Six keys to a more secure data environment

June 2018

charles SCHWAB

Own your tomorrow®

A holistic approach to data infrastructure security

Compliance professionals know better than anyone how compromised data can lead to financial and reputational risk. 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. Doing so requires a holistic approach to security infrastructure and a clear understanding of the scope.

Whether you are reviewing a third-party provider's security plan or your own, you should examine these six key categories together:

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

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, you should understand the baseline security measures in each area. As industry standards intensify and client expectations rise, becoming SOC 2® Type II certified is one way you can address these vital areas of security.

Data security at a glance:

Physical safeguards

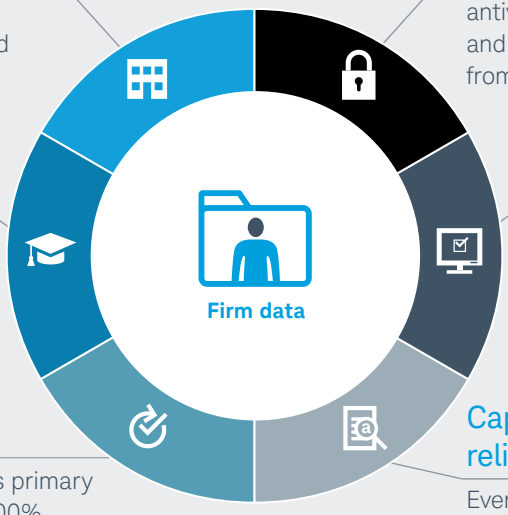
Data centers—both primary and disaster recovery centers—should be protected against natural disasters, sabotage, and power outages.

Network security

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

Employee training

A firm's employees introduce the potential for behavioral risk—intentional or not. Comprehensive training can help employees understand how the actions they take every day can help keep data safe.



Application security

Application-level security measures help ensure your data is protected for cloud-based solutions, such as employee-monitoring software.

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.

Capacity planning and reliability monitoring

Even if firms can handle business needs today, they should take care 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. 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 electricity 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. SOC 2 Type II compliance can provide firms with an independent view and review of controls within a standard practice.

Stringent policies and procedures
Policies reducing the exposure of data to unauthorized people, such as rules restricting visitor access and mobile devices, can help maintain confidentiality.

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

What is the SOC 2® Type II report?

SOC 2 Type II is quickly becoming the industry standard for data security. SOC 2 Type II compliance requires an annual examination by an independent auditor to confirm the design and effectiveness of the controls as they align to an organization's processes, based on the Trust Service Principles.*

The examination covers:

- Organization and management
- Communications
- Risk management and design implementation of controls
- Monitoring of controls
- Logical and physical access controls
- System operations
- Change management

*The Trust Service Principles, which SOC 2 is based upon, are modeled around four broad areas: policies, communications, procedures, and monitoring. Each of the principles have defined criteria (controls) that must be met to demonstrate adherence to the principles and produce an unqualified opinion (no significant exceptions found during the audit process).

Network security

Just as the physical barriers in a data center protect the servers, the network configurations, encryption, antivirus software, and regular testing protect the data.

The threat of cyberattacks in the financial services sector continues to rise as the industry remains a common target for cybercriminals and "hacktivists." It's important to know that you have strong measures in place not only to guard against data breaches and distributed denial-of-service (DDoS) threats, but also to keep your organization in regulatory good standing. Both the Financial Industry Regulatory Authority and the U.S. Securities and Exchange Commission identified cybersecurity as a 2018 exam priority.

When you evaluate network security measures, look at the following:

Firewall protection and intrusion detection

Firewalls and intrusion detection systems provide the 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 that 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.

File transfers

All file transfers should be encrypted using industry standards.

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.

Regular data scans

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

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.

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. 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

Conducting performance testing before launching any new function can help you 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 the system can continue to function if one device goes down.

Audit trails

Trace and find who did what when.

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 compliance program.

If 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 backup 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 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 server capacity as the primary site, which can help ensure 100% performance continuity in a failover event.

Regular data backup

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

To learn more about building your plan, read *Building a Strong Business Continuity Plan*.

Employee training

Even the strongest data security infrastructure can be compromised by human behavior. In fact, about two-thirds of all data breaches begin with a compromised internal user. When employees are not aware of basic security practices, they can unknowingly make decisions that put sensitive data at risk. But, with the right training, your employees can become one of your strongest defenses.

At a minimum, a strong information security training program for employees should cover:

Being email savvy

Employees should know to be suspicious of emails that come from an unknown sender—and of emails from trusted sources that sound "off," contain unusual information requests, or are full of errors (this could be a sign of phishing). They should also be aware of the dangers of sending sensitive data by email.

Reporting issues or concerns

Be sure employees know how to reach you, IT, and any other key leaders in case of a concern. Employees should know to get in touch with you about a security breach before putting anything in writing. Sharing your post-breach plans can help keep everyone aligned.

Creating and maintaining secure passwords

Weak, default, or stolen employee passwords are often the weakest link. Depending on your company's policies, consider passphrases or separate passwords for each account, or establish complexity based on the criticality of the system. Remember: It's about length—not complexity.

Keeping operating systems and programs up-to-date

Employees should be aware of the risks of out-of-date software. Keeping software up-to-date helps reduce the possibility that employees' systems have exposed vulnerabilities. Further, employees need to understand how downloading unauthorized software can open your organization to risk.

Stop. Think. Connect.

Looking for even more cybersecurity best practices and tips? Homeland Security's Stop.Think.Connect. Toolkit offers the latest resources for all segments of the community—including business.

Explore the toolkit today:
www.dhs.gov/stopthinkconnect-toolkit

Vetting a third-party provider? What you should ask*

The best way to evaluate a current or potential third-party provider's data security and reliability is to arm yourself with information. While a SOC 2® Type II audit will review third-party data security, you can also conduct an internal audit. Start by asking questions intended to uncover strengths or weaknesses in each of the six key data security categories:

Physical safeguards

- ☐ What type of physical security is in place for your data center and your business?
- ☐ Do you have video surveillance throughout your data centers?
- ☐ Do you have on-site security personnel to protect against unauthorized entry 24/7?
- ☐ Are your data centers located in unmarked, nondescript buildings?
- ☐ In the event of a power outage, do you have an uninterruptable power supply (UPS) system that can provide battery life for at least 30 minutes?
- ☐ Do your data centers have generators that can provide additional power during a power outage?
- ☐ Do you use an independent, third-party auditing firm to help test and identify security gaps?
- ☐ Do you have stringent policies and procedures in place to reduce exposure of data to unauthorized people?
- ☐ Do you conduct regular reviews of physical safeguards?

Network security

- ☐ What type of firewalls are in place to protect data?
- ☐ Do you have an intrusion detection system to give visibility to potential data security breaches?
- ☐ What type of infrastructure penetration testing is in place to gauge threats posed by both outsiders and those with inside information about the system?
- ☐ Is antivirus software active on all servers?
- ☐ Are security patches in place to help ensure that systems always operate on the most current version of a software application?
- ☐ Are back-end file transfers encrypted using the latest industry standards?

Application security

- ☐ Are data transfers between a user's browser and the application protected using Secure Sockets Layer (SSL) encryption?
- ☐ How do you test new functionality prior to launch?
- ☐ What controls are in place for deployment?
- ☐ Do you perform ongoing scanning for vulnerabilities? If so, how frequently?
- ☐ How do you protect the firm's sensitive personal information?
- ☐ Do you allow for a single-sign-on (SSO) authentication process?
- ☐ Is application penetration testing used to simulate internal hacking situations? If so, how frequently?

Capacity planning and reliability monitoring

- ☐ What is your capacity to grow within the next ___ years?
- ☐ What is your capacity planning process?
- ☐ How do you test new functionality prior to launch?
- ☐ Do you have real-time threshold monitoring?
- ☐ What measures are in place to help eliminate single points of failure?

Disaster recovery (DR) planning

- ☐ Do you have a DR plan in place?
- ☐ How often is the plan tested, and what are the most recent results?
- ☐ What is the scope of the recovery test?
- ☐ Do you have a secondary site/backup data center?
- ☐ Is your backup data center in a geographic region that is unlikely to be affected by a natural disaster?
- ☐ Is your DR site equipped with the same number of servers as the primary site to help ensure 100% performance continuity?
- ☐ Is your backup data center backed up regularly and ready to assume primary function at any time?
- ☐ Does your DR site contain the same security measures as your primary site to help ensure data security?

Business continuity plans (BCPs)

- ☐ Do you test your BCP, and if so, how often?
- ☐ What does the test cover? (e.g., pandemic, loss of building)
- ☐ What are the key elements of your incidence response plan?
- ☐ Have you invoked your BCP in the last 12 months?

Data loss prevention

- ☐ Can data be downloaded onto laptops?
- ☐ Do you have a data classification policy?
- ☐ Do you have an acceptable use policy?
- ☐ Do you conduct a periodic risk assessment on your vendors?
- ☐ Does the firm have a process to manage IT assets?
- ☐ Does the firm leverage industry standards for distributed denial-of-service (DDoS) intrusion detection?

Employee training

- ☐ Is data security part of your standard employee training?
- ☐ Are employees regularly required to change their passwords?
- ☐ What measures are in place to ensure that employees keep their operating systems and programs up-to-date?

*The above is not an extensive list of questions. Each situation will require different levels of due diligence.

Compliance Solutions prioritizes data security

With the full security commitment of The Charles Schwab Corporation behind us, we at Compliance Solutions put the security of your data first. Schwab Compliance Technologies® is one of the only employee-monitoring technology providers to regularly complete a SOC 2® Type II report. To help keep our clients' data secure, we conduct regular third-party penetration testing and weekly security scans, as well as annual business continuity and DR testing. We also employ a structured software development life cycle and code reviews to ensure integrity and security in our software. Our production servers are hosted by Rackspace, a global leader in managed security.

In addition, we've made significant technology investments to guard our clients' data on even greater levels. Some of the most recent upgrades to our system include:

- Enhanced firewall that provides an industry-strength Layer 7 protection to the application platform
- Increased primary site capacity
- Increased DR site capacity—our DR site offers 100% capacity
- Enhanced monitoring of infrastructure and application components to better evaluate the overall health of our system
- Redundancy throughout every layer of technology to provide for transparent failover and recovery

These investments, along with those we will continue to make in the future, are all part of our commitment to data security and reliability for our clients—one more way we help them protect their employees and their reputations.

About Compliance Solutions

Taking ownership of compliance means staying ahead of the regulatory landscape, seeing the big picture, and maintaining control. But it doesn't mean doing it on your own. Compliance Solutions' employee-monitoring offer includes Schwab Designated Brokerage Services™, cloud-based employee-monitoring software from Schwab Compliance Technologies, and a wide range of financial products and services for employees. These solutions can help you proactively manage compliance, promote a positive employee experience, build long-term value across your business, and instill trust with clients.

Learn more

Interested in learning more about Compliance Solutions? Contact us today.

877-456-0777

Talk to your Relationship Manager

schwab.com/compliancesolutions

Neither Schwab nor Schwab Compliance Technologies, Inc. provides specific individualized legal or compliance advice. Where such advice is necessary or appropriate, please consult your own legal and/or compliance counsel.

Compliance Solutions is comprised of Schwab Designated Brokerage Services (DBS), a division of Charles Schwab & Co., Inc. ("Schwab"), and Schwab Compliance Technologies, Inc. ("SchwabCT"), formerly Compliance11, Inc. Schwab Designated Brokerage Services provides brokerage solutions for corporate clients who monitor their employees' securities activity. SchwabCT provides technology solutions for corporate clients to help facilitate their compliance technology program implementation. Schwab Compliance Technologies, Inc. and Charles Schwab & Co., Inc. are separate but affiliated entities, and each is a subsidiary of The Charles Schwab Corporation.

Brokerage Products: Not FDIC-Insured ▪ No Bank Guarantee ▪ May Lose Value

The Charles Schwab Corporation provides a full range of securities brokerage, banking, money management, and financial advisory services through its operating subsidiaries. Its broker-dealer subsidiary, Charles Schwab & Co., Inc. offers investment services and products. Its banking subsidiary, Charles Schwab Bank (member FDIC and an Equal Housing Lender), provides deposit and lending services and products.

Charles Schwab & Co., Inc., 211 Main Street, San Francisco, CA 94105

©2018 Charles Schwab & Co., Inc. All rights reserved. Member SIPC. AHA (0518-8487) MKT82117-03 (06/18)
00209946

charles SCHWAB

Own your tomorrow®