Data Center Security | White Paper

Prepared by Yann Morvan

Why preventing human error should be a part of your Data Center access control strategy.

Contents

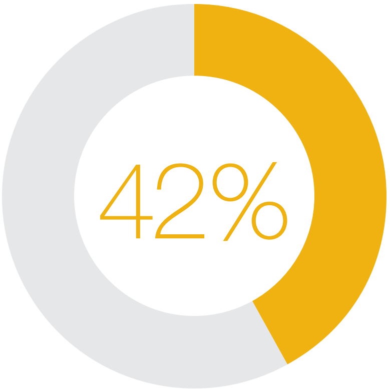
Data centers are the foundation of today's digital world and the most critical asset across every industry and every business. They store, process, and disseminate all the data and applications that keep the world moving and connected. Whether it's consumer activities, daily business transactions, or public operations, everything that happens online and digitally is supported by IT equipment housed in either cloud, enterprise-owned, or leased multi-tenant data centers.

As the world continues to digitize at break-neck speed, data centers are experiencing exponential growth, ever-increasing regulations, and greater risk of cyberattacks. As these environments become more complex, they are also becoming become more vulnerable to downtime, risk, and cost caused by human error. While most data centers do an excellent job of deploying access control to prevent unauthorized personnel from accessing the space, the missing link in data center access control strategy is preventing human error through the use of rack-level access control.

Where We Go Wrong: Human Error

Human error in the data center typically stems from misconfigurations and incorrect change management, such as moves, adds, and changes performed in the wrong rack. While to err is human, it is a growing problem in the data center. According to the Uptime Institute's 2022 Annual Outage Analysis, human error has now emerged as the primary cause of downtime, with more than 40% of surveyed organizations suffering a major outage in the past three years caused by human error.

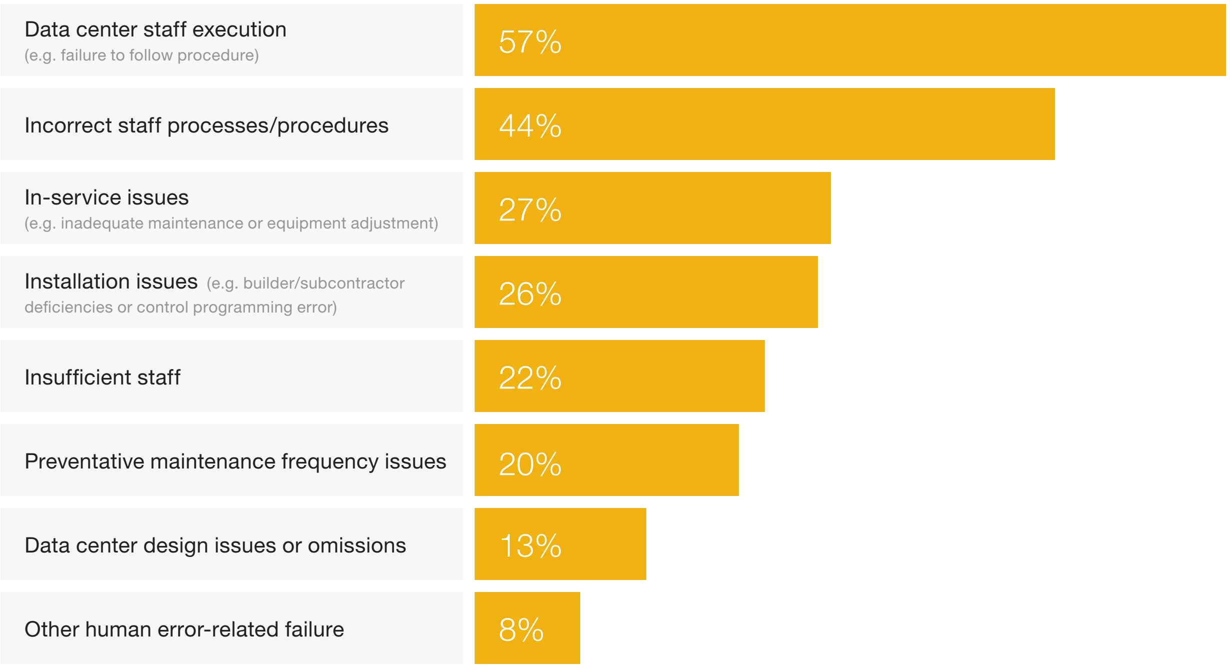
Why is human error on the rise? Data centers have become increasingly complex, with more data, more applications, and more diverse IT equipment and connections than ever before. Software-defined networking and highly virtualized server environments with resources distributed across multiple servers further increases complexity. At the same time, the Uptime Institute indicates an ongoing workforce shortage with nearly half of data center owners and operators



Percentage of data center managers that have experienced an IT outage due to human error in the last three years[1]

[1] Source: Uptime Institute

Most Commonly Cited Human Errors[2]



having difficulty finding skilled data center staff. The potential for human error is exacerbated by complexity and insufficient staff in data center environments.

Vulnerabilities caused by human error are compounded by rising cybersecurity attacks.

In addition to downtime, human error puts data center owners at greater risk for cybersecurity attacks and data breaches. When connections are misconfigured, or when equipment firmware upgrades are performed in the wrong rack, it raises the potential for unprotected points that can be exploited. According to the 2021 IBM Cyber Security Intelligence Index Report, 95% of their cybersecurity breaches were caused by human error.

Vulnerabilities caused by human error are compounded by rising cybersecurity attacks. Since the onset of the pandemic, the U.S. FBI reported a 300% increase in cybercrimes. Ransomware attackers are also shifting their target toward data centers that contain more critical information versus individuals. When bad actors gain unauthorized access to data center equipment remotely via misconfigurations, they can set up remote gateways, download malware, damage or steal hard drives, or install rogue devices designed to gain access to sensitive information.

[2] Source: Uptime Institute

The Financial Impact: Too Big to Ignore

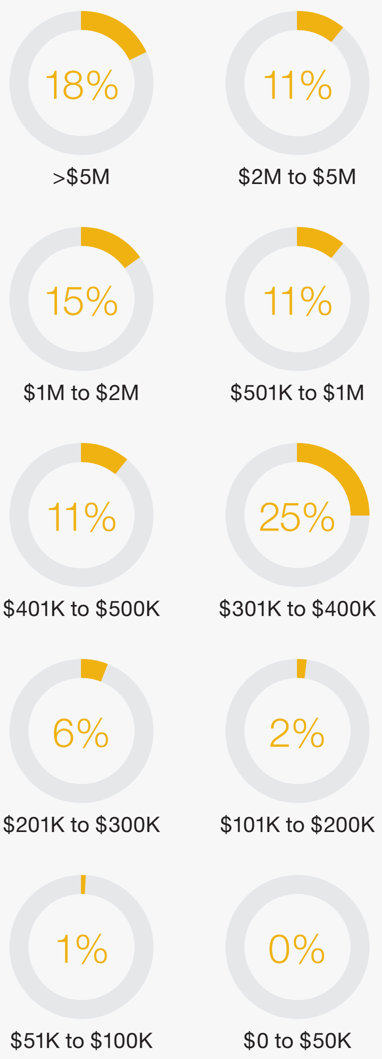
With nearly every business transaction happening online and digitally, the cost of unplanned downtime due to human error has increased significantly. According to ITIC's 2022 Hourly Cost of Downtime Survey, downtime costs increased 32% in the past seven years, with the hourly cost now exceeding $300K for more than 90% of enterprises and 44% of mid-sized and large enterprise reporting that a single hour of downtime can reach more than $1 million. The hardest hit industries include finance, entertainment, media, manufacturing, hospitality, transportation, healthcare, and retail.

While the cost of downtime is measurable based on lost revenue, labor, and recovery expense, it also includes hidden costs such as the fiscal impact associated with taking data center managers away from more strategic technology projects and the damage to a company's reputation. A PricewaterhouseCoopers customer experience report found that 77% of consumers leave a website without purchase if they encounter an error, with 60% unlikely to return.

Downtime costs increased 32% in the past seven years, with the hourly cost now exceeding $300K for more than 90% of enterprises.

Cybersecurity breaches caused by human error in the data center can also lead to crippling costs. IBM's 2021 Cost of a Data Breach Report found that the average cost of a data breach has reached $4.24 million, with a healthcare data breach along costing upwards of $9 million. The report also found that in 2021, it took an average of 287 days to identify and contain a breach.

91% Majority of Corporations Say Hourly Downtime Costs Exceed $300K[3]



$4.24M Average cost of a data breach (healthcare data breach costs upwards of $9M)

287 Average number of days to identify and contain a breach

[3] Source: ITIC's 2022 Hourly Cost of Downtime Survey

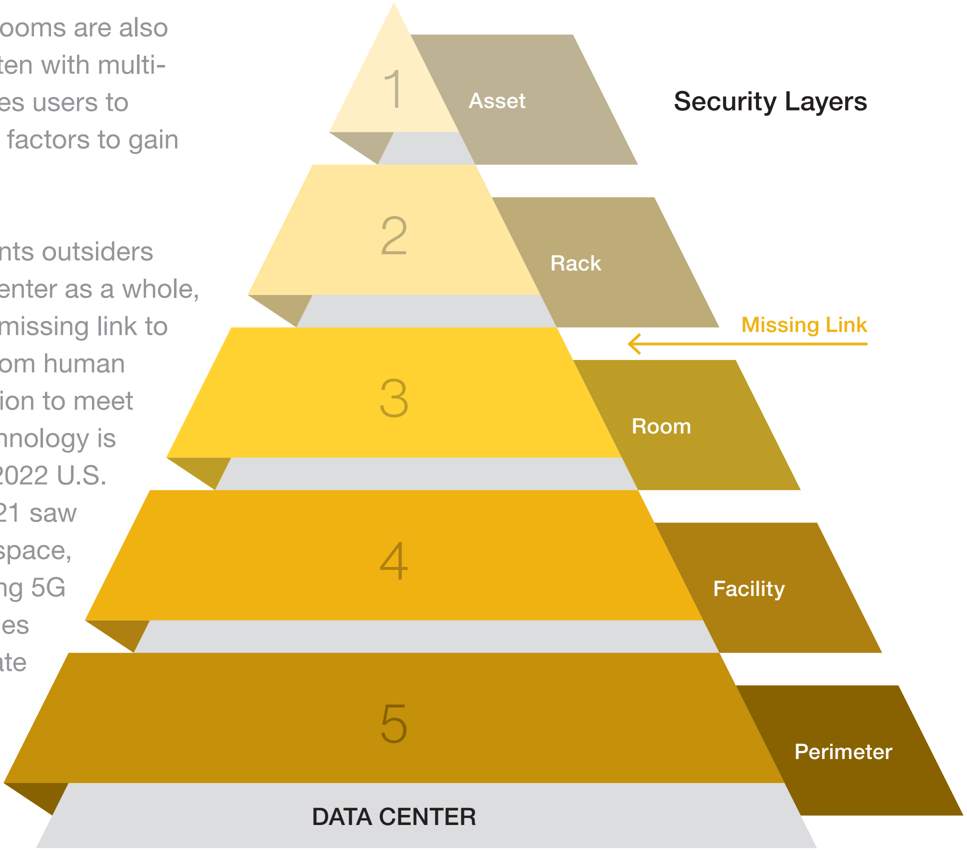
Rack-Level Access Control: The Missing Link

Best practice in optimizing data center physical security is to use a layering approach where perimeter, facility, and computer room security prevent unauthorized personnel from accessing critical data center space. This typically includes solutions such as access control at perimeter gates and building entrances, video surveillance systems, and the use of mantraps commonly found in multi-tenant data centers where a smaller room separates unsecure and secured areas. Highly secure spaces within the data center such as main entrance facilities, meet-me rooms, and cross-connect rooms are also secured with access control, often with multi-factor authentication that requires users to provide two or more verification factors to gain access.

While outer-layer security prevents outsiders from gaining entry to the data center as a whole, rack-level access control is the missing link to preventing downtime and risk from human error. Rapid data center expansion to meet the exponential demand for technology is partly to blame. According the 2022 U.S. Real Estate Market Outlook, 2021 saw a record growth of data center space, up 50% from 2020, and emerging 5G and edge computing technologies are expected to further accelerate growth in 2022 and beyond. In a rush to build or expand data center space, many data centers have failed to focus on controlling and managing inner-layer access control at the rack. Still others are under the misconception that perimeter, facility, and computer room controls are sufficient.

But given the impact of human error and the growing number of third-party contractors and service providers with access to the data center space, rack-level access control is more important than ever. Controlling and managing who has access to IT equipment within individual

While outer-layer security prevents outsiders from gaining entry to the data center as a whole, rack-level access control is the missing link to preventing downtime and risk from human error.



racks, cabinets, and enclosures can significantly reduce the chance of technicians and service providers performing moves, adds, and changes in the wrong rack that have the potential to cause downtime and put the data center at risk.

Rack-level access control also prevents those with authorized access to the data center from accessing highly-sensitive and valuable data with malicious intent. Within leased data centers where multiple tenants have access beyond the perimeter and facility level, inner-layer physical security is especially paramount. A Cyber-Art survey of 600 financial workers found that 41% admit to having taken sensitive data to a new position, with 69% of employers seeing full-time employees as the biggest threat. Labor shortages, high turnover rates, and the current economic and political climate are further driving malicious intent. According to a 2020 Cost of a Data Breach Report, 10% of malicious breaches in the study were caused by a physical security compromise, at an average cost of $4.36 million.

Regulatory Compliance: Another Call for Rack-Level Access Control

As data centers transmit and store more data from more devices, regulations are increasing in number and enforcement. Data privacy regulations like the EU General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA) require organizations to protect personal data, and several states and countries around the world are on the verge of adopting similar legislation.

In the healthcare industry, the Health Insurance Portability and Accountability Act (HIPAA) privacy rule requires the protection of any information regarding a person's health information. In the financial industry, any business that processes debit or credit card transactions must secure payment transaction data in compliance with the Payment Card Industry Data Security Standard (PCI DSS). Per the Federal Information Security Management Act (FISMA) of 2002, federal agencies must also implement information security plans to protect sensitive data. Fines for data breaches due to non-compliance of these regulations can reach well into the millions.

It's not just privacy data regulations that require compliance. All data centers today are facing scrutiny on how they manage, store, and control access to sensitive information. Overseen by the American Institute of Certified Public Accountants (AICPA), SSAE18 standards regulate how service providers manage, store, and control access to sensitive information and compliance is required as part of service level agreements (SLAs) among cloud, managed services, and multi-tenant data center providers.

While encryption, firewalls, and proper data management procedures are vital to complying with regulations that protect sensitive data, these regulations also require organizations to physical secure access to data environments. To track and identify sources of a data breach, several of these regulations require audit logs that record who accessed data and the equipment that processes that data, at what time, what actions they took, and what specific data they accessed.

Physically securing access to data environments and maintaining audit logs of who accessed equipment is simply not possible without rack-level security.

Developing a Strategy: Top Ten Considerations

While a data center access control strategy that prevents human error clearly calls for rack-level security, implementing access control at every rack can seem daunting—especially in data center environments that contain hundreds of racks. But it doesn't have to be. The following considerations and key features can help ease deployment and manageability of rack-level access control, while preserving operational efficiency as technology continues to evolve.

1 GO DIGITAL

Traditional unintelligent keys and mechanical locks that come with enclosed data center racks are insecure and unmanageable. Keys that can be easily copied, shared, or lost can end up in the wrong hands and require locks to be refitted and new keys issued. Plus, it's unfeasible to manage traditional keys for hundreds or even thousands of racks when different service staff need access to different racks. Maintaining an audit trail of which keys have been assigned to which users is difficult and often inaccurate, and unintelligent keys and locks offer no way to know who accessed equipment and when. Thankfully, like virtually everything else in the world, access control systems are shifting to digital with intelligence, centralized management, and advanced features that eliminate the problems associated with traditional keys.

2 SIMPLIFY INSTALLATION

Electronic locks need power to function and connectivity for centralized management, requiring the time-consuming and expensive task of implementing power and communications cabling to every rack. Battery-powered systems eliminate the need for power runs, but they are not as secure and can be difficult to manage since batteries eventually fail. Access control solutions that wirelessly transfer power to locks and send data can significantly simplify the required infrastructure, eliminating excessive labor, time, and expense. Vendor-agnostic solutions with locks that work on any vendors' enclosed rack can also ease deployment.

3 CUSTOMIZE TO SUIT

The ability to create customized user roles and permissions that limit access to specific data center racks at specific times reduces the chance of technicians and service providers performing moves, adds, and changes in the wrong rack and prevents intentional malicious behavior. Customized timeouts that limit access to a specific time period are especially ideal for controlling third-party provider access and managing time-sensitive tasks.

4 ENSURE EASE OF USE

An access control system should be easy to use for both administrators and users. Centralized-management platforms should be intuitive for administrators to easily add new devices and users, assign permissions, and set preferences. Platforms with user-friendly administration dashboards provide complete system visibility to facilitate monitoring. Users of the access control system should also be able to operate locks on their assigned racks easily and reliably with a single key. Solutions that offer a mobile platform for operating locks via smartphones can help improve ease of use and staff productivity.

5 ACHIEVE COMPLIANCE

For data centers needing to comply with regulations like HIPAA that require audit logs of who accessed data equipment, it's important to select a rack-level access control solution that provides 100% audit trails and reporting to ensure compliance. Knowing who accessed equipment when and where also provides an audit trail for quickly investigating, identifying, and addressing sources of downtime and data breaches.

6 PROTECT THE CRITICAL

While the required level of security varies from one data center to the next, key features to consider for mission-critical environments include dual-locking confirmation, multi-factor authentication, biometrics, and the ability to quickly and remotely deauthorize users. Security is also enhanced with solutions that provide 24/7 alerts of unauthorized attempts, unlocked locks, and other potential vulnerabilities. Solutions that offer continued protection in the event of a power and/or network failure are also vital to protecting critical assets.

7 LOOK TO THE CLOUD

Spending hours on site configuring access control equipment, setting up and managing users, and monitoring user activity and system performance is not an option for busy data center mangers. Cloud-based access control solutions eliminate the need for complex configuration of equipment, offer automatic data storage and backup, and use web-based software platforms and mobile apps that enable remote real-time visibility, send security alerts, and allow for managing permissions and assignments from any device.

8 CONSIDER INTEGRATION

Data centers may use existing solutions like Microsoft Active Directory for managing permissions to network resources or cloud-based facility access control platforms. It's important to consider the ability of a rack-level access control system to integrate with other security platforms through application programming interfaces (APIs).

9 KEEP PACE WITH TECHNOLOGY

Rack-level access control should not limit the ability of a data center to easily reconfigure or expand to support new services and technologies. Ideally, the access control system should have no limit on the number of users and locking devices across multiple data center sites. Locking devices should also be easily moved from one rack to another. Cloud-based solutions also help ensure scalability in that they enable automatic updates and support new features without the need to upgrade or replace any equipment.

10 THINK BEYOND THE RACK

Data centers can contain multiple zones, spaces, and enclosures for housing equipment, inventory, documentation, electrical circuits, and other critical mechanical systems. It therefore makes sense to consider systems that incorporate a variety of lock options beyond just enclosed racks, such as locks for indoor and outdoor wall-mounted electrical panels, air handlers, and other mechanical enclosures. Securing open-rack environments is also a key consideration and one that has long presented a challenge for data center owners and operators. In spaces where SLAs require tenant access control, open racks are often placed in secured cages. However, cages take up valuable space and they still don't allow for securing individual open racks within the cage. Newer access control innovations such as sensor field detection for open rack environments can eliminate the need for cages.

Secure Your Data Center Racks Today

If your data center access control strategy doesn't go beyond securing the perimeter, facility, and room level, you could be risking downtime or cyberattack due to human error that can cripple your business and cost well into the millions of dollars. Rack-level access control that ensures only the right individuals access the right racks at the right time is the last line of defense—and regulations demand it. Thankfully, understanding the key considerations and knowing what features to look for can make it easy to deploy and manage rack-level access control as technology continues to evolve.

Please visit invue.com/data-center-2022 to learn more about InVue's Data Center solutions for rack-level protection.