Keeping Our Client Data Secure

At Cohen & Company, we understand how important it is that our clients trust in our knowledge and services.

Part of building that trust is ensuring their data, as well as our own, is kept confidential and secure. We take that responsibility seriously and have architected a broad range of strategic technologies and processes to safely and effectively deliver secure business solutions.

In a continually evolving technology landscape, it is more important than ever to establish a security program than can flex and adapt quickly as new risks or threats are identified. As such, Cohen & Company has developed an approach to managing our security posture based on the concepts of continuous improvement and collective accountability. We never rest on the success of the past or view information security as someone else's issue, but instead are constantly evaluating what else we can do as a firm and as individuals to keep our clients' information safe. Further, our overlapping layers of protection increase our ability to identify and stop new threats while minimizing the chance of a single point of failure creating unacceptable risk exposure.

Administrative Safeguards

While most people associate information security with technical defenses like firewalls and virus scanning tools, Cohen & Company believes that technical defenses will not be effective unless supported by a robust set of policies and processes, including:

- Defined information security and acceptable use policies refreshed at least annually
- A firmwide Risk Management Council, which includes information security as a standing agenda item
- Monthly security awareness training required for everyone within Cohen & Company
- Phishing prevention program, including monthly testing, reporting tools and proactive purging of suspect messages
- Security consulting during application design and security reviews throughout the development process
- Robust incident management processes, which include assessment, remediation and communication expectations
- Defined third-party security due diligence required prior to conducting business
- Continuous monitoring of the firm's networks, systems and applications for suspicious activity
- Vulnerability and penetration testing using third-party tools and experts to help identify potential risks to our infrastructure or operations, and to remedy any issues

Cohen & Co®

Behind the Strategy

Our approach covers physical, data, network and computer systems, applications, change management and incident response. The guiding rule behind our security architecture is that all our data is confidential and private. Since the firm's information technology environment is designed to enable users to access data anytime and anywhere on approved devices, one of our primary design principles and policies is that we encrypt all confidential and electronic data.

We follow best practices and subscribe to the highest standards requiring that companies have comprehensive information security programs in place. We use the Hitech standard as a benchmark because it establishes a comprehensive and secure framework built on NIST (National Institute of Standards and Technology) best practices, which encompass the various regulations to which we adhere. Hitech is designed to minimize risk and protect sensitive information, such as financial or health information. Combined with policies, guidelines and design principles, this provides a full spectrum security and risk management approach.

Security threats continue to grow in sophistication, and strong defenses are needed. We recognize that partnering with the strongest security solution and service providers allows us to maintain the most robust security position today and in the future.

Technical Safeguards

Cohen & Company's Technology Services team employs an array of technical safeguards and tools that protect the firm's infrastructure and applications from cybersecurity threats, such as malware, viruses and other attacks. In addition to having a certified Tier III external data center, we use a number of layers to address risks, including firewalls, email filtering, endpoint protection, content filtering and mobile device management. The operating system features and third party tools we employ allow us to continually monitor our networks and systems to identify and diagnose problems, and automate the inventory of firm computer systems. In addition, we perform intrusion detection at external access points, inspect traffic for known sites and suspicious behavior, and perform automated vulnerability and penetration scans.

Physical Safeguards

At Cohen & Company, we understand the need to add physical protection to our robust digital safeguards to address the risks of information being physically lost or stolen. As with any security measure, there is overlap. For example, encryption is a key component of both technical and physical safeguards. The fact that laptops, USB drives, tablets and cell phones are fully encrypted provides protection against data loss if one of these devices is lost or stolen. Likewise, following strict data wiping protocols prior to disposal of laptops prevents "bad actors" from accessing data through recycled equipment.

In addition to device management, our physical safeguards extend to access controls within our physical offices:

- Access to office space is controlled by locked doors or the presence of a receptionist.
- Keycard access is used across all offices for employees and is monitored via video surveillance.
- Office policy calls for a firm representative to supervise any visitors; visitors are not permitted in a firm facility unaccompanied.
- We keep our data servers in controlled areas that prohibit access, except to authorized personnel.

Disaster Recovery and Business Continuity

To minimize service interruption due to hardware failure, natural disaster or other catastrophe, Cohen & Company has implemented a multi-faceted disaster recovery and business continuity program, which includes the following measures:

- Creating a high availability and resilient environment where systems are designed to eliminate single points of failure for fast recovery. All production data servers employ redundant arrays of independent disks (RAID). The firm has 100% server virtualization and is configured in an N+1 topology for critical systems. We maintain a private high speed fiber MPLS network, which provides enhanced availability. As a backup network, all offices have diverse internet connections that can support VPN access in the event of a network outage.
- Testing our disaster recovery procedures at least annually to ensure both our technology and our people are prepared in the event of an emergency. We also test the fundamental technology component of our business continuity plan daily, as our people leverage a hybrid work model that supports work in remote locations.
- Ensuring minimal data loss and service disruption by replicating firm data and systems to a secondary, off-site data center.

It starts with a conversation

We would be happy to answer any additional questions about how we're safeguarding information. Contact our chief information officer to learn more.

Kevin Sexton, CSM
Chief Information Officer
216.774.1250
ksexton@cohencpa.com