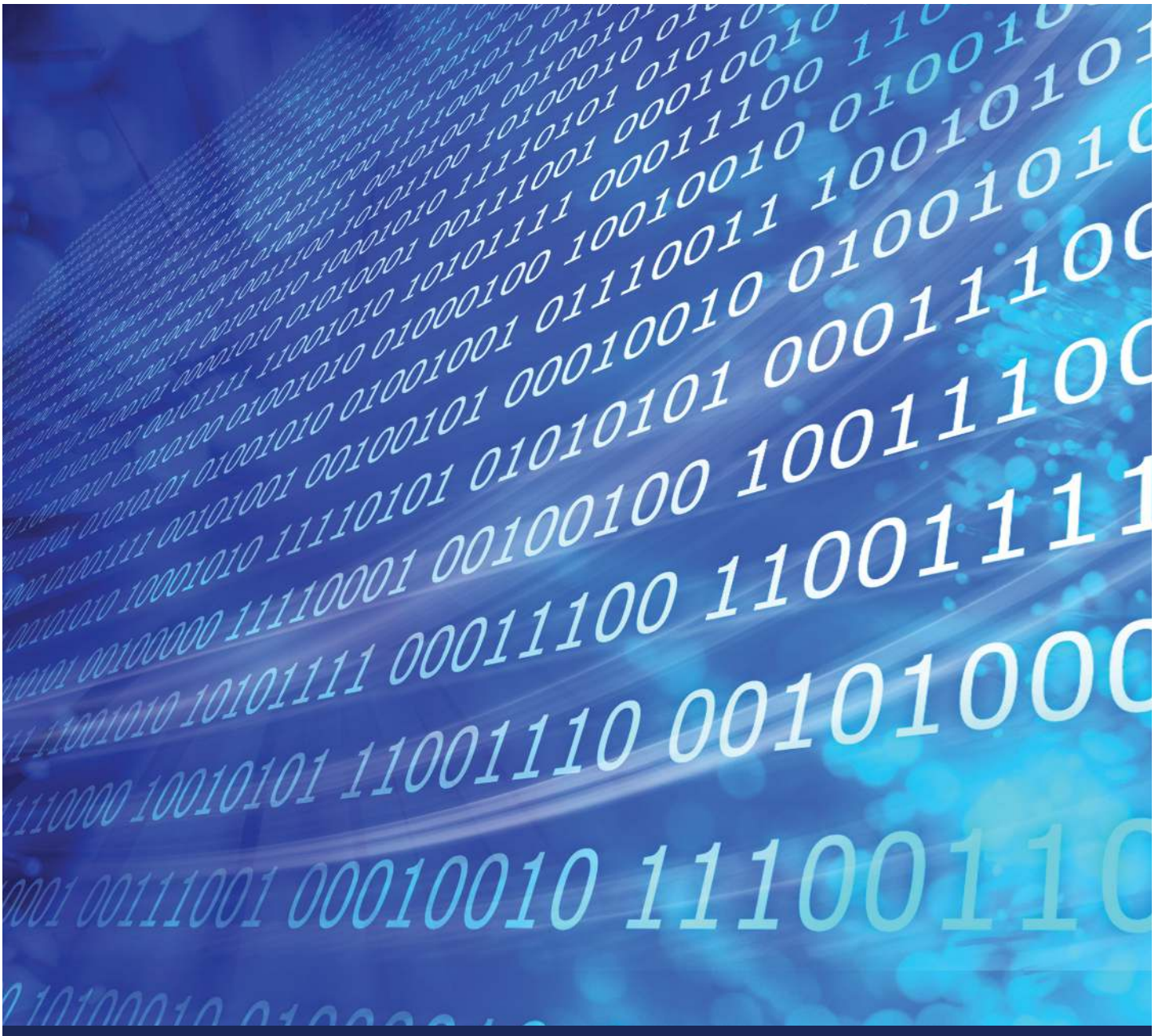
EXECUTIVE REPORT

CyrusOne

Defining Data Security

What you need to know about data security in a complex environment



Keeping data secure is a complex, multilayered process and a full-time job. Whether a company is in finance, legal, healthcare or technology, there exists a business and financial obligation to keep clients' sensitive information secure.

A recent study by PricewaterhouseCoopers states cybersecurity is a top priority for CEOs in the U.S. Having a multifaceted data protection plan and process in place is paramount to success. Accordingly, research shows companies are increasing theirinvestment in data security. Gartner predicts global IT security spending will growroughly 8% a year, to close to $80 billion in the next couple of years. Heightened levels of sensitivity and concern about data security come on the heels of recent major data breaches. While critical and necessary, data security is not every company's core expertise.

Many choose to look outside for assistance. Concerned with more than the present,data security is about anticipating future business needs and scaling solutions to meet those needs. Third-party data centers strategically blend online and offline security measures, including digital monitoring.

More companies are making data security a primary focus, developing effective plans to address issues beyond where to store the data and establishing clear guidelines for how to manage and monitor data.

Is Your Data Secure?

Data security is a seemingly simple question with a complicated answer. Recent and devastating company security breaches create more questions.

Whether storing data in an on-site or off-site data center, uninterruptable power andcooling, on-site monitoring of the facility, and redundant connectivity are critical 24/7 year-round.

The procedures data centers take to protect a company's sensitive business dataare extensive. Knowing what to look for in a data center provider and matching its security posture with a company's needs will best mitigate risk and offer the highest level of protection.

Physical Data Security

Executives and internal technology teams can take several critical steps to maintain peace of mind and ensure data remains secure, enabling them to focus on more strategic aspects of their core business.

Securing the facility in which a company's data and networks are housed begins with basic requirements. Physical data center security entails a comprehensive approach to keeping applications and networks safe in a facility offering the right levels of redundant power, cooling, backup and accessibility.

Most colocation service providers implement strict layered security measures to manage physical access within their data centers. Security personnel monitor all security cameras, guard building entrance and exit access points, and control keycard access throughout secured spaces.

Compliance is another essential component of physical security. Regardless of whether a company owns/manages its own data center or if they use a third-party provider, complying with current standards and regulations is critical. Important certifications and audits include ISO 27001, PCI and SSAE 18.

Securing All Points of Entry to Your Network

Staying one step ahead of cyberattackers and securing a network infrastructure is an ongoing challenge. Companies need to pay special attention to publicly available

methods of access to their network. Years ago this meant securing the perimeter of the network; now, however, with new bring-your-own-device (BYOD) deployments and widely accepted outsourced, cloud and access-anywhere technologies, companies need to be even more diligent in making sure all points of entry into their network are correctly secured.

News headlines prove there are a great number of threats still attacking the perimeter of company networks. Most attacks exploit a software limitation or other known bug. While external assaults certainly cause a lot of headaches and carry their fair share of problems, internal attacks, typically responsible for data leaks, are even more alarming. Based on a recent Gartner Magic Quadrant Report, security information and event management (SIEM) is a $1.6 billion market that continues to grow at double-digit rates.

It is important to remember that not everyone on your network can, or should, be trusted. A company wouldn't grant an employee from engineering access to accounting department files, just as a visitor would not have unrestricted, unsupervised access to any office at corporate headquarters. If physical separations and safeguards are so important, why do companies often allow network access without a second thought?

Installing corporate and guest networks and provisioning user access must be considered and implemented by the entire IT team. Establishing necessary segmentation between working groups and outside groups is important, as is placing checkpoints, logging and controls in place wherever different segments intersect.

Define from a business perspective exactly who needs access to what internal and external resources, document permissions, and ensure necessary controls are in place at the network level. Be willing to re-evaluate this framework constantly and make adjustments as necessary. Leveraging products that identify anomalies in inbound and outbound

traffic is important; being able to block irregularities goes even further in protecting the network. Designing and building out an infrastructure enabling this level of oversight is key to securing next-generation, always-available networks.

Tasked with protecting one of an organization's most important assets – data – IT infrastructure and managed service providers understand data access and security are mission-critical. Resiliency and redundancy are top priorities. Teams of highly trained professionals use robust technology to protect and monitor companies' networks. Additionally, data security experts are well-versed in the latest intrusion detection and protection tools.

Logical Data Security

Third-party data centers offer scalable solutions with a laser focus on efficiency, cost and performance.

Forbes recently posted a roundup of cloud computing fore-casts and market estimates through 2018 that points to continued growth in spending. Yet for many businesses, the decision about whether or not to move data to the cloud continues to present security concerns. Businesses must plan for and implement comprehensive measures to protect data against potential cloud-based security threats.

Working with trusted partners, companies can determine which cloud environment – public, private or hybrid – best meets their needs. Data center providers have the most comprehensive and thorough online data monitoring tools to keep data safe. Due to the gravity and breadth of threats in any cloud environment, partners must constantly refine their threat-detection process.

Security devices exist in many of today's data centers as well as in their clients' physical office spaces, providing data security wherever there are assets to protect. Regardless of configuration, reporting is shared between partners to deliver optimal data security and monitoring.

Alert Logic's "Cloud Security" report revealed that cloud hosting provider environments experienced significant increases in security attacks. The report also points to increases in brute-force attacks and vulnerability scans.

On-premises environments are still more likely to be attacked than cloud environments, but there has been a consistent increase in cloud attacks. As cloud adoption continues to accelerate, brute-force attacks – which increased in on-premises environments – have surged among cloud hosting providers, likely due to the increasing presence of "theft-worthy" data in the cloud.

– Alert Logic

An often overlooked component of logical data security is the impact of employees using personal devices for business. Many companies have BYOD policies and security patches, yet frequently exclude these devices. It is important to work with an outsourced IT team to enhance any BYOD policy to ensure compliance with othervirtual data protection policies and procedures.

Data security is a complex process. Building it correctly demands a constant focus onreliability and resiliency. Protecting data requires collaboration between internal IT staffand third-party providers to design, implement and build efficient solutions that deliver the highest levels of data protection.

Whether outsourcing data storage to an IT infrastructure and managed services provider for the first time, or revamping virtual security policies and procedures, it's imperative to plan for the worst and hope for the best. With cyberattacks on the rise, businesses face the unenviable task of protecting their current data and developing or obtaining a heightened security posture that is well-suited to handle the increased level of cyberattacks. Regardless of industry or current data protection configurations, companies require creative, cost-effective, long-term security solutions.

Is Your Data Secure?

Planning for "When," Not "What If"

Catastrophic natural events such as Superstorm Sandy and Hurricane Ike prove that when disaster strikes, recovery is often a slow process. Whether a power outage prevents access to a place of business or a network connection is down, the result can be lost time and lost data – both of which negatively impact bottom lines.

For businesses today, security is about more than making sure data is protected and remains accessible when natural disaster strikes. It is about making sure data is also secured against man-made threats, including software failures, hardware failures, electrical outages, employee security breaches and cyberattacks. Regardless of the nature of any interruption, companies need to know they can maintain near-100% uptime, while keeping clients satisfied and data and applications safe. An integrated, proactive approach to data security should align with corporate business planning.

Support from trained data security professionals and third-party providers enables companies to conduct risk assessments identifying likely and significant security threats. These professionals can also build new or update existing business continuity plans, ensuring staff are well-versed in how operations will shift should a data breach or natural disaster occur.

It is important to update and test business continuity plans, including disaster recovery strategies, on-site and off-site at least once every year. As businesses grow and evolve, so do associated data security needs.

The time to discover that the executive tasked with leading disaster recovery plan implementation has left the company is not when a disruption happens.

About CyrusOne

CyrusOne specializes in providing highly reliable, flexible and scalable enterprise data center colocation that meets the specific needs of customers across its broad portfolio of carrier-neutral data center facilities in the United States, Europe, Asia and Latin America. CyrusOne employs its Massively Modular® engineering and design approach to optimize design and construction materials sourcing and enable just-in-time data hall inventory to meet customer demand. The company engineers its facilities with redundant power technology, including an available 2N architecture.

CyrusOne customers can mix and match data centers to create their own production and/or disaster recovery platforms by combining facilities via the low-cost, robust interconnectivity provided by the CyrusOne National Internet Exchange (IX).

For more information contact us at 855-564-3198 or visit CyrusOne.com