charles
SCHWAB

Keys to a more secure data environment

Own your tomorrow®

A holistic approach to data infrastructure security

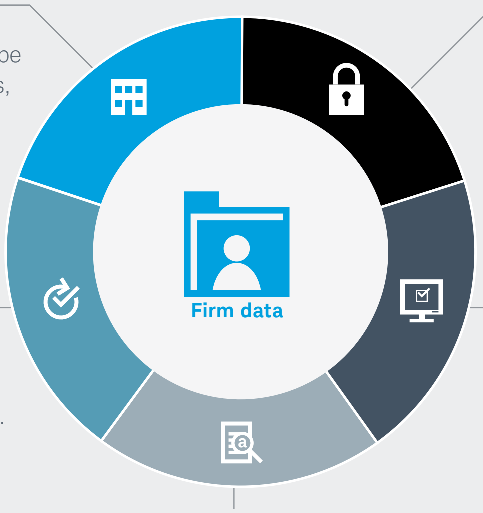
The current fraud and regulatory landscape makes it clear that every firm needs a comprehensive strategy for protecting their firm and their clients from the threat of cybercrime. Experiencing a cyberattack that leads to compromised data can dilute the trust your clients place in you and lead to both financial and reputational risk to you and your firm. But security is a large, multifaceted endeavor, and it can be challenging to step back and see the full picture. Firms need to be equipped to handle a range of potential threats—from natural disasters and technological failures to cyber- or real-world criminal activity. To do so requires a holistic approach to security infrastructure, with a clear understanding of the scope.

Whether reviewing a third-party provider's security plan or your own, it's important to examine these key categories together:

1. Physical safeguards
2. Network security
3. Application security
4. Capacity planning and reliability monitoring
5. Disaster recovery (DR) planning

Each of these factors is one part of a strong security infrastructure. Many firms have excellent safeguards in some areas but allocate fewer resources to others. To identify and eliminate gaps that could put your own firm at risk, it's important to understand the baseline security measures in each area.

Data infrastructure security at a glance:



Physical safeguards

Data centers—both primary and disaster recovery centers—should be protected against natural disasters, sabotage, and power outages.

Network security

Network configurations, encryption, antivirus software, intrusion detection, and regular testing help protect data from cyberattacks.

Disaster recovery planning

If a disaster event incapacitates a firm's primary data center, a secondary center with 100% redundancy can help provide seamless continuity and prevent data loss.

Application security

Application security helps ensure your data is protected over the Internet for cloud-based solutions such as employee-monitoring software.

Capacity planning and reliability monitoring

Even if firms can handle business needs today, it's important to ensure that no lapses in service, security, or data reliability will occur as the business grows or new functionality is added.

Physical safeguards

Hackers and data breaches make for high-profile news stories, and while cybersecurity is imperative, it's important not to overlook old-fashioned physical security. Without the right measures in place, data centers can easily be compromised—and all it takes is one break-in or power outage to disrupt business. Strong physical security can help keep business running as usual by accounting for these risks.

The most secure data centers feature strong perimeters, surveillance systems, and authentication-only access points.

At a minimum, a secure data center will have the following:

Camera security

Cameras should be located throughout the facility to monitor and record activity.

Security personnel

On-site staff provide additional protection against unauthorized entry 24 hours a day, 7 days a week.

Unmarked building

A low-profile building is a reduced target for criminal activity.

Uninterruptible power supply (UPS) systems

In the event of a power outage, UPS systems can provide 30 minutes of battery life under peak load—enough time to save files and prevent critical data loss.

Generators

Generators should have enough fuel stored to provide up to 48 hours of power in the event of a power outage. The data center should also have access to additional fuel, and cooling units should be in place to keep generators functioning properly.

Third-party security auditing

Physical security auditing by an independent firm can help identify gaps. SSAE 16 compliance can provide firms with recognized systems reporting.

Stringent policies and procedures

Policies limiting exposure of data to unauthorized people—such as those restricting visitor access and mobile devices—can help to maintain confidentiality.

Regular reviews

Physical safeguards should be reviewed regularly with the security, site, or operations manager.

Network protection

Firms located in close proximity to neighboring businesses (such as suites or in a strip mall) should protect their network from use by their neighbors.

What is SSAE 16 compliance?

The Statement on Standards for Attestation Engagements (SSAE) No. 16 is one of the current standards for reporting on service institutions. To become SSAE 16 compliant, data centers undergo a rigorous third-party audit to assess internal business procedures and IT controls.

Network security

Similar to how physical barriers in a data center protect its servers, network configurations, encryption, antivirus software, and regular testing protect its data from digital attacks.

The financial services industry, in particular, is a common target for cybercriminals and hackers. In fact, the threat of cyberattacks in the financial services sector has been rising. It's important to know that your firm has strong measures in place to guard against data breaches and denial-of-service (DoS) threats.

When evaluating network security measures, look at the following:

Firewall protection and intrusion detection

Firewalls and intrusion detection systems provide protection and visibility necessary to minimize the threat of security breaches.

Ongoing third-party network penetration testing

Infrastructure penetration simulates an external hacking threat—uncovering vulnerabilities and gaps in the network. This testing can help gauge how vulnerable the network is to both external and internal threats.

Antivirus software

Antivirus software should be active on all servers.

Security patches

Security patches help ensure systems always operate on the most current version of a software application. For software to stay up-to-date, these patches should be applied whenever necessary.

Encryption

All back-end file transfers should be encrypted using the latest industry standards.

Regular data scans

Data scans should be conducted at least once a week to help monitor for any unknown hacking situations.

Application security

Application security is an extension of network security, which has become increasingly important as more and more software applications become available over the Internet. The applications can include cloud-based compliance and employee-monitoring software.

When evaluating application security, look for the following standards:

Secure Sockets Layer (SSL) encryption

All data transferred between a user's browser and employee-monitoring software should be protected using SSL encryption.

Database encryption

Firms' sensitive personal information should be encrypted in their databases.

Application architecture

Applications should be built using industry-leading technology standards.

Single sign-on (SSO)

With an SSO authentication process, user access to multiple applications is granted via the firm's corporate directory. This process eliminates the need to authenticate separately for each application, which reduces the need for multiple IDs and passwords.

Third-party application penetration testing

Application penetration tests simulate an internal hacking situation, in which intruders have some privileges or inside information about the system but are attempting to go beyond the activities for which they've been authorized.

Open Web Application Security Project (OWASP)

Visit OWASP to find industry-leading standards for application security.

Vetting a third-party provider?
It may be practical for your firm to hire a third party to perform some of the auditing, monitoring, and testing needed to ensure your firm has a strong infrastructure. Use the **Vendor Due Diligence Sample Questionnaire** as an example of the types of questions to ask when vetting third-party providers.

Capacity planning and reliability monitoring

Capacity planning is a vital part of security. Even if a firm has the capacity to handle today's business needs, planning is necessary to ensure that client service can continue at the same level and that data can keep flowing as the business and client base grow.

But scalability alone is not a guarantee that data will remain reliable after growth. In order to ensure reliability as systems evolve, firms must conduct regular monitoring and testing—especially as they add new functions or applications.

Consider the following reliability standards:

Site access

Websites should be accessible 365 days per year, 24 hours a day—regardless of access point or traffic load.

Performance testing

Before launching any new function, performance testing can assess whether the system can accommodate the new features and increased load.

Reliability monitoring

Devices should be consistently monitored to help diagnose problems before they happen. Reliability monitoring can also help to identify errors quickly so that they can be repaired swiftly. Real-time dashboard tools can help analyze the overall health of critical websites.

Device redundancy

Redundancy for every device in a network helps ensure that if one device goes down, the system can continue to function.

Disaster recovery planning

No one can predict when disaster will strike—but everyone can take measures to prepare. Natural disasters, technological breakdowns, and crime all pose threats to the security of your data and that of your clients, making a DR plan essential to any firm.

In the event your primary data site is incapacitated, a secondary site can help provide seamless continuity and prevent data loss.

A DR site should always be ready to assume all critical functions of the primary site. For that reason, all the same security measures in place for the primary site—physical, network, application, capacity—should also be implemented in the DR environment.

As a best practice, the back-up data center should have the following:

Secure, low-risk location

DR sites should be located in a geographic region unlikely to be affected by natural disasters and far from the primary site. The same physical security measures that apply to the primary site should also apply to the DR site.

Server parity

A DR site should be equipped with the same number of servers as the primary site, which can help ensure 100% performance continuity in a failover event.

Regular data backup

The site is ready to assume primary function at any time—which means data should be frequently and regularly backed up from the primary site to the DR site.

Reliability testing

Any testing conducted at the primary site should also be conducted at the DR site to ensure reliability.

Business continuity plans (BCPs)

A DR plan is a vital component of keeping a firm's technology environment secure and its data flowing in the event of an emergency. In addition, a detailed BCP can help ensure critical resources are available and able to continue working in the event that access to the primary office or working facility is limited. BCPs should be tested annually.

AS Cybersecurity Resource Program

The current fraud and regulatory landscape makes it clear that every firm needs a comprehensive strategy for protecting their firm and their clients from the threat of cybercrime. And, as you've just learned, having a strong business continuity plan is an important component of any cybersecurity program.

Schwab Advisor Services™ has developed a program that delivers information, tools, and resources to help advisors:

- Understand the regulatory environment
- Develop, strengthen, and maintain their cybersecurity program
- Educate their employees on roles and responsibilities for protecting firm and client information
- Educate their clients on best practices for protecting information
- Understand Schwab's practices for protecting firm and client data

Our action-oriented methodology and resources will guide you through steps for enhancing data security at your firm and heighten awareness with your employees and clients.

Visit our online **Cybersecurity Resource Center** to learn more.

For informational purposes only. Neither Charles Schwab & Co., Inc. nor any of its affiliates or employees is responsible for any damages or other harm that might occur as a result of, or in spite of, use of any information, tools, resources, or processes described in these materials. Your firm alone is responsible for securing your systems and data, including compliance with all applicable laws, regulations, and regulatory guidance.

Schwab Advisor Services serves independent Registered Investment Advisors (RIAs) and includes the custody, trading, and support services of Schwab.

Independent investment advisors are not owned by, affiliated with, or supervised by Schwab.

charles SCHWAB

Own your tomorrow.