CYBERSECURITY REGULATIONS AND THREAT PREVENTION

NorthStar Financial Services Group, LLC (NorthStar), is parent company to CLS Investments, LLC (CLS). NorthStar developed this content in an effort to provide a comprehensive understanding of the growing malware threat, how NorthStar and its subsidiaries are protected, and the means by which NorthStar protects its clients.

Advisors who partner with CLS have peace of mind that through our parent company, NorthStar, CLS is actively adhering to the SEC's cybersecurity regulations and proactively enhancing our cybersecurity capabilities.

A cyberattack is any type of malicious maneuver that attempts to steal, alter, or destroy a specific target by hacking into a susceptible computer system, network, infrastructure, or device.

Research shows that 10% of cyberattacks are against financial services and insurance organizations, most of which discover they've been attacked via notifications from government agencies an average of 320 days later. Currently, Microsoft Windows is the most targeted system for compromise. Phishing – an attempt to steal sensitive information such as usernames, passwords, and credit card information through fraudulent emails – is the number one threat to financial institutions. And, around 63% of data breaches are due to weak, default, or stolen passwords. With the "internet of things" (the billions of devices that connect to the internet) exceeding the human population in 2017, organizations are even more exposed to cyberattacks, as most critical infrastructure wasn't designed for this increasingly interconnected world.

In 2014, the Securities and Exchange Commission's (SEC) Office of Compliance Inspections and Examinations (OCIE) began examining for cybersecurity compliance procedures and controls as part of their National Exam Program for SEC-regulated financial institutions. The SEC's formal jurisdiction over cybersecurity is directly focused on the integrity of market systems, customer data protection, and disclosure of material information. In April 2015, the SEC issued guidance stating that investment advisors' and broker-dealers' failure to implement adequate cybersecurity protections could be a violation of regulatory requirements. This guidance represented the SEC's first set of recommendations about what firms should do to provide adequate cybersecurity. It underscored the critical need for investment companies, broker-dealers, and investment advisors to review their cybersecurity. Following is a summary of the SEC's primary expectations for the firms under its jurisdiction.

Understand access rights and controls	Firms should know who their users are and how they're accessing their systems. The guidelines clearly state that the SEC expects firms to have basic controls in place to prevent unauthorized systems access. This includes tracking user credentials and implementing authentication methods to lessen the risk of a data breach by an individual.
Data loss prevention	Firms must protect data transferred outside their walls by clearly understanding how their staff transmits data, such as email attachments, and by monitoring the volume of data being transmitted. They should also track the same type of information for third parties, like any email programs or advisor technology software they use.
Vendor management	Since a firm is responsible for understanding how its clients' data is handled no matter who is doing the handling, the firm is responsible for managing its vendors accordingly. The SEC has the authority to access firm contracts and its due diligence for monitoring and overseeing the processes its vendors use when handling data.
Established policies for data breaches	Firms should have detailed, written processes in place so advisors know what to do in the case of a data breach. The SEC expects to see established policies and procedures, including assessments of possible vulnerabilities.
Training	Firm employees must all be regularly trained on firm policies regarding cybersecurity and understand the protocol should a risk or breech be identified.

Likewise, the Financial Industry Regulatory Authority (FINRA), which is monitored by the SEC and sanctioned to enforce its rules and regulations, called cybersecurity "one of the most significant risks" firms face. It established cybersecurity priorities in 2017 that include a focus on firms' data lost prevention and vendor relationship management policies.

Though NorthStar already had extensive cybersecurity strategies in place, we took this additional guidance seriously, as ongoing protection of our clients' assets is critically important. At NorthStar, before any computer traffic enters the network, it passes through a series of hardware devices and software that closely inspects all bits and bytes for malicious content. Based on very complex and sophisticated rules, logic, and algorithms, traffic is either blocked outright, quarantined for review, or allowed onto the network. However, even with these tools in place, it is possible for new variants of malware to evolve and make it past. If something does slip through our perimeter defenses, NorthStar has tools on servers, desktop PCs, and laptops to contain and mitigate any compromise. These tools add an additional layer of protection to detect, prevent, quarantine, and clean malicious content from endpoint devices, such as PCs, laptops, and smart phones.

NorthStar's portfolio accounting subsidiary, Orion Advisor Services, which powers the back office of CLS Investments, NorthStar's professional money management arm, is also hyper-focused on securing data from digital threats. Orion, which is SSAE18 Type II audited and ISO 27001:2013 certified (along with all of NorthStar), provides advisors an on-demand record of who has access to their portfolio accounting system. Advisors also have full rights management, so they can assign permissions as needed and delete users immediately whenever necessary. Additionally, all data that advisors transmit to Orion goes through a proprietary secure email system, removing the potential for interception. Other account security methods and options include dual authentication of all our website entities and text messaging updates.

NorthStar also utilizes encrypted servers and physical redundancy to eliminate the risk of data loss. Our recovery and restoration program is designed to resume operations and critical systems as quickly as possible. To facilitate recovery, NorthStar has implemented alternate work sites and remote technologies allowing employees to resume critical operations and making data continuously accessible to our clients even in the event of a power loss. NorthStar's multiple geographically dispersed state-of-the-art data centers are equipped with mirroring and replication technologies, allowing for efficient fail-over recovery of critical systems and complete resumption of business.

A minimum of four times per year, NorthStar's information technology division conducts disaster recovery testing during which they follow their activation procedures to enable critical technology systems and infrastructure. Designated testers then use predefined, web-based surveys that guide them through business-critical tests.

In sum, NorthStar takes cybersecurity and the trust our clients put in us to safeguard their assets and information extremely seriously. We are committed to investing the time, talent, and technical resources necessary to ensure the safety of investors' financial data, as well as the continuity of our partners' business operations.

What is ISO 27001 Certification?

NorthStar and its subsidiaries have adopted an **Information Security Management System (ISMS),** which complies with ISO/IEC 27001:2013. Recognized as the highest security standard in the technology industry, the ISO 27001 certification verifies that an organization possesses the required internal controls to operate, monitor, and maintain an ISMS that meets international guidelines.

NorthStar's security tools include:

- **Secure Email Gateway.** Searches all inbound emails for malicious attachments and embedded links that could take users to malicious sites. If discovered, the software quarantines the emails for review or outright deletes them if known to be malicious.
- **Intrusion Detection/Intrusion Prevention Systems (IDS/IPS).** Inspect network traffic at a very low level (bits and bytes). Upon detection of suspicious content, these systems automatically block it before it can enter NorthStar's systems. In addition, they filter out traffic from specific geographical locations known to be the source of malware (i.e. Russia, Iran, etc.).
- **Advanced Network-based Endpoint Protection.** Scans for and detects attacks and malicious network packets, as well as command and control communications (when malware communicates back to a home base for additional attack code or content).
- **Web Filtering.** Blocks access to sites with known malicious content. NorthStar's web filtering software is actively updated, so users are automatically blocked from accessing any site that is registered or identified as being able to spread malicious content.
- **Advanced Endpoint Protection.** Works similarly to and in conjunction with NorthStar's Advanced Network-based Endpoint Protection, but on the PC level instead of the network level.
- **Anti-Virus Software.** Actively scans and monitors traffic to and from each PC to detect malicious software. Also conducts traditional local PC anti-virus scans to detect viruses that might be stored, but not active, on the hard drive.
- **Log Collection.** Collects and analyzes PC, server, and network logs looking for questionable activity *within* internal networks. Correlates all log activity and alerts in real time on passable indicators of compromise (IOC).
- **Endpoint Data Loss Prevention (DLP).** Blocks access to external devices, such as flash drives, DVDs and CDs, to prevent data from being takes offsite. It also prevents executables from being ran from external devices on computers and laptops to prevent the installation of unauthorized software (which is strictly forbidden in our Employee Policy Manual).
- **Data Recovery Tools.** Can be used to quickly recover systems and data if such an attack was successful and original files needed to be restored.

2930-CLS-9/7/2017