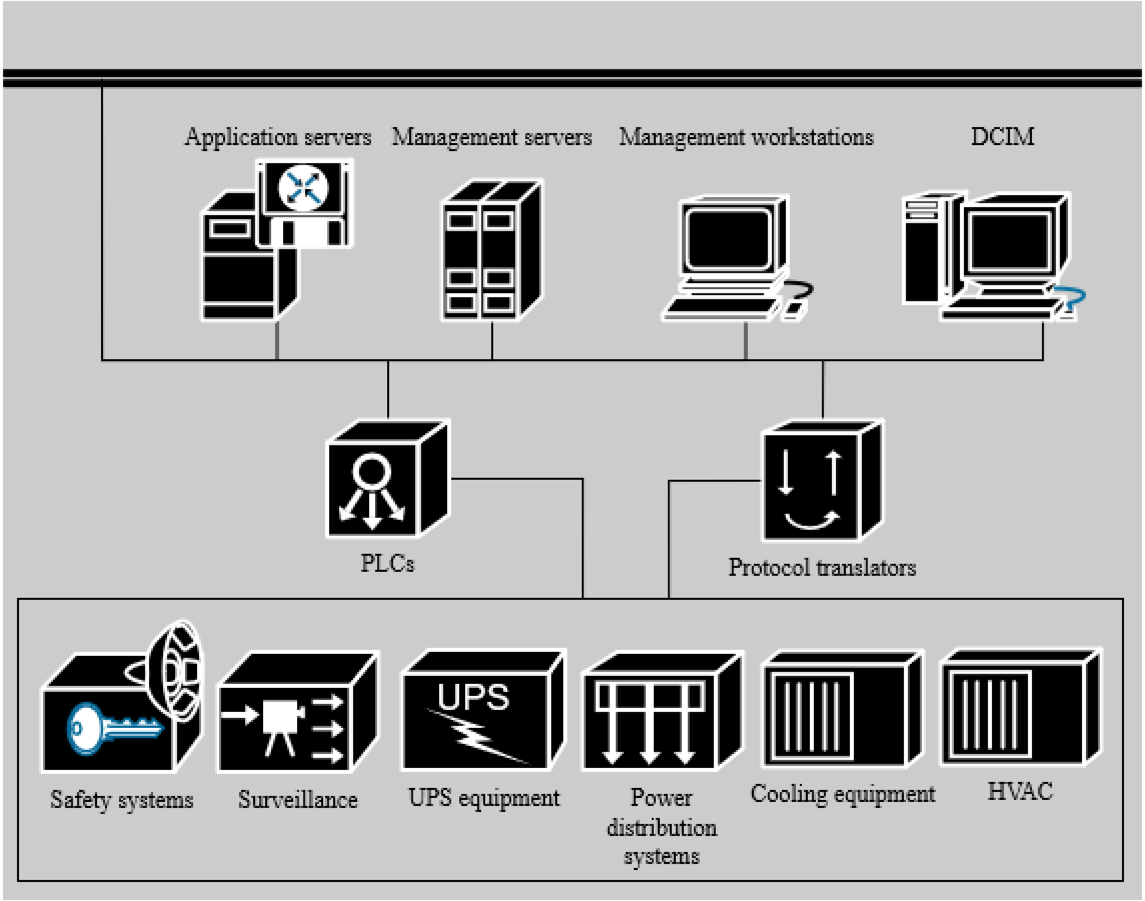

Figure 1. Generic overview of data center support infrastructure.

2.1 Data center classification levels

Data centers can be classified to different tiers depending on the amount of redundant systems in their support infrastructure. These tiers are divided into four categories (I-IV) and they define a certain level of availability and performance of these facilities [3]. This also means that the higher the tier, the more complex the supportive infrastructure grows. The differences between the tiers are summarized in Table 1.

Table 1. Differences between data center tiers [3].

	Tier I (basic site infrastructure)	Tier II (redundant capacity components site infrastructure)	Tier III (concurrently maintainable site infrastructure)	Tier IV (fault tolerant site infrastructure)
Availability (approx.)	*99.67%* *(28.8h/y downtime)*	*99.75%* *(22h/y downtime)*	*99.98%* *(1.6h/y downtime)*	*99.99%* *(0.8h/y downtime)*
Annual shutdowns (approx.)	*twice a year (total 2*12h)*	*3 every 2 years*	*not required*	*not required (1/5y)*
Active capacity Components	*N*	*N+1*	*N+1*	*N+N*
Power distribution paths	*1*	*1*	*1 active, 1 alternative*	*2 simultaneously active & independent*
Concurrently maintainable	*no*	*no*	*yes*	*yes*
Fault tolerant (single event)	*no*	*no*	*no*	*yes*

Tier I facilities are considered to be basic data centers with no redundant components making the redundancy of active capacity components required to support the computing load N, where N equals the amount of components. The requirements for this tier include a separate IT system area, dedicated cooling systems, and a UPS system and a generator for power outages. Concerning the operational availability, tier I data centers are susceptible to both planned and unexpected disturbances such as equipment replacement and -failures, and may require shutting down the facility for maintenance activities. Typically tier I data centers reach the availability of 99.67% with 28.8 hours of annual downtime caused by maintenance or support system malfunctions [3].

Tier II centers contain single redundant components for power delivery and cooling systems (N+1 redundancy). It is possible to maintain one of them without affecting the normal facility operations, but system failures concerning other components of the infrastructure can still disturb the data center operations and cause facility-wide shutdowns. Typical annual downtime for Tier II data centers is approximately 22 hours making their availability 99.75%. The downtime is caused by maintenance activities and support system faults [3].

Tier III facilities are described as concurrently maintainable sites, meaning that planned maintenance activities can be performed without affecting the data center operations. In addition to the redundant components on lower tiers, all computing equipment are dual powered. Tier III data centers are also N+1 redundant, but they can still be susceptible to unplanned disturbances caused by multiple system failures. The availability of these centers is approximated to reach 99.98% with 1.6 hours annual downtime caused by unexpected system faults [3].

Tier IV data centers are considered to be fault tolerant, so each active capacity component has a redundant component (N+N redundancy). Tier IV facilities also have two simultaneously active independent power distribution paths to make sure that severe power system faults do not affect the operations of the computing equipment. The approximated downtime for these centers is 0.8 hours per year making their availability 99.99% [3].

It is important to recognize that all data centers are not aiming to be tier IV facilities due to the higher maintenance cost brought along by the additional infrastructure. Depending on their risk model and customer base it may be financially more sensible for some operators to focus their resources to other subjects. This can be the case e.g. in geographical areas where natural disasters and disturbances causing outages are deemed highly improbable. Nevertheless the possibility for them should be taken into consideration when creating the risk model.

2.2 Building and infrastructure management

As other modern buildings often do, data centers can utilize a separate building management system (BMS) in managing the mechanical housing systems of the facility. BMS can be used to improve the energy efficiency of the building by allocating resources based on the observed or predicted demand. The system can also introduce additional capabilities or features for monitoring and controlling the building environment in a centralized manner. HVAC, lighting controllers, door and elevator systems, emergency alarms and physical access control systems (PACS) can all be integrated into the BMS enabling the communication between different components of the support infrastructure. This can be useful for adding new features to the environment. For instance, if a smoke detection system alerts the control panel of a potential fire inside a computer room, the BMS can command the air ventilation to halt while the suppression system begins to extinguish the fire. BMS can also be used as an integration point for collecting data for other systems, e.g. data center infrastructure management system (DCIM).

DCIM system is often used in data centers for centralized monitoring, asset management and creating different level reports of the data center operations. Its purpose is to collect and combine useful data from the support infrastructure and building systems such as energy consumption, cooling system temperatures and server equipment workloads and refine it to insights and visualizations for different level reports. These reports can offer accurate information of data center operations for both technical staff and business decision makers [4 p. 601-618][5]. DCIM solutions have a strong foothold in data centers and the majority of them have either implemented or are planning to implement a DCIM system for managing different areas of their infrastructure [6]. New capabilities are added to DCIM systems constantly and it is estimated that in the future DCIM solutions will utilize more advanced analysis and prediction methods and that way increase their role in the data center operations [7].

Although BMS and DCIM systems may first seem like similar systems when it comes to their aim to centralize monitoring and control, their use cases are different. BMS centralizes the management of mechanical building systems such as the environmental control system (e.g. HVAC, server room cooling and humidity) and power distribution system while DCIM is used to manage and keep records of the infrastructure assets and network infrastructure, collect data from the building systems and create reports based on the collected data. Essentially DCIM resembles more of a facility management system (FMS) which focuses on the business level asset management, for which BMS acts as an integration point or communication gateway for the mechanical building systems.

Typical BMS contains components running on three levels: 1) field level consisting of building sensors and mechanical equipment; 2) automation level consisting of protocol translators, system-specific automation controllers and programmable logic controllers (PLC) and; 3) management level consisting of the application server and operator workstations. Field level components communicate with automation level devices using serial interfaces while automation controllers and protocol translators are connected to the BMS server via Ethernet-based local TCP/IP network. Operator workstations are connected to the same network and they are used by building operators to access the web UI of the BMS running on the application server. The BMS server can provide data collected from the building systems for other parties and systems (e.g. DCIM) via REST API. Using a separate API with permission management scheme allows the building owner or facility manager to control which parties have access to different features of the BMS which is useful especially in situations when a data center provider is not the only tenant in a building complex.

The architecture of a typical DCIM resembles BMS. It can operate on multiple levels, but the main component is the DCIM software running either on a local or remote application server. The server is connected to the TCP/IP building system management network and it uses REST API to receive data and enable integration with building systems and other infrastructure components. Data center technicians can use the web UI of the system in the local network to manage assets and request automated reports. There are several DCIM systems commercially available and depending on the vendor, some may offer complete integration solutions for different systems in addition to the REST API. The reference system used in this report is based on OpenDCIM [8], an open source data center infrastructure management system. DCIM typically allows multiple tenants to use the system, so if a data center operator provides colocation service to their customers, they can also offer them access to the DCIM. A single DCIM system can also be used to centralize the management of multiple sites.

2.3 Cooling

Data centers can utilize several types of cooling system solutions. Computer Room Air Condition (CRAC) units use either water, refrigerant, glycol or air as transport fluid to move heat energy from computer room air to the outside of the data center. Instead of CRAC units, direct or indirect air cooling may be utilized when outdoor conditions are suitable for it [9]. Regardless of how the computer room air is cooled, it must be distributed inside the computer room and hot airflow directed to exhaust or back to the CRAC unit. Typical data center layout follows hot-aisle-cold-aisle principle, where aisles may be contained to minimize mixing of hot and cold air [10].

Regardless of the cooling solution used, the main purpose of it is to keep the computing equipment at safe operating temperatures. Cooling solutions are heavily affected by economic viewpoints, because portion of total electric power of data center is used to cooling can vary from 30% to 55% [11][12] Costs of cooling may also tempt data center operators to not increase cooling capabilities when necessary or let equipment run on higher temperatures [13], which may lower tolerance for cooling failures or unexpected heat load [14]. Uptime Institute reports that cooling problems have caused 13% of data center outages [15]. Failures in cooling may cause self-protective emergency shutdown of servers if dangerous temperature is reached. When considering high power density cabinets, temperature rise in case of total cooling loss (airflow and air conditioning stopped) can be very rapid, and time to emergency shutdown is expected to be seconds rather than minutes [16].

2.4 Moisture and purity control

Data centers that utilize direct air cooling solutions must take care of air moisture control and gaseous and particle impurities. Dust is not generally harmful, but it may introduce some risks for computer equipment. Accumulated dust on circuit boards may decrease cooling efficiency by obstructing airflow and dust in humid environments absorbing water promotes corrosion or ion migration. Data center computer rooms are recommended to meet ISO 8 class of cleaness and upper limit of 60% relative humidity. Computer room air is recommended to be continuously filtered with class MERV 8 filters and air entering the data center to be filtered with MERV 11 or MERV 13 filters [17].

Three types of gases may cause corrosion in electronics: Acidic gases, caustic gases, and oxidizing gases. Typically acidic gases, which include for example hydrogen sulfide, sulfur and nitrogen oxides, are most harmful to computer equipment [17][18]. Especially data centers located near sources of pollution, such as traffic, factories or power plants, have an increased chance to experience corrosion related hardware failures [19][20].

2.5 Power distribution

To reach high availability, the computing hardware requires an uninterrupted and constant supply of electricity. Lack of power can cause major outages to services provided by the data center and unsteady power supply may even damage the equipment. Power distribution architecture is the lifeline of all electrical systems in the data center, and according to Uptime Institute, 37% of data center outages in 2020 were related to disturbances in supplying power [15]. It is crucial that the electrical infrastructure can continue its operations independently even in disruptive situations. It consists of power distribution units (PDU), automatic transfer switches (ATS), uninterrupted power supplies (UPS), and generators capable of creating enough power to let the center operate, in case there is a larger disturbance in the electrical grid.

UPSs play an important role in keeping the power supply steady. They can be used to temporarily keep the computing equipment running for typically 1-15 minutes if the main power is unavailable [15]. For situations when an electrical outage lasts longer, the UPS system is paired up with a generator that can produce enough power to keep the computing equipment and cooling systems running continuously. Cooling equipment should not be run off the UPS because 1) it can often consume more power than the computing equipment, 2) on/off switching can cause output overload and UPS circuit breaker to trip and 3) the required additional capacity is not a cost-effective solution [16]. The UPS system should allow the computing equipment to operate continuously while the backup generator starts and the cooling system is able to restart in a controlled manner. This should be taken into account when estimating the capacity requirements for the UPS.

There are two main types of UPSs: static and rotary. Static UPS is the dominant type of these two and it uses the energy stored in batteries to keep the power supply steady. Rotary UPSs combine static UPS and a generator and are more suitable for high power level facilities with multiple random inrush of power. Data centers almost exclusively use static UPSs rated typically from 20kW to 500kW, but some data center facilities where multiple megawatts of UPS capacity is required can also utilize rotary UPSs [21]. Depending on the capacity and type of the UPS system, data center UPS units can be mounted to each rack [22], separate cooled cabinets in-, or outside the server room or in another space dedicated for battery cabinets. The status of the UPS can be monitored using the LCD displays integrated in the units or over a local network using vendor-provided management software or interface, third party management software or, BMS and DCIM integration.

PDUs are used to distribute the main power of the data center to the branch circuits in computing equipment cabinets via conduits hidden under a raised floor or on a cable tray suspended from the ceiling. A single PDU can provide power for a row of cabinets and they are often rated from 50kW to 500kW depending on the power consumption estimates. Larger PDUs also generate more heat and countering it with a powerful cooling system decreases the efficiency of the data center. Branch circuits are typically rated from 1.5kW to 15kW and multiple may be needed to provide enough power for each system [23]. PDUs are often in their own cabinets either separated from the computing equipment or in one end of the row. Monitoring the load and status of PDUs can be done in the room using an integrated display or in a local network using vendor-provided software, some third-party software, or BMS and DCIM integration.

ATS manages the connection to primary and secondary power sources through a single cable. It detects when a fault occurs in the main power distribution and sends a startup command to the generator. After it is producing electric power, ATS transmits commands to circuit breakers to begin using the alternative power source. Once the electrical supply of the main power line is recovered, circuit breakers are switched to using it and a stop command is sent to the generator [24]. The ATS controller typically uses Modbus to send these commands over serial line but some units can also contain a serial to Ethernet gateway to send Modbus traffic over TCP connection. This way it is also possible to integrate the ATS with the DCIM system to monitor it in a centralized manner.

2.6 Safety systems

In case of emergencies or natural disasters causing threat to the equipment such as fire or natural disasters, data centers utilize a variety of safety systems consisting of sensors, detectors, countermeasures and alarms. One of the most important safety systems is the fire suppression system which consists of heat and smoke detectors, alarms and suppression equipment. When a smoke detector detects smoke in a space or temperature rises high enough to melt an alloy inside a heat detector, an alarm signal is sent to a fire alarm control panel. The control panel first activates the sirens and sends an automated alert to the local fire department and property maintainers. Then it starts the suppression system consisting of sprinklers in the workspace and a gas extinguishing system in the computer room. In situations like these, cooperation is required from many building systems to minimize the amount of physical damages to the equipment.

2.7 Staff

Supportive infrastructure which keeps the data center core under suitable conditions is designed to work as autonomously as possible under normal situations. There is economic incentive to reduce human presence to minimum by attempting to build unstaffed “lights-out data centers” [24]. However, current data centers still rely on the existence of staff to handle maintenance situations or other regular operations with reasonable response time.

Working at a data center may require a specific set of skills depending on the task, making capable workers valuable assets and provoking regulators to classify them as “essential” [25][26]. As demand for competent staff increases, finding replacements or new recruits has been [6] and is expected to be a challenging task for data center operators in future [27][28].

3 Data center supportive infrastructure threats

Related studies have presented some concerns about the state of security of critical infrastructure [29]. Data center supportive infrastructure has similar features as other critical infrastructure, such as networked operational technology and heterogeneous set of connected devices, building automation systems, and the requirements of remote access and control. Therefore similar concerns may be raised with the supportive infrastructure of data centers than in ICS and other critical infrastructure.

Value of a data center is generated in its core. The data itself and the ability to process it on-demand are targets of high interest for adversaries. By attacking the supportive infrastructure of data centers, certain goals can be achieved. They include:

1) Disrupting data center operations
2) Gaining a foothold to supportive infrastructure in a way that allows further attacks on internal data center operations and data.

There are many possible paths that malicious actors can take to achieve these goals. An overview of these is presented in Figure 2. In this report, these are divided into three threat categories: personnel threats, physical threats, and system security threats. In addition to these three, a fourth category is presented which does not provide direct attack paths. Information leakage threats can however provide malicious actors information that they can use to perform their attacks. A brief listing of these categories is presented in Table 2.

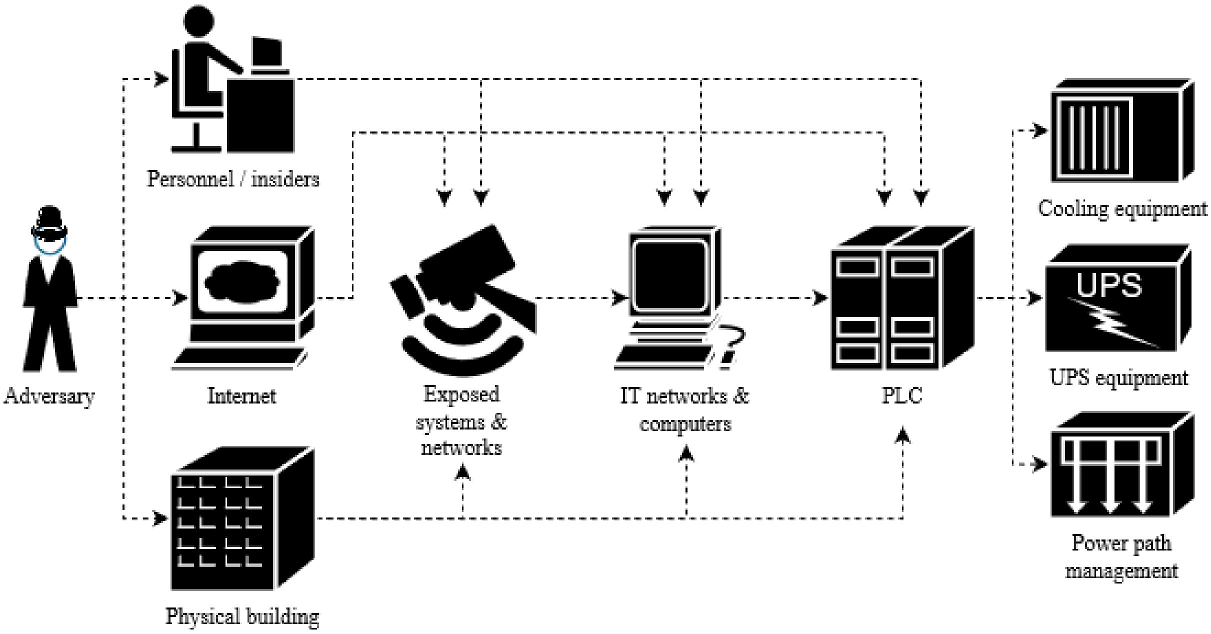

Figure 2. Paths adversaries may utilize to disturb data center operations.

This chapter discusses different types of actors that may have interest in making malicious actions against data center facilities and presents threat scenarios concerning the security of the facility and the support infrastructure systems. For describing specific weaknesses in software and hardware as threats against the systems, this report refers to Common Weakness Enumeration (CWE) [30], a comprehensive list of common software and hardware weakness types.

Table 2. Threat categories

Threat category	Examples	Potential consequences
Physical threats	*Sabotage, physical intrusion, leveraging physical access to devices and networks*	*Destroyed/tampered assets, disrupted operations, access to systems*
Personnel threats	*Phishing, insiders, social engineering attacks*	*Access credentials to systems, sabotage, physical access to systems*
Information leakage	*Espionage, reconnaissance, OSINT*	*Information helping with further attacks*
System security threats	*Vulnerable systems, public-facing applications, configuration errors, improper permission and access control*	*Disrupted operations, exposed services, compromised environment*

3.0.1 Finland and Sweden as data center locations

Finland and Sweden are considered states of high sustainability [31] and very low risk places to locate data centers [32]. Nordic countries are considered safe investment places for data centers because of high energy grid reliability, data center friendly and low-hazard climate, decent supply of qualified workforce, and political stability [33]. Disruption of data center operations by political instability, random acts of violence or unreliability of common state-wide supportive infrastructure can be considered to be low-probability events in Finland and Sweden. Finland and Sweden have been considered to have a decent state of cybersecurity in comparison with other European countries and worldwide [34].

3.0.2 Attacker profile

As data centers are considered a valuable part of the critical infrastructure, well organized and equipped criminal organizations or state-level actors may have interest in targeting them. Attacks by criminal groups usually include some mechanism for how an attack should result in the usual goal - the money. This could be done, for example, by capturing data or the critical infrastructure control systems to be used as bargaining chips, as seen recently in Colonial pipeline hack [35]. State-supported actors may have different goals than monetary gains. Motives of state-supported actors geopolitical, and attacks may have the purpose of for example to apply political pressure, be an act of cyber warfare, undermine trust in target nation cyber security or hurting the target nation economy. To achieve these goals knocking out data center systems may be enough instead of gaining the control of them.

Another type of potential threat actors are individuals who are willing to harm data center operations based on their beliefs or personal motives. Terrorist attacks and threats motivated by conspiratorial beliefs against data centers have been occurred in United States. Other types of individual actors causing threats are malicious insiders, who are willing to perform harmful acts such as sabotage or stealing valuable data, for example, because of personal grievances or financial gain.

3.1 Physical threats

Regular accidents, mistakes or simply unexpected conditions can cause serious damages, outages or accidental chain reactions leading to them. Fires [36-44], unexpected trigger of fire exhaust system [45], triggering of fire exhaustion system causing damages [46-48], overheating due to outside temperature and different HVAC failures or other mistakes [49-54] have potential to cause serious data center outages. Uptime Institute reports that 50% of data center outages in 2020 were related to power or cooling failures [15]. Skilled saboteur who gains physical access to critical supporting systems, such as power supply or cooling, has huge potential to wreak havoc in data centers.

Any other device and structure that is physically accessible is a potential target for sabotage, tampering or weakening. Pipes, wires, cameras, locks, sensors, computers, and any other device or structure which serves some purpose may be an interesting target. Accidents have been caused frequently by wild animals [55], so it should be expected that intentional sabotage could yield similar results. Sabotage may also be part of a larger attack plan. In Finland, for example, a company headquarters was targeted by an attacker who sabotaged the camera over the entry point and then came back later to execute the intrusion, all the way to the server room [56].

Attackers also may want to use more blunt attack methods to permanently knock out data center [57][58] or be willing to forcibly enter or utilize social engineering techniques to data center premises in order to steal valuable assets [59][60]. Destructive attacks or attack attempts against data centers are not publicly known in Sweden or Finland, but sabotages of network infrastructure have occurred in Sweden and suspected sabotage in Finland [61].

In addition to simply breaking anything that is physically accessible, gaining physical access to networks or devices will open up new possibilities to attackers. Possibilities could include for example connecting unwanted devices to internal networks, using accessible workstations or other endpoints to perform actions that could not have been performed remotely. If data center supportive infrastructure or other devices communicate via wireless network, physical close proximity may allow listening network or attempting to launch attacks targeting wireless network weaknesses.

3.2 Personnel related threats

Economical and practical incentives exist to cut down the amount of human work needed in data centers, but data centers and supportive infrastructure still require human effort to keep data centers running.

Insider threat is the possibility that a person, who has authorized access to or critical knowledge about organizations systems, will cause intentional or unintentional harm to organization [62]. Insider threats may be malicious like blunt sabotage [63][64][65] or theft of valuable assets, but insider threats can also be caused unintentionally by human errors or being victim to social engineering attacks causing trusted personnel to perform unwanted actions or reveal confidential information.

Malicious insiders may have a variety of motives such as money, loyalty to other entities or revenge and a variety of forms, such as IT sabotage, theft of intellectual property of assets, fraud or espionage. Most common motive for sabotaging IT assets was revenge and common traits of perpetrators are being technically skilled and having privileged access to the system [66]. As supportive infrastructure contains a variety of critical electrical and physical equipment, malicious insiders with skill and motive to sabotage the data center may have a plethora of opportunities to do that.

Human-related errors are a significant source of problems in data centers. Uptime Institute claims that the yearly average of data center incidents caused by human error is 63% [15]. They also claim that 79% of data centers have had human error related outages during the last 3 years [67]. These include all human related problems, such as inadequate maintenance, bad management and incorrect staff procedures.

3.3 Information leaks

Variety of information about data centers could be found openly online. For example, in online discussions, personnel social media profiles, informational organization web pages or satellite images. Information can also be acquired from more uncommon sources, such as dumpsters. Data center personnel may be followed physically or online in the purpose of collecting information passively or actively by utilizing social engineering techniques. Unintended information leaks can happen in unforeseen and unexpected forms. Lights on windows, taken parking spaces or activity of wireless networks could be used to determine if a data center site is occupied and by who. Carelessness with handling of the information is claimed to be surprisingly common, such as leaving a medium containing important data in cars [68]. Utilizing and combining a variety of information sources could result in emerging knowledge about personnel or organizational layout, data center subcontractors, layout or deployed supportive infrastructure. One example of unintended information leaks happening is fitness apps revealing military base location and personnel identities [69][70]. Even innocuous-looking information could be acquired and creatively combined by the attacker to plan later stages of the attack [68].

3.4 System security threats

Traditionally building automation environments have consisted mainly of mechanical appliances with serial communication interfaces, automation controllers and PLCs, and the centralized management system that is used with the operator workstation via IP network. Due to the development and adoption of new embedded systems, sensors, and communication protocols, modern building automation environments can however include a heterogeneous mix of devices ranging from legacy equipment to wireless sensor networks (WSN). This increases the complexity of the system and can cause unexpected behaviour which can lead to additional vulnerabilities [72]. In addition to the increased complexity of these environments, there are several issues concerning the security of these systems. The operational technology and automation system domain is considered to lag behind when it comes to improvement of security practices because of the 1) “security through obscurity” mindset, 2) the thought that there are no threats toward automation systems because they are designed to be used in isolated environments, and 3) security solution by itself does not provide any easily calculable or convertible monetary value [73].

3.4.1 Software vulnerabilities and remote access threats

Buildings are designed with a long lifespan in mind, and one of the main characteristics of building systems and the embedded computers in them is that their lifespan is longer than with typical computer systems. This can introduce challenges when it comes to maintaining and supporting the system throughout that time. The different technologies used in the system can become obsolete causing issues in the future similar to the current situation with legacy systems [72]. It is also possible that new vulnerabilities are discovered during the time period when the system is in active use. For situations like this, the equipment should be updatable or upgradeable [74].

Patching the newly discovered vulnerabilities is important especially with systems that offer some type of accessibility from systems connected to external networks. Vulnerable public-facing systems can provide a potential entry point to the internal network and a study by Forescout found out that almost 40% of publicly found BAS devices (protocol gateways, HVAC PLCs and access control PLCs) and over 90% of publicly found IP cameras had some previously known or unknown vulnerabilities [75]. Keeping the systems updated may help counter known vulnerabilities, but it does not necessarily mean that the system is secure. If a vendor is unaware of a vulnerability in their equipment, they are also not aware of the need to patch it. As the report shows, some previously unknown vulnerabilities were also identified in publicly reachable systems including XSS (CWE-725), path traversal (CWE-23) and arbitrary file deletion (CWE-73) vulnerabilities in access control PLC, XSS (CWE-725) and authentication bypass (CWE-1211) in HVAC PLC and XSS (CWE-725) vulnerability in protocol gateway. These vulnerabilities presented in the report are present in the management interfaces and can be exploited to disrupt the system, inject malicious content in the management application, and gain a foothold in the system. This foothold could then be used to access other systems within the same network. DCIM may also provide interfaces for monitoring and controlling the infrastructure systems remotely. Vulnerabilities in them and the gateways and firewalls between these systems, and the public internet may put the whole datacenter at enormous risk.

DCIM systems can support multi-tenant configurations, and especially in colocation data centers it can be useful to have a single system that allows tenants to access the monitoring capabilities concerning their own equipment. This increases the significance of securely implemented permissions, privileges and access controls (CWE-264). Even if the DCIM is used only in the local environment with no remote access possibility, the security of the system is an issue that should be taken into consideration.

Mismanaged credentials and inadequate access control and permission schemes in systems connected to operational equipment can lead to very serious consequences. Housing equipment may allow the vendor to perform some type of remote monitoring or maintenance on it. This would require the vendor to have valid credentials and a method for accessing the system remotely. In the report [75], they discovered that the equipment contained hardcoded credentials (CWE-798) for vendors to use when they are performing maintenance. If the valid credentials of systems, even unrelated ones, end up in the hands of malicious actors (e.g., by password reuse or compromise of third parties), they may be able to use those to gain the initial foothold for their attacks [35][76].

Data center networks or supportive infrastructure may interact with various devices, such as sensors, smart displays, employee laptops, and phones. Any of these devices could contain vulnerabilities which may cause additional risks to the data center infrastructure. Risks may come from unexpected directions, like smart light bulbs leaking wireless network credentials [77]. Failures in internal networks or devices can cause unexpected consequences and for example during Facebook outage 2021, a failure in the internal network prevented access to the entire building and server areas which hindered incident assessment and repair attempts [78].

3.4.2 Configuration errors

Vulnerabilities or weaknesses of the system environment are not always caused by errors in software or hardware design or implementation. The vendors may perform thorough auditing procedures on their equipment before distribution but the system may still end up being misused in illegitimate actions. Configuration vulnerabilities may be generated when a system is installed, updated or used in such a way that does not follow the procedures defined by the vendor. This can cause equipment that should be run in an isolated network, such as PLC, be accessible from the internet. For instance, a DCIM web interface intended to be used by data center personnel in a local management network is also connected to a remotely accessible network that provides vendors access to a maintenance interface of their equipment. This may lead to unauthorized access to business data and even compromised systems if combined with software vulnerabilities.

4 Data center supportive infrastructure security measures

As threats towards all critical infrastructure may take various forms, similarly threats toward data center supportive infrastructure can vary a lot. Specialists of different fields should carefully compose a multi-disciplinary set of countermeasures to achieve desired security goals.

Multiple different security measures have been suggested to protect the critical infrastructure. In this chapter, security measures connected to the securing of the supportive infrastructure of the data center are discussed. The presented security measures include technical and administrative control mechanisms against intentional hostile actions. It also contains measures against common risks such as accidents and emergencies, because the consequences in both cause similar consequences. An overview of how some of the presented countermeasures respond to threat categories can be seen in Table 3.

It should be noted that sensibility, cost-effectiveness, and practicality of any security measure should be carefully considered before deployment case-by-case. As the budget for security is not unlimited, any countermeasure should also be weighted against potential threat and importance of protected assets.

Table 3. Threat categories and related prevention measures

Threat category	Examples of countermeasures
Physical threats	*Structural strength, layout design, physical access control, intrusion detection*
Personnel threats	*Countering social engineering, procedures for critical assets*
Information leakage	*Information control procedures, personnel awareness*
System security threats	*Update procedures, permission and access control, network security measures, system auditing*

4.1 Physical security measures

Backbone of security of assets is the physical security of them. Malicious physical access to protected assets may efficiently circumvent security and safety measures that are applied to protect them [79]. Building physical security of a data center requires a wide spectrum of professional knowledge to be utilized, including, for example, topics like building construction and design, physical alarm and access control systems and administrative security controls. All physical security measures can not be sensibly applied to data centers. Small colocation data centers and dedicated data center sites have very different possibilities to physically isolate risks because of the existing infrastructure and layout of them. Every physical measure must be balanced with the importance of protected assets, expected threats, and economical resources [71].

4.1.1 Strong and resilient structures

Structurally sufficiently strong walls, doors, gates, windows, and fences. Material and strength of structures should be picked based on importance of what they are supposedly protecting and form of expected physical threats. In addition to having a purpose to slow down or thwart potential intrusion into the data center, fire, flood, and other natural disaster resilience of structures and building solutions should be considered [20][71][80].

4.1.2 Physical surveillance and environmental monitoring systems

Physical intrusion or unusual human activity may not be preventable, but surveillance systems can make it detectable. CCTV solutions and motion detectors may reveal the unwanted human presence and record any visible actions. Other sensors, such as door contact sensors, window break sensors, and vibration sensors, may detect that some unusual activity is happening at a monitored target. Monitoring systems should also consider other environmental hazard monitoring sensors, such as humidity, smoke, leak, heat, and air contaminant sensors suitable to trigger alerts and countermeasure actions [81].

4.1.3 Other structural design considerations

Multiple different security measures may be implemented to hinder attempts of physical intrusion. Concerning the surroundings, there should be a clearly defined security perimeter around the facility and measures to prevent unauthorized vehicle entry. The building itself should have only a limited number of entry points. Fewer entry points makes it simpler to implement adequate controls to all entrances and exits, such as surveillance and anti-tailgating doors. Exit and maintenance doors should be openable only from inside and they should be installed so that the door hinges can not be tampered with from the outside. The same can be applied to windows and there should be no windows that would allow visibility to critical spaces of the building. Cabling and piping should also be hidden and not accessible from unnecessary places, such as corridors. In equipment and maintenance rooms, sufficient quality of mechanical locks, cabinets, and cages should be used to protect the critical equipment from tampering [71][80].

4.1.4 Physical access control to secure areas

Data center may consist of areas that have different purposes and importance, such as a computer room, reception area, delivery area, HVAC or UPS equipment areas.

Defense in depth approach may be considered when physical security of critical spaces or equipment of a data center is considered. For example, sensitive equipment itself may be protected by a cage or cabinet, which is located in the room with restricted access. Room cannot be accessed without entering the building and the building itself may also be surrounded by a security fence as outer perimeter. Idea of multiple layers of security is that different access controls can be applied to different importance of areas and inner areas are also enclosed by outer perimeter security controls.

If an attacker breaches a single outer security perimeter, it does not result in access to more sensitive inner areas [80].

Access to areas and equipment should be limited by identity and purpose. For example, visitors should not have access to any other places than visitor areas, office workers should not have access to HVAC equipment rooms, or warehouse workers should not have access to managers' offices. Access to areas may also be given as a temporary basis only when needed. For example, visitors and contractors may only need temporary access to premises. Access logs should be collected and the list of access rights of different areas personnel should be strictly maintained [71][80].

Controlling physical access usually includes checking the identity of the person asking for access. Identification methods may include physical tokens (keys, keycards), abstract tokens (passwords, keycodes) or biometrics (fingerprints, iris). All methods have upsides and downsides (such as possibility to lose/forget tokens or reliability of identification), so careful planning should be done before deploying different access controls. Also combining multiple different methods of identification for accessing more sensitive areas is possible to strengthen the security [80].

4.1.5 Other physical security measures

Multiple different security measures have been suggested to improve physical security of data centers by reducing risks of unknown variables or to make social engineering attempts more difficult. For example, visitors could be allowed only pre-planned visits, required to present government-issued ID, or be escorted on data center premises. Other practices may, for example, require all personnel to keep identification badges visible or reject unexpected deliveries arriving on data center premises. Regular patrols and inspections may be conducted to detect any signs of physical tampering on structures or devices [71]. No single measure or even combination of them can assert perfect security, but carefully thought out and followed security practices will certainly make social engineering attempts or intrusion more difficult or easier to detect.

4.2 System security measures

As previously mentioned, traditionally operational technology has lagged behind when it comes to improving the security of the systems [72]. As the use of more feature-rich equipment and non-proprietary technologies becomes more common in the form of sensor networks and building systems utilizing common communication protocols and open standards, the existing technical security solutions become more suitable to be used in cooperation with them. The following paragraphs describe some examples of how to it is possible to prevent and prepare for threats concerning the support infrastructure systems

4.2.1 Network security

One of the fundamental network security practices is network segmentation. Dividing networks into multiple segments allows the administrator to control the traffic between different subnets with predefined policies. In traditional automation network environments, the systems have used physically isolated air-gapped networks without possibility to access them remotely, but this is not the case anymore as the use of interconnected systems has become the new standard [82]. One of the most common models for designing a network architecture is the Purdue Reference Model [83] presented in Figure 3, which divides the network to different levels separated with firewalls. Firewalls are used to restrict network access to only the necessary devices based on a predefined policy. The rules in this policy can, e.g., allow only outbound connections, block the use of specific ports and restrict access to a network based on unique device identifiers, such as their IP or MAC addresses. There are methods for bypassing some if not all of these rules (e.g. IP spoofing), so defining a comprehensive firewall policy is important. For defining the policy, the zero trust security model, where network clients should only have permissions they require to complete their tasks, offers a good baseline.

Due to the complexity of modern automation environments and the operational protocols used, some segmentation technologies and network security controls may not be applicable [84]. Firewalls and intrusion detection systems used in information technology networks may not be suitable for operational network traffic. Therefore, additional zoning between information technology networks and operational technology networks may be required. Some studies also recognize the lack of fully-functional IDS and IPS solutions concerning the application and network layer security in operational networks [85][86], but although there may be some concerns of the applicability of existing systems, they can still be used for detecting malicious traffic and flagging anomalies in the management network [87].

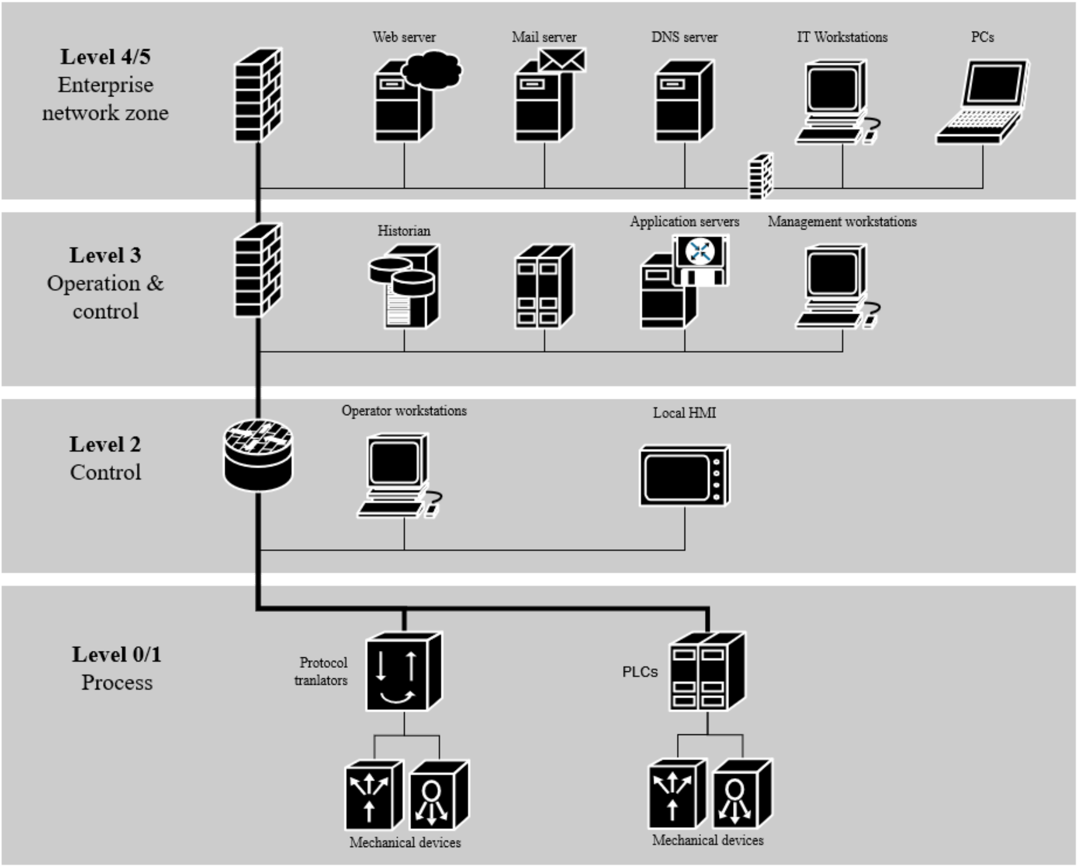

Figure 3. Purdue Reference Model.

4.2.2 Update policies

Since the lifespan of support infrastructure systems is relatively long, it should be possible to update the firmware and other software components of the equipment. Major vendors often publish security advisories at specific intervals which describe security issues discovered in their equipment and the corrective actions required to keep them secure [88][89]. The advisory typically contains a Common Vulnerability and Exposure (CVE) identifier that can be used to look for additional information about the vulnerability, description of the vulnerability and its severity and list of all the products and versions the vulnerability affects. Typical update process starts when a vendor sends a security advisory concerning equipment used in the receiving facility. After the legitimacy of the information is confirmed, the updated firmware is requested from a reliable source, meaning usually downloading it from the software distribution portal in the vendor's website. The integrity of the update should be confirmed by calculating a hash value (checksum) of it and comparing it to the one provided by the vendor in the download portal or possibly even in the security advisory. If the checksums do not match, someone may have maliciously tampered with the update and it should not be installed. Since the system should be operated in a separate network, the downloaded firmware is then transferred to the management or maintenance system with removable media. These devices should also be inspected for preventing malware spreading across air-gapped networks [87].

Some major vendors can also offer on-site support where they handle the maintenance, equipment inspections and firmware updates. This service comes at an additional cost, and some data centers may prefer to perform maintenance in-house. Whichever the case, the update policy should be defined for both routine maintenance and unexpected issues.

In addition to the facility systems, the update policy should cover all systems used in the connected networks. This is important especially for devices that do not operate in isolated networks. Workstations and other equipment may also contain vulnerabilities that malicious actors can leverage.

4.2.3 Auditing systems

Concerning the vulnerability management procedures, system audits are a more proactive approach. The term covers activities from network and vulnerability scanning in hopes of discovering weaknesses in the environment to certifying the facility by performing a full auditing based on some criteria or standard. Several criteria exist concerning the security of system environments, such as ISO/IEC 27000 family of standards concerning the organizational and process level and the EN 50600 standard which focuses on the physical security of data center facilities specifically. System audits can help to assess what risks and threats are most relevant to the audited environment and detect technical vulnerabilities and too permissive security setups that would otherwise be noticed after security incidents have occurred [90].

The main objectives of security audits are to investigate existing security policies, procedures and security controls on multiple levels, identify system vulnerabilities, and provide recommendations on how identified issues can be corrected. Depending on the scope of the audit, there can be many methods of how this can be achieved. In network security audits, the proposed [91] steps include 1) scanning the infrastructure, 2) auditing logs and system reports, 3) assessing the existing security architecture, 4) verifying that adequate security controls are used, 5) inspecting the workflow, 6) investigating the security policies of the organization, and 7) assess the risks and threats against the systems. This should not be considered as a complete list of required steps however as it may not cover all aspects, but more of a suggestion for planning system audit activities. Many commercial operators provide certification services based on existing comprehensive standards or criteria, and when performed thoroughly, security audits can be an effective measure in preventing security incidents.

4.3 Administrative security measures

Humans are often considered as the weakest link of security and their actions may lead to vulnerabilities. In human behaviour, there are four areas of special concern that can be identified [92]:

1. access control and use of credentials
2. failures in following procedures
3. configuration errors in network components
4. poor configuration management

This section presents some measures organizations can take to prevent human-originated threats concerning these issues.

4.3.1 Permissions, privilege, and access control

Access and privilege control in networks and systems should be carefully managed. Similar to the zero trust model mentioned in 4.2.1. concerning the network restrictions, access to infrastructure systems should also be based on the least-privilege principle and role-based permits. Minimizing the access levels for each role and for each system can reduce the attack surface and lower the security risks [93]. A comprehensive least privilege -based system access control policy should contain user-specific accounts to systems necessary for them to complete their duties, designated user roles and groups and credential management policy. Using separate accounts enables more control over user-specific permissions and increases the accountability aspect in the environment since actions can be traced to corresponding accounts making it also an effective measure against insider threats [94]. Managing user-specific accounts in large organizations may be challenging, so role or group-based policies are often a more suitable access control strategy for managing the permissions.

Credential management policy defines how users are authenticated. It should contain the requirements for strong passwords. Although some concerns about the security of using passwords have been presented [95], the user-password combination is still the prominent authentication method as of 2021. Some systems may allow the use of biometric or multi-factor authentication methods, but usually they require a user-created password or passphrase as well. Some common requirements for secure passwords policy include 1) minimum length requirement, 2) password expiration and renewal, 3) using both upper and lower case letters, 4) use of numerals, and 5) using punctuation symbols and special characters [96]. There is however some controversy on what should be considered an effective requirement, and for example password expiration is estimated to have only a minimal security effect [97]. Organizations should enforce the use of multi-factor authentication and application-specific passwords [98] in all applicable systems. Third parties may also have access to data center networks, systems, or interfaces of data center supportive infrastructure, and they should follow the same policies and caution as any other party holding credentials.

4.3.2 Security education and awareness

Since humans are considered the weakest link in security, increasing the skill level and knowledge of employees and individuals could be a sensible method for countering threats. The issues listed in 4.3. can lead to harmful consequences, and the main method for responding to them is security education. Security training can improve the awareness of employees on how their actions can counter the security threats. Some practical examples of this include motivating them to create stronger passwords and use them more safely, improve their own awareness on security-related issues, and follow the security-related procedures more carefully [99]. Raised awareness can also help employees to recognize social engineering attempts [100].

In addition to security training, safety training is important for emergency situations. Disasters can occur suddenly and they can affect human lives, so it is important to rehearse different scenarios beforehand so personnel are able to act accordingly. In Finland, organizations are obligated by law to create rescue plans in case of emergencies, and they should be reviewed and practiced with the personnel.

4.3.3 Controlling publicly available information

Limiting openly available or easily gatherable information is most likely not going to thwart dedicated attackers but low-hanging fruits still should not be offered to them. Variety of suggested security measures exist to make information collection harder and increase resistance to social engineering attacks. Communication procedures may, for example, limit certain types of critical information (such as credentials) given via phone or email, require verification of identity before discussion or limit phone or email discussions in spaces where risk to being eavesdropped or shoulder-surfed is obvious. Other information control procedures may control how digital media or physical documents are safely disposed of or how organizations or members of organizations appear online. Staff should understand the possible risks of discussing too openly about internal matters of organization such as business partners, customers, running projects, or other important assets. Variety of measures exists, and it is important to think from the viewpoint of what are assets that need to be protected and what kind of information leaking would cause risks to those assets [68].

4.3.4 Preparing for disruptions

When enough time passes, even low-probability incidents may happen with the supportive infrastructure. Natural conditions and disasters, physical and cyber attacks by malicious actors, or just unlucky equipment failures may cause data center infrastructure to discontinue support of core operations of the data center. Regardless of the reason for failure, redundancy of support infrastructure may allow continuing support to core operations of the data center and adequate preparations for disastrous situations may limit or prevent damages. The redundant communication channels become vital in situations where external help is needed, and any connections to emergency services should be doubled. For example, fire alarms should be sent using several communication mediums like via wired connection and cellular network.

Multiple suggestions for testing and planning for disasters have been presented: Testing regularly that redundant support systems (such as UPS and generators) are working as expected, testing that emergency systems do not have unexpected consequences (such as fire extinguishers causing unexpected damages when triggered), or verifying recovery capabilities (for example that emergency shutdowns or restarting/replacing/reinstalling systems will be possible and achievable in wanted timeframe). Relevant emergency situation contacts inside the organization, state actors/regulators and other vendors/organizations potentially providing additional resources should be listed. Response procedures and roles during incidents should be planned and trained. For example, responses could be planned for detected ongoing or previously happened unauthorized physical access to critical spaces or network intrusion, suspected compromise of access credentials, or situations when some systems are known to be compromised [4 p. 639-666][101].

4.3.5 Human security

Humans are often considered the weakest link of the security of different systems. Similarly from the perspective of data centers, a significant amount of accidents are human-related and human interactions with systems may open possibilities for human-targeted attacks. On the other hand, the human element can be the only and last line of defense when unexpected situations manifest themselves. Vigilant and skilled staff is capable of responding to unexpected problems or security situations with human mobility, flexibility, or creativity like no other non-human security measure would. Staff should be thoroughly trained in both technical skill and resistance against social engineering. Procedures for problem situations should be designed and practiced regularly [80].

Combating malicious insider threats is difficult, and some of the risks may be impossible to fully control. Some mitigations to malicious insider threat have been presented: Access to assets should be granted with least-privilege principle and managed strictly, detecting events that do not fit into expected patterns, establishing procedures to diminish emotional disturbances of negative work-related experiences, procedures for reporting concerns or incidents, training to raise awareness of insider threat, separation of duties, requiring two persons confirmation to access/modify critical assets, regular monitoring and auditing of events, designing measures to ensure survivability/recoverability of critical assets, or performing background checks [66][71][102][103].

4.4 Examples of related resources for data center supportive infrastructure security

Table 4 presents additional resources to be considered when planning data center supportive infrastructure security. This list is not exhaustive as a large number of topics would fit under the scope of data center supportive infrastructure security.

Table 4. Related resources for data center supportive infrastructure security

Resource	Related topics
ISO/IEC 27001 Annex A.6	Security roles, segregation of duties, contact with relevant parties
ISO/IEC 27001 Annex A.7	Human resource
ISO/IEC 27001 Annex A.8	Asset and information management
ISO/IEC 27001 Annex A.9	Access control to systems
ISO/IEC 27001 Annex A.11	Physical security
ISO/IEC 27001 Annex A.12	Operational security procedures, backups, auditing
ISO/IEC 27001 Annex A.13	Network security
ISO/IEC 27001 Annex A.14	Remote interfaces security
ISO/IEC 27001 Annex A.16	Incident management
ISO/IEC 27001 Annex A.17	Disruption preparation
ISO/IEC 27033	Network security
ISO/IEC 27035	Security incident management
ISO/IEC 27039	Intrusion detection and prevention systems
ISO/IEC TS 22237-6	Data center infrastructure security
ISO/IEC TS 22237-7	Data center management and operations
ISA/IEC 62443	Building automation systems
NIST Special Publication 800-82	Securing operational technology
NIST Special Publication 800-184	Security incident recovery

5 Discussion

Majority of data center outages and incidents are caused by different types of accidents, mistakes, or natural conditions, so higher resources used towards preventing those than the threat of a malicious human attacker is an understandable choice. Improving resilience against non-intentional risks by improving data center supportive infrastructure redundancy, reliability, and recovery capabilities or procedures for performing operations, can be seen to also contribute to the security of infrastructure against certain types of human-made threats. All protective measures planned are always weighted against available resources so every possible measure may not be sensible to implement, even if threat is known to exist.

Threat actors and their motivations should be considered when defense of data center supportive infrastructure is planned. Common cyber threats to different organizations are professional criminal gangs who have financial gain as their goal. Organizations operating critical ICS have become very interesting targets for ransomware attackers [104]. During Colonial pipeline hack, intruders installed ransomware to computers, but critical operational technology remained unharmed [35], which implies that attacking operational technology was not deemed necessary to make successful extortion. Growing concern has been expressed about operational technology being targeted by destructive and ransomware attacks [105] so in the future there is a possibility of rising interest to attempt ransomware attacks directly on operational technology devices and networks instead of just IT assets. These aspects should be taken care accordingly when security data center supportive infrastructure devices and IT assets are considered.

When considering state-level threat actors, unlike criminal actors, the purpose of monetary gain may not be the sole driver of the attack. If data centers will be considered to have major significance to the smooth running of daily living or operation of critical organizations, it should be expected that data centers will be considered as suitable targets for cyber or physical attacks to disrupt the functioning of the society. Knocking out the supportive infrastructure of the data center may not allow stealing or destroying the data, but it effectively makes the data center unavailable for everyone, possibly for a long time. State-level actors may have advanced capabilities to perform for example hardware tampering [106]. With enough resources and time, it could be possible to tamper critical systems such as building automation or other equipment even at the construction time of the data center.

Building automation systems and devices used in data centers contain some security concerns. They may not be designed with physical or cyber security as priority, they may be more difficult to update than IT devices, and some of the systems used in current data centers are obsolete by the standards of today. When looking through a list of disclosed vulnerabilities [107] concerning building automation systems, there seem to be patterns of reporting multiple vulnerabilities at the same time. This could be interpreted that they are only reported at specific intervals when security advisories are sent to customers, but it could also suggest that when these automation systems are tested, a range of vulnerabilities are discovered. Furthermore, most of the vulnerabilities are discovered from a specific system which would support the latter statement. This raises the question of how other automation systems are tested and what is their status concerning system security. It may also be the case that vendors are evaluating the security of their products and just fixing them silently afterwards. Nevertheless, the list of vulnerabilities shows that further investigation on building automation security is needed.

Although it seems that the amount of data centers has decreased [108], the amount of hyperscale data centers has increased [109]. This suggests that the trend is moving towards large facilities. Majority of data center operators however consider the demand for edge data centers to increase [67], which suggests that we should see new facilities being built in the future. This distributed model of hyperscale centers and smaller edge data centers may offer improved performance for customers who want their data centers to be located geographically closer to them, but it may also have some impact on the overall state of security in the industry. Although focusing operations to specific locations could mean that there is only a single environment that needs to be managed and secured, it also offers malicious actors the possibility to disrupt operations by targeting that single facility. Managing the support infrastructure in large facilities may be challenging and it requires a comprehensive infrastructure design from data center operators and the use of scalable security measures. Whatever the case may be, only time will tell how these issues are taken into consideration concerning the decisions about the scale of future data centers and their geographically distributed locations.

Demand for skilled workforce in data centers seems to be increasing. Incentive to minimize the amount of needed human work and presence in data centers is obvious from economical and security perspectives, but due to the complexity of the environment human workforce may still be required for some time in the future. As the majority of data center incidents are tracked back to the failures of humans (bad management, bad procedures, understaffing and mistakes), acquiring an appropriate amount of skilled workforce and thoroughly training them should be considered as an important outage-prevention measure.

6 Conclusions

Support system disruptions have the power to halt the operations of the whole data center. Although there are several approaches that malicious actors can take to do so purposely, there are also several countermeasures that data center operators can implement to protect their environment. These measures are not necessarily specific to certain threats, and some may have the capability to affect the security on multiple domains. For example, proper security training can help to prevent human-originated threats concerning access to physical assets by raising the security awareness of the employees, or mismanaged systems by underlining the importance of following defined procedures when performing maintenance or installing operational equipment. Security training is also an effective method to prepare against personnel-related threats, and safety training and rehearsals can be used to confirm that personnel can act accordingly during emergencies.

The physical security of the data center facility provides the backbone for safe and secure operations in the facility. Measures concerning the resilient structure of the data center, surveillance capabilities and controlling the access to assets should be enforced to keep the physical environment secure and safe.

Although the security of the support infrastructure systems is considered to lag behind, studies aiming to improve the situation by applying the security measures familiar from IT environments exist. Due to the long lifespan of automation systems, it may take time to see some of the results implemented in environments so it is important to use the current systems in a way that they are meant to. Configuration errors may cause unwanted interfaces to be exposed to public networks which may lead to incidents caused by remote attackers. Following the procedures defined by software or equipment vendors can help to avoid these configuration-caused vulnerabilities.

Organizations should consider what their corrective actions contain regarding vulnerabilities discovered in their systems. The long lifespan of automation systems means that there is a possibility that the technology may become obsolete during the active use period of the system, so it is important that a plan for updating software or hardware components of these systems exists.

Security audits based on publicly recognized criteria is a good method for confirming that the state of the data center is as secure as it is considered to be. There are several standards that can be used to certify the facility from both administrative and technical aspects, and using external parties to vet the facility can offer a neutral perspective in its state. Internal audits can also be an effective measure in detecting configuration vulnerabilities in networks.

Data center operators should review their risk model with these observations in mind and perform corrective actions if required. The reviewed and composed support infrastructure security observations are also used to improve the current security study portfolio in University of Oulu. The gathered knowledge is used to define an additional workshop that can be used as laboratory work in a computer security -related course. The workshop focuses on support infrastructure and building automation security and it contains operating and investigating hostile actions taken in a live environment built on top of a cyber range platform. The workshop can give students additional skills and knowledge of security threats specific to the automation domain and its goal is to provide skilled graduates for the industry operators.

7 References

[1] JLL. (2021). Data Center Outlook 2021. JLL.

[2] Hern, A. (2020, March 13). Covid-19 could cause permanent shift towards home working. The Guardian. https://www.theguardian.com/technology/2020/mar/13/covid-19-could-cause-permanent-shift-towards-home-working

[3] Turner IV, W. P., PE, J., Seader, P. E., & Brill, K. J. (2006). Tier classification define site infrastructure performance. Uptime Institute

[4] Geng, H. (2014). Data center handbook. John Wiley & Sons.

[5] Cole, D. (2012). Data center infrastructure management. *Data Center Knowledge*.

[6] Kleyman, B., Gillooly, B., & Letourneau, K. (2021). The 2021 State of the Data Center Report. AFCOM. https://www.datacenterworld.com/sites/default/files/AFCOM_State%20of%20the%20Data%20Center_FINAL_2021_5-10-21.pdf

[7] Healey, J. (2020). DCIM 101: What is Data Center Infrastructure Management?. Schneider Electric. https://blog.se.com/datacenter/dcim/2020/02/06/dcim-101-what-is-data-center-infrastructure-management/

[8] OpenDCIM - Open Source Data Center Infrastructure Management. (n.d.). OpenDCIM. https://www.opendcim.org/

[9] Evans, T. (2012). The different technologies for cooling data centers. APC white paper, 59.

[10] Rasmussen, N. (2012). The Different Types of Air Distribution for IT Environments. Schneider electric, APC cooling.

[11] Song, Z., Zhang, X., & Eriksson, C. (2015). Data center energy and cost saving evaluation. Energy Procedia, 75, 1255-1260.

[12] Cho, J., Lim, T., & Kim, B. S. (2012). Viability of datacenter cooling systems for energy efficiency in temperate or subtropical regions: Case study. Energy and buildings, 55, 189-197.

[13] El-Sayed, N., Stefanovici, I. A., Amvrosiadis, G., Hwang, A. A., & Schroeder, B. (2012, June). Temperature management in data centers: Why some (might) like it hot. In Proceedings of the 12th ACM SIGMETRICS/PERFORMANCE joint international conference on Measurement and Modeling of Computer Systems (pp. 163-174).

[14] Gao, X., Xu, Z., Wang, H., Li, L., & Wang, X. (2018, February). Reduced Cooling Redundancy: A New Security Vulnerability in a Hot Data Center. In NDSS.

[15] Lawrence, A. (2021) Annual outage analysis 2021: The causes and impacts of data center outages. Uptime Institute Intelligence.

[16] Active Power. Data Center Thermal Runaway. 2007. Active Power. https://powertechniquesinc.com/wp-content/uploads/2015/08/Active-Power-WP-105-Data-Center-Thermal-Runaway.pdf

[17] American Society of Heating, Refrigerating and Air-Conditioning Engineers. (2011). 2011 Gaseous and Particulate Contamination Guidelines For Data Centers. American Society of Heating, Refrigerating and Air-Conditioning Engineers. https://www.ashrae.org/File%20Library/Technical%20Resources/Publication%20Errata%20and%20Updates/2011-Gaseous-and-Particulate-Guidelines.pdf

[18] Muller, C., & ARENT, C. (2015). Air Quality in Data Centers: Humans vs. the Machines.

[19] Heslin, K. (2014). Solving Air Contaminant Problems in Data Centers. Uptime Institute. https://journal.uptimeinstitute.com/solving-air-contaminant-problems-data-centers/

[20] Torell, W. (2012). Site Selection for Mission Critical Facilities. Schneider Electric. https://it-resource.schneider-electric.com/white-papers/wp-81-site-selection-for-mission-critical-facilities

[21] Cottuli, C., & Christin, J. F. (2008). Comparison of static and rotary UPS. Schneider Electric. https://download.schneider-electric.com/files?p_File_Name=DBOY-78KRZE_R2_EN.pdf&p_Doc_Ref=SPD_DBOY-78KRZE_EN

[22] Moss, S. (2020). AWS develops its own in-rack UPS. Data Centre Dynamics. https://www.datacenterdynamics.com/en/news/aws-develops-its-own-rack-ups/

[23] Rasmussen, N. (2009). A scalable, reconfigurable, and efficient data center power distribution architecture. APC by Schneider Electric, Tech. Rep, 129. http://hosteddocs.ittoolbox.com/scalablereconfigurable_efficientdata.pdf

[24] Judge, P. (2021). What is lights out data center? Data Centre Dynamics. https://www.datacenterdynamics.com/en/analysis/what-lights-out-data-center/

[25] Judge, P. (2020). Data center staff classed as "essential" during pandemic. Data Centre Dynamics. https://www.datacenterdynamics.com/en/news/data-center-staff-classed-essential-during-pandemic/

[26] Easterly, J. (2021). ADVISORY MEMORANDUM ON ENSURING ESSENTIAL CRITICAL INFRASTRUCTURE WORKERS' ABILITY TO WORK DURING THE COVID-19 RESPONSE. U.S. Department of Homeland Security. https://www.cisa.gov/sites/default/files/publications/essential_critical_infrastructure_workforce-guidance_v4.1_508.pdf

[27] Ascierto, R., Lawrence, A., Bashroush, R., & Heslin, K. (2019) Ten data center industry trends for 2020. Uptime Institute Intelligence

[28] Ascierto, R., Brown, C., Traver, T., Dickerman, F., & Van Loo, R. (2021). The people challenge: Global data center staffing forecast 2021-2025. Uptime Institute Intelligence.

[29] Kulshrestha, S. (2021, October 18). Abysmal State of Global Critical Infra Security. CloudSEK. https://cloudsek.com/download/18101/

[30] CWE - Common Weakness Enumeration. (n.d.). MITRE. https://cwe.mitre.org/index.html

[31] FFP. (2021). FRAGILE STATES INDEX ANNUAL REPORT 2021. FFP. https://fragilestatesindex.org/wp-content/uploads/2021/05/fsi2021-report.pdf

[32] Cushman & Wakefield. (2016). Data Centre Risk Index. Cushman & Wakefield. https://verne-global-lackey.s3.amazonaws.com/uploads%2F2017%2F1%2Fb5e0a0da-5ad2-01b3-1eb8-8f782f22a534%2FC%26W_Data_Centre+Risk_Index_Report_2016.pdf

[33] Christensen, J. D., Therkelsen, J., Georgiev, I., & Sand, H. (2018). Data centre opportunities in the Nordics: An analysis of the competitive advantages. Nordic Council of Ministers. https://norden.diva-portal.org/smash/get/diva2:1263485/FULLTEXT02.pdf

[34] ITU. (2021). Global Cybersecurity Index 2020. ITU. https://www.itu.int/epublications/publication/global-cybersecurity-index-2020/en/

[35] Turton, W., & Mehrotra, K. (2021, June 4). Hackers Breached Colonial Pipeline Using Compromised Password. Bloomberg. https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

[36] Judge, P. (2021, September 29). Fire could cost OVHcloud €105 million, IPO filing reveals. Data Centre Dynamics. https://www.datacenterdynamics.com/en/news/fire-could-cost-ovhcloud-105-million-ipo-filing-reveals/

[37] Dawn-Hiscox, T. (2020, August 27). Report: faulty UPS triggers fire at Telstra's London data center. Data Centre Dynamics. https://www.datacenterdynamics.com/en/news/report-faulty-ups-triggers-fire-at-telstras-london-data-center/

[38] Data Centre Dynamics. (2015, June 25). Fire at BT Belfast causes internet disruption. Data Centre Dynamics. https://www.datacenterdynamics.com/en/news/fire-at-bt-belfast-causes-internet-disruption/

[39] Jones, P. (2012, August 8). Fire brings down data centers in India and Canada. Data Centre Dynamics. https://www.datacenterdynamics.com/en/news/fire-brings-down-data-centers-in-india-and-canada/

[40] Moss, S. (2021, August 31). Data center at New Orleans City Hall catches fire, taking down gov sites during Hurricane Ida. Data Centre Dynamics. https://www.datacenterdynamics.com/en/news/data-center-at-new-orleans-city-hall-catches-fire-taking-down-gov-sites-during-hurricane-ida/

[41] Judge, P. (2021, April 21). Fire destroys Nigerian electoral commission data processing equipment. Data Centre Dynamics. https://www.datacenterdynamics.com/en/news/fire-destroys-nigerian-electoral-commission-data-processing-equipment/

[42] Moss, S. (2019, July 8). Ghanaian MoH server room catches fire; security blocked by biometric locks. Data Centre Dynamics. https://www.datacenterdynamics.com/en/news/ghanaian-moh-server-room-catches-fire-security-blocked-biometric-locks/

[43] Dawn-Hiscox, T. (2018, October 16). Power switch fire, service outage at AT&T data center may have been caused by a lightning strike. Data Centre Dynamics.

https://www.datacenterdynamics.com/en/news/power-switch-fire-service-outage-t-data-center-may-have-been-caused-lightning-strike/

[44] Smolaks, M. (2015, November 17). Data center fire kills Internet in Azerbaijan. Data Centre Dynamics.
https://www.datacenterdynamics.com/en/news/data-center-fire-kills-internet-in-azerbaijan/

[45] Judge, P. (2015, December 18). Fire suppression kills Glasgow City Council's IT. Data Centre Dynamics.
https://www.datacenterdynamics.com/en/news/fire-suppression-kills-glasgow-city-councils-it/

[46] Swinhoe, D. (2021, September 28). UK TV broadcasts disrupted over weekend after fire suppression system triggered. Data Centre Dynamics.
https://www.datacenterdynamics.com/en/news/uk-tv-broadcasts-disrupted-over-weekend-after-fire-suppression-system-triggered/

[47] Alley, A. (2020, November 9). Global Switch's fire safety 'malfunction' damages Sydney data center servers. Data Centre Dynamics.
https://www.datacenterdynamics.com/en/news/global-switchs-fire-safety-malfunction-damages-sydney-data-center-servers/

[48] Dawn-Hiscox, T. (2018, April 19). Fire suppression failure at DigiPlex brings down Nordic Nasdaq. Data Centre Dynamics.
https://www.datacenterdynamics.com/en/news/fire-suppression-failure-at-digiplex-brings-down-nordic-nasdaq/

[49] Moss, S. (2020, September 15). Cooling loss causes outage at Microsoft Azure's UK South region. Data Centre Dynamics.
https://www.datacenterdynamics.com/en/news/cooling-loss-causes-outage-microsoft-azures-uk-south-region/

[50] Jones, P. (2013, March 14). Overheating brings down Microsoft data center. Data Centre Dynamics.
https://www.datacenterdynamics.com/en/news/overheating-brings-down-microsoft-data-center/

[51] Verge, J. (2015, January 6). Heatwave, Cooling Failure Bring iiNet Data Center Down in Perth. Data Center Knowledge.
https://www.datacenterknowledge.com/archives/2015/01/06/heatwave-cooling-failure-bring-iinet-data-center-down-in-perth

[52] Miller, R. (2007, November 13). Truck Crash Knocks Rackspace Offline. Data Center Knowledge.
https://www.datacenterknowledge.com/archives/2007/11/13/truck-crash-knocks-rackspace-offline

[53] Miller, R. (2010, January 20). U. of Penn Data Center Overheats. Data Center Knowledge.
https://www.datacenterknowledge.com/archives/2010/01/20/u-of-penn-data-center-overheats

[54] Miller, R. (2010, March 25). Wikipedia's Data Center Overheats. Data Center Knowledge.
https://www.datacenterknowledge.com/archives/2010/03/25/downtime-for-wikipedia-as-data-center-overheats

[55] Ricciuti, E. (2019, October 29). Fear the Squirrel: How Wildlife Causes Major Power Outages. The Nature Conservancy.
https://blog.nature.org/science/2019/10/29/fear-the-squirrel-how-wildlife-causes-major-power-outages/

[56] Tuominen, T. (2021, June). True forensics uncovered SE01 E03: too close to home. F-Secure. https://www.f-secure.com/en/consulting/our-thinking/true-forensics-uncovered-se01-e03

[57] Moss, S. (2021, January 7). Nashville bombing caused fires and floods at AT&T facility. Data Centre Dynamics. https://www.datacenterdynamics.com/en/news/nashville-bombing-causes-fires-and-floods-t-facility/

[58] United States Department of Justice. (2021, April 9). Texas Man Charged With Intent to Attack Data Centers. United States Department of Justice. https://www.justice.gov/usao-ndtx/pr/texas-man-charged-intent-attack-data-centers

[59] Miller, R. (2007, November 4). Armed Robbery at Chicago Data Center. Data Center Knowledge. https://www.datacenterknowledge.com/archives/2007/11/04/armed-robbery-at-chicago-data-center

[60] Miller, R. (2007, December 8). 'Ocean's 11' Data Center Robbery in London. Data Center Knowledge. https://www.datacenterknowledge.com/archives/2007/12/08/oceans-11-data-center-robbery-in-london

[61] Numminen, P. (2020, April 20). 5g-mastojen tuhoaminen levisi Ruotsiin - myös Pohjanmaalla paloi kännykkämasto. Iltalehti. https://www.iltalehti.fi/ulkomaat/a/31130a4d-bd55-472a-a3d9-074c453f9eb5

[62] CISA. (n.d.). Defining Insider Threats. CISA. https://www.cisa.gov/defining-insider-threats

[63] Kemp, T. (2018, July 19). What Tesla's Spygate Teaches Us About Insider Threats. Forbes. https://www.forbes.com/sites/forbestechcouncil/2018/07/19/what-teslas-spygate-teaches-us-about-insider-threats/

[64] Ferguson, S. (2020, August 29). Ex-Cisco Engineer Pleads Guilty in Insider Threat Case. BankInfoSecurity. https://www.bankinfosecurity.com/ex-cisco-engineer-pleads-guilty-in-insider-threat-case-a-14917

[65] Kanaracus, C. (2014). IT pro gets 4 years in prison for sabotaging ex-employer's system. Computerworld. https://www.computerworld.com/article/2489761/it-pro-gets-4-years-in-prison-for-sabotaging-ex-employer-s-system.html

[66] Kont, M., Pihelgas, M., Wojtkowiak, J., Trinberg, L., & Osula, A. M. (2015). Insider threat detection study. NATO CCD COE, Tallinn. https://ccdcoe.org/uploads/2018/10/Insider_Threat_Study_CCDCOE.pdf

[67] Bizo, D., Ascierto, R., Lawrence, S., & Davis, J. (2021). Uptime Institute Global Data Center Survey 2021. Uptime Institute Intelligence.

[68] Allsopp, W. (2010). Unauthorised access: physical penetration testing for IT security teams. John Wiley & Sons.

[69] Hern, A. (2018, January 28). Fitness tracking app Strava gives away location of secret US army bases. The Guardian. https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases

[70] Kozera, C. A. (2020). Fitness OSINT: Identifying and tracking military and security personnel with fitness applications for intelligence gathering purposes. Security and Defence Quarterly, 32(5), 41-52.

[71] Ascierto, R., & Traver, T. (2021). Data center security: Reassessing physical, human and digital risks. Uptime Institute Intelligence.

[72] Thomas, M. (2014). SMART BUILDING SECURITY. *Science in Parliament*, *71*(1), 20.

[73] Mansfield-Devine, S. (2019). The state of operational technology security. *Network security*, *2019*(10), 9-13.

[74] Stamatescu, G., Stamatescu, I., Arghira, N., & Făgărășan, I. (2020, June). Cybersecurity Perspectives for Smart Building Automation Systems. In 2020 12th International Conference on Electronics, Computers and Artificial Intelligence (ECAI) (pp. 1-5). IEEE. https://www.grigorestamatescu.com/files/iwsss20.pdf

[75] dos Santos, D., Speybrouck, C., & Costante, E. (2020) Cybersecurity in Building Automation Systems (BAS), Forescout Technologies. https://www.forescout.com/resources/bas-research-report-the-current-state-of-smart-building-cybersecurity-2/

[76] Kassner, M. (2015, February 2). Anatomy of the Target data breach: Missed opportunities and lessons learned. ZDNet. https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/

[77] Goodin, D. (2014, July 8). Wi-Fi passwords can be stolen by hacking smart lightbulbs. WIRED. https://www.wired.co.uk/article/crypto-weakness-lightbulbs

[78] Isaac, M., & Frenkel, S. (2021, October 4). Gone in Minutes, Out for Hours: Outage Shakes Facebook. The New York Times. https://www.nytimes.com/2021/10/04/technology/facebook-down.html

[79] Hutter, D. (2016). Physical Security and Why It Is Important. SANS Institute.

[80] Niles, S. (2011). Physical security in mission critical facilities (Revision 2). Schneider Electric. https://it-resource.schneider-electric.com/white-papers/wp-82-physical-security-in-mission-critical-facilities

[81] Cowan, C., & Gaskins, C. (2006). Monitoring physical threats in the data center. Buildings, 100(12), 26.

[82] Mathezer, S. (2021, October 1). Introduction to ICS Security Part 3. SANS Institute. https://www.sans.org/blog/introduction-to-ics-security-part-3/

[83] Williams, T. J. (1994). The Purdue enterprise reference architecture. Computers in industry, 24(2-3), 141-158.

[84] General Electric. (2017). Network Segmentation for Industrial Control Environments. General Electric. https://www.ge.com/digital/sites/default/files/download_assets/network-segmentation-for-industrial-control-environments-whitepaper.pdf

[85] Kaur, J., Tonejc, J., Wendzel, S., & Meier, M. (2015, May). Securing BACnet's pitfalls. In IFIP International Information Security and Privacy Conference (pp. 616-629). Springer, Cham.

[86] Peacock, M. (2019). Anomaly Detection in BACnet/IP managed Building Automation Systems.

[87] Bakuei, M., Flores, R., Remorin, L., & Yarochkin, F. (2021). 2020 Report on Threats Affecting ICS Endpoints.

[88] Siemens. (n.d.). Siemens ProductCERT and Siemens CERT. https://new.siemens.com/global/en/products/services/cert.html

[89] ABB. (n.d.). Cyber security alerts and notifications. https://global.abb/group/en/technology/cyber-security/alerts-and-notifications

[90] Lampson, B. W. (2004). Computer security in the real world. Computer, 37(6), 37-46.

[91] Suduc, A. M., Bîzoi, M., & Filip, F. G. (2010). Audit for information systems security. Informatica Economica, 14(1), 43.

[92] Boyce, M. W., Duma, K. M., Hettinger, L. J., Malone, T. B., Wilson, D. P., & Lockett-Reynolds, J. (2011, September). Human performance in cybersecurity: a research agenda. In Proceedings of the Human Factors and Ergonomics Society annual meeting (Vol. 55, No. 1, pp. 1115-1119). Sage CA: Los Angeles, CA: SAGE Publications.

[93] Netwrix. (2020). Best Practice Guide to Implementing the Least Privilege Principle. Netwrix.

[94] Neumann, P. G. (2010). Combatting insider threats. In Insider Threats in Cyber Security (pp. 17-44). Springer, Boston, MA.

[95] Weinert, A. (2019). Your Pa$$word doesn't matter. Azure Active Directory Identity Blog, Microsoft. https://techcommunity.microsoft.com/t5/azure-active-directory-identity/your-pa-word-doesn-t-matter/ba-p/731984

[96] Sarkar, S., Sarkar, S., Sarkar, K., & Ghosh, S. (2015, September). Cyber security password policy for industrial control networks. In 2015 1st International Conference on Next Generation Computing Technologies (NGCT) (pp. 408-413). IEEE.

[97] Zhang-Kennedy, L., Chiasson, S., & van Oorschot, P. (2016, June). Revisiting password rules: facilitating human management of passwords. In 2016 APWG symposium on electronic crime research (eCrime) (pp. 1-10). IEEE.

[98] Smith, T., Ruoti, S., & Seamons, K. E. (2017). Augmenting Centralized Password Management with Application-Specific Passwords. In SOUPS.

[99] Eminağaoğlu, M., Uçar, E., & Eren, Ş. (2009). The positive outcomes of information security awareness training in companies–A case study. information security technical report, 14(4), 223-229.

[100] Bullée, J. W. H., Montoya, L., Pieters, W., Junger, M., & Hartel, P. H. (2015). The persuasion and security awareness experiment: reducing the success of social engineering attacks. Journal of experimental criminology, 11(1), 97-115.

[101] Schneider Electric. (2011) A Practical Guide to Disaster Avoidance in Mission-Critical Facilities (Revision 0). Schneider Electric. https://download.schneider-electric.com/files?p_enDocType=White+Paper&p_File_Name=VAVR-8K4TYD_R0_EN.pdf&p_Doc_Ref=SPD_VAVR-8K4TYD_EN

[102] Keeney, M., Kowalski, E., Cappelli, D., Moore, A., Shimeall, T., & Rogers, S. (2005). Insider threat study: Computer system sabotage in critical infrastructure sectors. National Threat Assessment Ctr Washington Dc.

[103] NCCIC/US-CERT. (2014). Combating the Insider Threat. NCCIC/US-CERT. https://us-cert.cisa.gov/sites/default/files/publications/Combating%20the%20Insider%20Threat.pdf

[104] Larson, S. & Singleton, C. (2020, December). Ransomware in ICS Environments. Dragos.

[105] CISA. (2021, June). Rising Ransomware Threat To Operational Technology Assets. CISA. https://www.cisa.gov/sites/default/files/publications/CISA_Fact_Sheet-Rising_Ransomware_Threat_to_OT_Assets_508C.pdf

[106] Greenwald, G. (2014). How the NSA tampers with US-made internet routers. The Guardian. https://www.theguardian.com/books/2014/may/12/glenn-greenwald-nsa-tampers-us-internet-routers-snowden

[107] CVE Overview. (n.d.). MITRE. https://www.cve.org/About/Overview

[108] Mlitz, K. (2021). Number of data centers worldwide in 2015, 2017, and 2021. Statista. https://www.statista.com/statistics/500458/worldwide-datacenter-and-it-sites/#statisticContainer

[109] Mlitz, K. (2021). Number of hyperscale data centers worldwide from 2015 to 2021. Statista. https://www.statista.com/statistics/633826/worldwide-hyperscale-data-center-numbers/