interxion™
A DIGITAL REALTY COMPANY

Whitepaper

Security in the Data Centre

Physical and Cyber Converge for New Opportunities

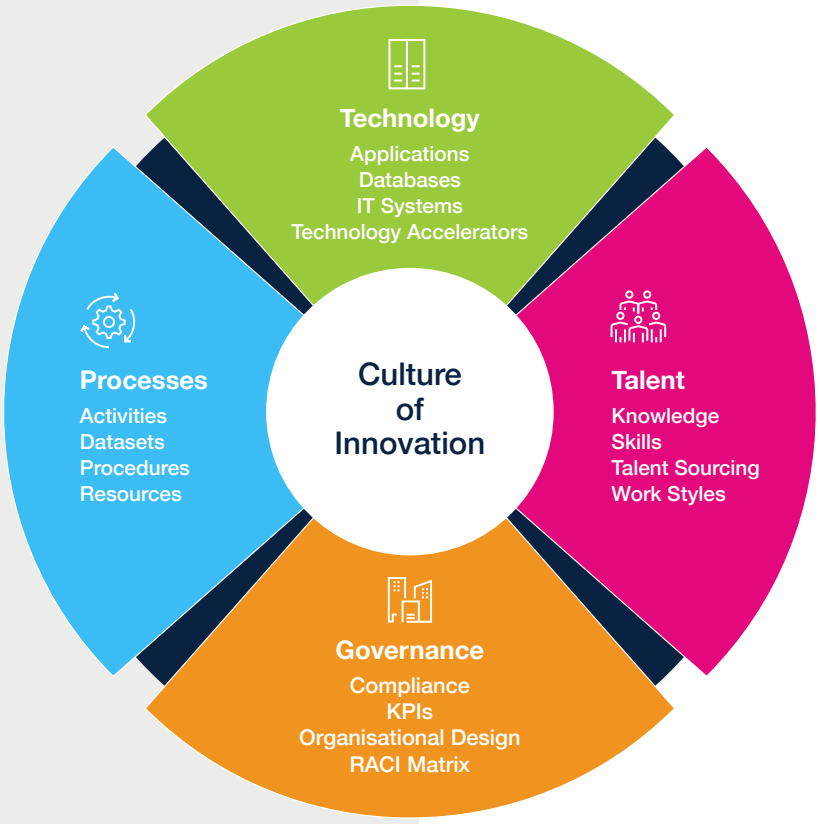
INTRODUCTION

> *Data centres must be diligent to ensure physical and cyber systems are protected in a unified way...*

Data centres are entering a new transformational era. Gone are the days of air-gapped networks. Data centres are monitored and managed through a network of hundreds or even thousands of sensors used for real-time telemetry—temperature and humidity control, maintenance alerts, physical security, and much more. Yet, in addition to introducing new opportunities for enhanced operational efficiencies and greater visibility and control, digital transformation (DX) presents new challenges.

Manipulation of heating and ventilation controls (HVAC) could result in critical infrastructure systems being shut down or compromised. Physical cameras could be hacked and commandeered to disguise a robbery or unauthorized entry into a secure location.

Data centres must be diligent to ensure physical and cyber systems are protected in a unified way, and that their convergence does not create additional risks. Further, data centres will begin to see advanced technologies such as artificial intelligence (AI) and machine learning (ML) deployed to pinpoint anomalies in both physical and cyber security and to enact real-time controls and remediation processes.



New Capabilities Required by Digital Transformation (DX)

The enterprise must develop new capabilities to succeed in digital transformation. Each new capability must be made up of these four elements: technology, talent, governance, and processes.

Source: IDC

Digital Transformation Presents New Data Centre Challenges

The data centre for many businesses is seen as a strategic lever in their efforts to support business acceleration requirements.

Business acceleration objectives include:

- **Addressing emerging markets**
- **Lowering costs while improving operating efficiencies**
- **Creating more and better customer engagement**
- **Tapping new revenue opportunities**

Remaining competitive and maintaining aggressive margins requires ongoing innovation, and DX stands at the centre. The data centre plays a pivotal role in enabling many DX initiatives. **Data centres are where the cloud lives**. Leveraging this fact allows data centres to become private cloud service centres that streamline processes while retaining control of operations and security. These give organisations the scale required to tackle these new DX initiatives—the compute power and storage capabilities to power the new applications and accompanying data that is generated. A significant factor driving this is the growing reliance of AI and ML on big data.

To address this new data centre landscape, many organisations are opting to use colocation facilities rather than building out their own data centres. But just as the new evolution of the data centre is helping to enable DX, the data centre is also undergoing a DX transformation—one that has its own challenges.

Colocation Creates a Convergence of Physical and Cyber Security

It's critical that physical and cyber security be approached in a unified manner since they have become increasingly convergent in recent years. The most obvious example of this is the fact that physical security deployments (card readers, CCTV) now all reside on the network. This results in a physical security dependency on strong cybersecurity controls to ensure the integrity of physical security infrastructure. However, this dependency in turn offers intriguing new ways to leverage both disciplines to drive new security paradigms. For example, if an employee logs into a computer in San Francisco yet physically accesses a New York data centre, that would constitute a major red flag. With artificial intelligence and machine learning, the system could adapt to such a situation to alert responders and revoke access permissions immediately without human intervention. But with technical innovation comes new attack vectors and vulnerabilities, for the truth is that hackers are always looking for undetected paths into your systems. Many traditional physical devices now represent threats to cyber security. Things like ID cards, biometrics, HVAC, laptops, smartphones, and USBs are all cyber security threats since they are now IP-enabled. In fact, IoT devices experience an average of 5,200 attacks per month (Source: Symantec).

DX requires a rethink of physical security. However, the need to focus on controlled access, meaning designated workers should be able to access only the areas, systems, and applications to which they should have access, remains the foundational concept of ensuring the confidentiality, integrity and availability of data wherever it resides and regardless of how it is used.

69%

of global leaders surveyed noted a significant increase in cyber attacks at their companies this year. However, despite the elevated risk environment, leaders plan to continue to invest heavily in digital transformation—with 94% of chief financial officer (CFO) respondents looking to move their financial systems or ERP to the cloud

Source: Deloitte Global 2021 Future of Cyber Survey

To ensure adherence to these access protocols, organisations need to institute digital and physical monitoring—which must occur at the rack level and provide a complete compliance audit trail, full transparency and reporting, and automated processes for revoking access. Regulations that may apply include the Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), the Federal Information Security Management Act (FISMA), the European Union's General Data Protection Regulation (GDPR), and Sarbanes-Oxley Act 2002 (SOX). But organisations should not stop at government and industry regulations; they should also consider implementing security standards such as the National Institute of Standards and Technology (NIST), the International Organization for Standardization (ISO), the Center for Internet Security (CIS) controls, and others.

AI and ML provide the means to monitor physical security devices such as doors and cameras, pinpointing anomalies, sending real-time alerts to data centre personnel, and even acting as a digital system to immediately combat threats without human intervention. As noted at the beginning of this section, the convergence of cyber and physical security allows physical security alerts to activate cybersecurity protocols such as blocking access to data and systems for users, devices, and applications based on predetermined business rules. As this technology matures and becomes ubiquitous, it will shift the security paradigm from one of "detect and respond" to one of "prevent and counter".

A Physical Security Data Centre Checklist

When vetting colocation facilities, organisations need to evaluate solutions based on criteria that include questions such as:

01. Is the data centre redundant?

It is important for your data centre to be prepared for the unexpected. Any number of things could go wrong such as utility failure, cooling system equipment failure, fire, air quality issues and natural disasters. That is why building out a redundant design for your data centre is crucial. There are three redundancy maturity models. The first involves building redundancy across all system elements which are critical and must deliver the capacity required to power, backup, and cool a facility at full IT load. But achieving a full IT load is not enough in the event of a component failure or if a system element must undergo maintenance. In order to address these events that cannot be predicted, data centre design calls for at least one independent backup unit for every 4 needed (the second maturity model is referred to as N+1). The final maturity model, 2N, refers to redundancy where there are two independent distribution systems—from power supplies to cabling. Finally, does the redundancy model extend beyond power, cooling and backup to include the physical security infrastructure? If not, a significant exposure to the security of your data can be as close as the next power outage.

02. Is the building constructed to withstand external attacks or natural disasters?

Wall density should be designed to withstand explosive devices and natural elements. Windows should be minimised, used only for public spaces and employ shatter resistant window film. A buffer of at least 100 feet should extend around the site to protect from vehicles and, ideally, security guards/ stations should be employed for access. Kevlar fire-resistant walls are also an important requirement.

03. Are entry and exit points limited?

There should be one main entrance to the building and a loading dock on the backside, typically located at the rear of the building. Vehicle pathways leading to entrance areas should be blocked by crash-resistant bollards, industrial concrete planters or other barriers to prevent vehicle penetration at these critical access points. Fire doors should be exit-only and both entry points should be monitored 24x7 using IP-enabled video surveillance. These cameras should be integrated into the network firewall to ensure they are protected from cyber-attacks.

04. What physical intrusion detection policies are in place?

Automated electronic intrusion detection systems, including event-driven closed circuit television cameras (CCTV) and alarms, are a requisite. Here, data centre teams must have documented policies for response to ingress and egress violations.

05. What security surveillance cameras are in use?

Camera systems should be tailored to their application. This may include motion-detection, pan-tilt-zoom, and low-lighting capabilities. They also need to be integrated into network security with passwords and credentials designated for access (viz., IP-enabled) and isolated by data centre firewalls to ensure they cannot be compromised, or be used to compromise the internal data centre network. Organisations also need to implement data retention and destruction policies for surveillance footage. These must comply with relevant laws, industry regulations and IT standards. We would suggest retaining surveillance video footage for a minimum of 90 days.

06. Is multi-factor authentication employed?

Ingress and egress access must be controlled by multi-factor authentication. Biometric identification helps ensure that personnel access only those areas to which they are authorized. Given privacy concerns about the sensitivity of biometric data, it is recommended that biometric data remain in the possession of the end-user, e.g., the biometric algorithm should reside directly on the user's credential as opposed to a central database.

07. Are hardened access layers used?

Any person who enters the most secure area of a data centre should be required to authenticate at least four times—for example, building perimeter entrance to lobby/loading dock, lobby/loading dock entrance to common space, entrance from common space to data centre space and entrance to the most secure area (cage, cabinet, etc.).

Cyber Threats to the Data Centre

The biggest challenge to data centre security today is not physical threats but rather cyber threats. The proliferation of applications and burgeoning mounds of intellectual property and private information—often governed by regulators—makes data centres a central target for cyber criminals and even nation-states.

Defending Against Data Centre Attacks

As a result of DX, the cyber-attack surface for the data centre is expanding and becoming increasingly harder to defend. These threats can target physical devices and systems used to manage cooling and video surveillance, among others. They can also target personnel through spear phishing, gaps in authentication protocols, and other malicious means.

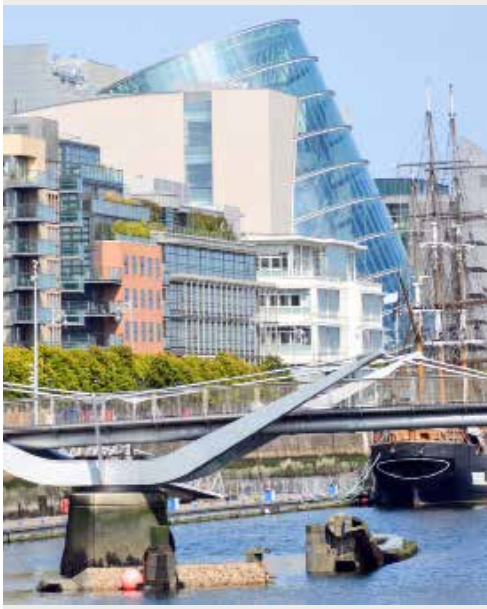
Unless data-centre vulnerability is internet-facing, attackers must be persistent and employ advanced strategies to achieve a successful exploitation:

01. Implement two-factor or multi-factor authentication:

Many data centres rely on local authentication options in the event of an emergency. These local authentication channels are not logged and the same login credentials are often shared across hosts and workloads (for simplicity). This exposes them to bad actors, who, once they have stolen them, can use them to gain access to the data centre. Adding multiple layers of authentication for a single user through two-factor or multi-factor authentication will ensure a higher level of security, making it much more difficult for an intruder to access systems they are not allowed to access.

02. Target known vulnerabilities with patching and updates.

Virtualised environments and resources must still run on physical hardware— specifically, virtual disks are dependent on physical disks that reside on physical servers. Management planes have their own management protocols, power, processors, and memory that are managed via protocols such as Intelligent Platform Management Interface (IPMI). These latter protocols reside beneath virtualisation layers and are slow to receive updates and patches. Known to have security weaknesses, bad actors target vulnerabilities in IPMI. Organisations must ensure they practice good cyber hygiene and that their patching and updates target known vulnerabilities being targeted by cyber criminals.



03. Build barricades.

Threats from outside the data centre such as email, web gateways, DevOps, Internet of Things (IoT), and operational technology (OT) present substantial risk, and cyber criminals are exploiting each of these attack surfaces. Here, lateral (east-west) movement of malicious intrusions allow cyber criminals to gain access to the data centre.

An emerging trend is the move to augment point-in-time penetration tests designed to validate cyber integrity with a reliable continuous monitoring capability that operates in real time. Tools are available to analyse incoming network traffic for anomalies and identify those which require more scrutiny by information security engineers. This builds assurance that network security is operating effectively over prolonged periods of time and serves to validate pen test results.

04. Build a virtual or a digital system.

The reality is that no matter how much you try to protect against security breaches from coming in, it's becoming increasingly more and more difficult to do so. Threats can come in the form of hacked devices, such as servers, routers, switches, and firewalls. In these instances, known vulnerabilities are targeted in these devices, employing rootkits that sit below the operating system and are hard to detect. Ironically, the very devices intended to protect an enterprise are infected and turned into malicious gateways into the data centre. That's why AI and ML are starting to be implemented as security strategies to act more like an immune system by detecting and fighting threats from within instead of purely focusing on keeping threats out at the perimeter. These strategies can act like antibodies in the human body to combat suspicious behavior that falls outside the norm without shutting the entire system down.

Future of Data Centre Security

Keeping pace with the rapidly evolving threat landscape necessitates a security program that is comprehensive, integrated, and employs advanced technologies. This approach encompasses cybersecurity and physical security as both are important. With data centres—a critical lever for DX initiatives and private cloud adoption growing their footprints in many instances—successful exploitation of these data centre threats can have serious ramifications.

Looking to the future, data centre leaders need to embrace additional cyber and physical security strategies. At the forefront and reaching across the entire security fabric is the integration of cyber and physical security. Attacks are becoming increasingly multi-stage, targeting physical security through cyberattacks that create physical exposure. And with 34% of attacks involving internal players, physical security remains critical. The moral here is that cyber and physical security are complementary parts of a complete security program.

Data centres need to ensure that their cyber and physical security is seamlessly integrated. Physical systems and devices must reside on secure networks and behind firewalls. This helps protect them from malicious attacks, while providing seamless incident response capabilities in the event of an intrusion.

Other security strategies that data centre leaders should have in place include:

01. **Data governance—at rest and in transit, across and between multiple cloud environments.**

The volume of unstructured data is set to grow from 33 zettabytes in 2018 to 175 zettabytes, or 175 billion terabytes, by 2025. Source: VentureBeat 2021. To protect this information, whether on-premises or the cloud, organisations need to implement data governance policies in control—for moving data across and between different environments and between applications.

02. **Cloud transparency and controls.**

For public clouds, organisations need to ensure they have the right governance policies and controls in place. These are important.

03. **Security integration.**

83 percent of IT leaders cite organisational complexities as putting them most at risk. A new, integrated security framework is needed. Traditional security architectures are fragmented, and it is difficult to share information across and between the different elements. This includes new data centre attack surface areas such as DevOps and the cloud for full transparency and centralised controls.

04. Protecting the edge of network.

5G increases the ease and speed at which devices attach to the network as well as the amount of data that can be accessed and moved. IoT poses substantial risk (as these devices cannot be managed via traditional security models), and lateral intrusions can impact data centre security. Software-defined wide area networks (SD-WAN) leverage 5G as an additional bandwidth channel, which bypasses traditional data centre security controls. This increases risk that can back-funnel into the data centre via lateral movement.

05. Threat intelligence: artificial intelligence and machine learning.

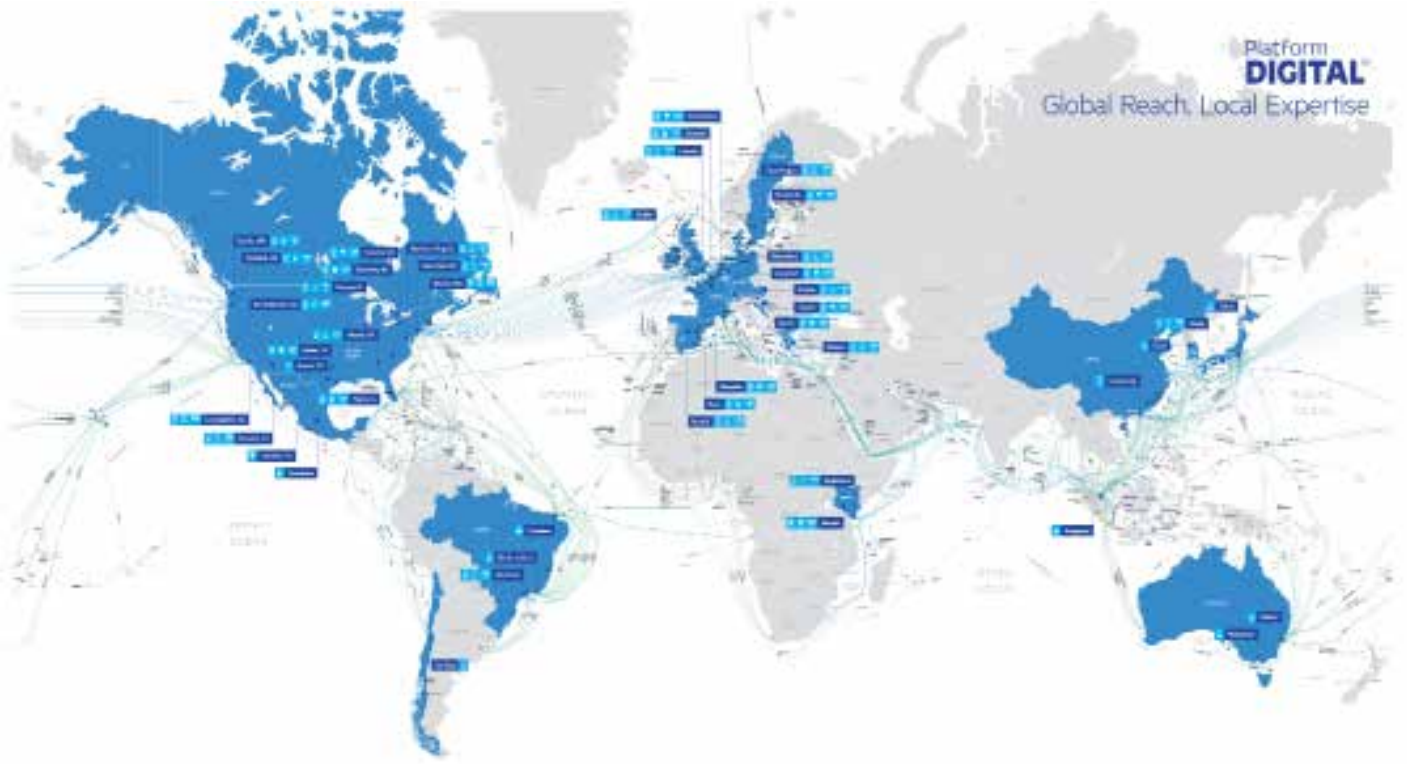
85% of organisations indicate threat intelligence is critical to a strong security posture. But only 42% believe they are very effective in using threat intelligence. Part of the problem is lack of in-house expertise (50%). To keep pace with security threats that are using artificial intelligence (AI) and machine learning (ML) and are polymorphic and multi-vector, cybersecurity leaders must employ ML and AI capabilities themselves, or switch to tools that have AI/ML enhanced capabilities. This enables them to reduce the attack surface for prevention, detection, and remediation.

Turning the Data Centre into a DX Enabler

DX is propelling business acceleration, and the data centre is the engine making much of it possible. But with this expanded attack surface, also comes greater threats to the data centre—both physical and cyber. DX is also driving a transformation of the data centre that presents new security challenges.

To protect their environments from these new and expanded threats, IT leaders must ensure they have the right defences in place. The convergence of physical and cyber threats necessitates the integration of data centre security. Here, IT leaders need to ensure their physical systems and devices are integrated into network security and behind firewalls. Finally, to counter advances in the threat landscape, data centres need to tap cybersecurity that leverages AI and ML capabilities.

Our Global Reach



About Interxion: A Digital Realty Company

Interxion: A Digital Realty Company is a leading provider of carrier- and cloud-neutral data centre services across EMEA. With more than 700 connectivity providers in over 100 data centres across 13 European countries, Interxion provides communities of connectivity, cloud and content hubs. As part of Digital Realty, customers now have access to 49 metros across six continents.

For more information, please visit **www.interxion.com**

www.interxion.com
customer.services@interxion.com

International Headquarters
Main: + 44 207 375 7070
Email: hq.info@interxion.com

European Customer Service Centre (ECSC)
Toll free Europe: + 800 00 999 222 / Toll free US: 185 55 999 222
Email: customer.services@interxion.com