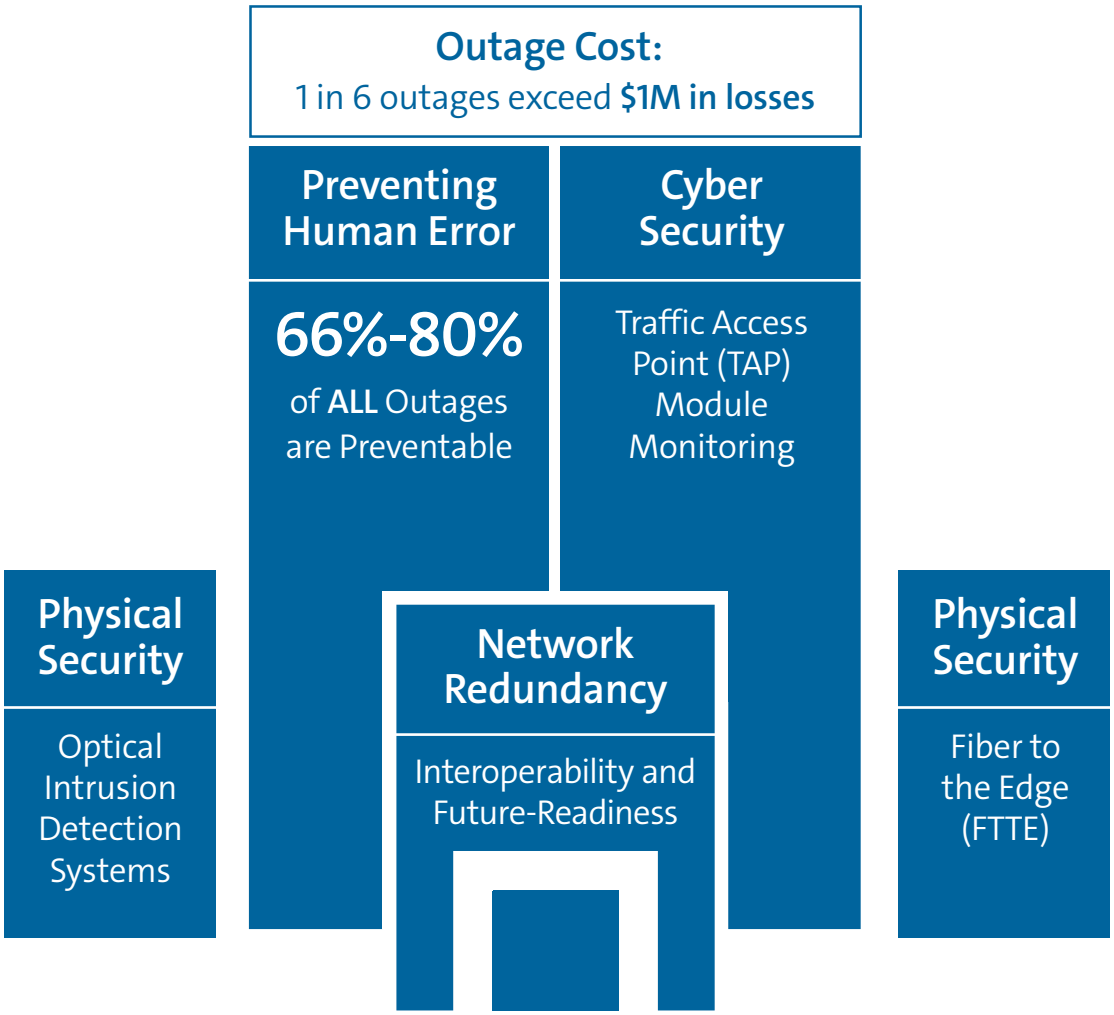
CORNING

# Don't Let Your Data Drop:

## Four Essential Considerations for Data Center Security




## Simply put, data centers are the engines behind much of modern society.

Maximizing their resiliency is vital for keeping the digital spaces we all enjoy up and running. If you're like me, you spend a lot of time watching streaming services or using social media to check up on loved ones—all of those rely on massive data centers. Downtime for the data centers behind these applications isn't only disruptive, it's also growing increasingly costly: **a recent survey** of IT and data center managers found that many outages cost between $100,000 and $1 million, and that one in six outages exceeded $1 million in losses.

Keeping data centers online requires a multifaceted proactive security plan that encompasses various potential points of failure, from redundancy planning to physical and cybersecurity measures, to prevention of human error. Here's how a modern fiber optic infrastructure can help data centers not only run their best today and into the future, but also facilitate a comprehensive security and uptime plan, as well.

## 1 Physical Security

Most people jump to cyber security when they think about safety; however, I think we too often neglect the physical element of data centers and their specific vulnerabilities. Fiber optic networks can lay the foundation for all manner of physical security measures to prevent intrusion. Security cameras must be placed at a multitude of points across a facility, particularly around its perimeter. For hyperscale centers with sprawling footprints, that can mean exceptionally long cable runs to connect these cameras back to the network, and fiber is often the most practical solution. It's also prudent to employ a battery of access systems along a facility's various entrances. Again, this requires extending connectivity across great distances to enable security checkpoints with badge readers and biometric access systems.

Beyond its ability to reach far-flung areas of a campus, fiber is also the most secure method for connecting perimeter security systems. Unlike copper cabling, fiber can be enhanced with **optical intrusion detection equipment** to monitor any disturbances in pathways up to 80 km in length. This can provide an extra layer of visibility into any efforts to tamper with cabling—whether by a bad actor or just an overzealous groundhog.

## 2 Cyber Security

Staying one step ahead of cyberattacks is a never-ending struggle; for data centers, where the stakes for breaches are astronomical, it's essential to implement as many safeguards as possible to thwart hackers before they can inflict damage.

Like physical security, keeping a data center's network safe requires maximizing visibility. This requires a sophisticated network monitoring system to track performance and raise alerts about possible threats. One method involves deploying equipment at the network switch. However, this approach can lead to cost overruns in the eventuality of network expansion—an upgrade from 1 Gb to 10 Gb, for example—would require a new transceiver.

Instead, the more economical, future-ready method is to deploy a **traffic access point (TAP) module** in line with the fiber. TAP modules work by splitting the signal on the network link to replicate the traffic without interrupting its transmission. The simultaneous copy of the signal is then sent to a monitoring center that can perform diagnostics and evaluate for irregular traffic that could indicate an intrusion.

Modern TAP modules carry numerous advantages over switch-level monitoring equipment. They're passive devices that require no power, and can be integrated into existed structured cabling, eliminating the need for extra rack space. They're also capable of handling up to 400 Gb of traffic, making them highly adaptable to network expansion.

## 3 Network Redundancy

Think of network redundancy like a backup tire. It is always there to support you if experience a flat tire. Imagine if you had a replacement tire that automatically activates once your first tire runs flat – that is network redundancy. It is a multilayered line of defense at any potential failure point in your system that enables your network to remain up and running if a failure occurs. The more redundancy you have, the less of a chance of network downtime.

Here's where smart planning and future-readiness can pay dividends. It's crucial to plan out a fiber infrastructure that can easily accommodate future expansion, so that no disruptive construction will be required down the road. From a service disruption point of view, it also means running multiple cable feeds into the data center for redundancy: you should always have an A and B network configuration, so there's no single point of failure in the cabling infrastructure or in the electronics.

Another important consideration in this planning is ensuring that the cabling and equipment used is both backward and forward compatible. Therefore, adjustments can be easily made and the system can adapt as needed. As Corning continues to make advancements to our EDGE™ product line, each new iteration retains compatibility with previous generations, allowing data centers to easily evolve with changing demands.

## 4 Preventing Human Error

Human error is an innate possibility, however in data centers, it's incredibly costly. According to some sources, mistakes among operators factor into some **66%-80%** of all data center outages. Today, as the tech industry continues to trudge forth through a shortage of skilled labor, the toll of missteps is only getting worse. Mistakes can happen in many ways, but the most common errors involve physical missteps—where a technician accidentally bumps a connector—and mental mistakes—where the wrong patch cord is unplugged. Both of these incidents can cause widespread disruptions, and are very easily avoidable through the use of modern solutions.

Corning's **EDGE™ Lockable Uniboot Jumpers** can prevent the connection from being accidentally dislodged. Additionally, our latest data center innovation, the **EDGE Distribution System** incorporates color coding to give technicians added assurance that they're unplugging the right cable. Corning also provides solutions and services to help data centers build out their network properly from beginning to end; these resources are particularly valuable for organizations that are experiencing skilled labor shortages. We also offer **preconnectorized cabling solutions** designed to take complexity out of the hands of installers and speed the process of scaling-up to meet the increasing data processing demand. Corning's systems engineers can also recommend cabling and network designs for customers during the planning phase, as well as technical and maintenance support down the line.

When it comes to fortifying data centers against security threats and unplanned downtime, I believe the best foundations are laid with fiber. By engineering facilities with the right fiber infrastructure, data centers will have the bandwidth and expandability to handle future growth with ease, along with unparalleled visibility into performance and threats.

*Content compiled from **The Signal Blog**.*

## Contact a Corning representative today

to learn how to increase network uptime and optimization for **multitenant data centers**, **enterprise/private data centers** and **hyperscale/cloud operations**.