A GUIDE TO THE NEW YORK DEPARTMENT OF FINANCIAL SERVICES CYBERSECURITY REQUIREMENTS (23 NYCRR 500)

Brite People.
Brite Solutions.
Brite

A GUIDE TO THE NEW YORK DEPARTMENT OF FINANCIAL SERVICES CYBERSECURITY REQUIREMENTS (23 NYCRR 500)

NYS DFS Cybersecurity Regulation 23 NYCRR 500 is a marathon, not a sprint. You may need to sprint to compliance on for the first deadline on August 28, 2017, but Brite will be your training partner for the entity of your compliance journey to ensure you cross the finish line by the March 1, 2019 date. this ebook is to be used as a guide to assist each step of the way.

CYBERSECURITY POLICY

What this is:

Each institute must implement and maintain a written cybersecurity policy that sets forth policies and procedures for the protection of its information systems and nonpublic information stored on its information systems and must be approved by a Senior Officer, the institute's board of director or equivalent governing body. The cyber security policy shall be based on the institute's risk assessment and address the following areas:

- Information security
- Data governance and classification
- Asset inventory and device management
- Access controls and identity management
- Business continuity and disaster recovery planning and resources
- Systems operations and availability concerns
- Systems and network security
- Systems and network monitoring
- Systems and application development and quality assurance
- Physical security and environmental controls
- Customer data privacy
- Vendor and Third Party Service Provider management
- Risk assessment
- Incident response

Why is this important:

A formal security plan ensures all critical aspects of a secure organization are addressed. A formally documented security plan can be reviewed and strategically modified.

How to become compliant:

Scroll through each section to learn how to individually address. Need guidance going through the process? Contact Brite and one of our representatives will assist you in evaluating you current security structure and make suggestions of how to move forward.

PENETRATION TESTING AND VULNERABILITY ASSESSMENTS

What this is:

Penetration testing is the practice of an organization attacking its own IT systems, just as an attacker would, in order to uncover active security gaps on your network. Penetration testing is conducted in a way that allows organizations to safely simulate these attacks, so they can discover the organization's actual vulnerabilities – whether within technologies, people, or processes – without taking down the network.

Why is this important:

If a company does not know what their security weaknesses are, it is impossible to fix them. Continuous penetration and vulnerability testing provides a company with insight

How to become compliant:

Rapid7 allows an organization to prioritize your vulnerabilities by likelihood of use by an attacker, discovered through penetration testing, ensuring you always fix the most dangerous issues first. Organizations can easily automate the entire vulnerability management process from scanning to report distribution, and set up dynamic asset groups with granular filters to ensure that team members get only the information relevant to them. Use live assessment and dynamic dashboards to get a constant scoreboard for how the program is working.

Tenable brings clarity to your security and compliance posture through a fresh, asset-based approach that accurately tracks your resources and vulnerabilities while accommodating dynamic assets like cloud and containers. Tenable.io maximizes visibility and insight and effectively prioritizes your vulnerabilities while seamlessly integrating into your environment.

BriteProtect brings our team of certified security engineers to work closely with you to understand your business requirements, identify the infrastructure and applications that will be in scope for the penetration test, and to schedule the 4 days of comprehensive testing. We will then simulate real-world attacks against the in-scope assets using best of breed open source and proprietary tools with the latest threat intelligence. Any identified risks and vulnerabilities will be documented and our security engineers will review the findings with your team and provide guidance on how to remediate the vulnerabilities.

AUDIT TRAIL

What this is:

Every institute must securely maintain the records that will allow them to reconstruct material financial transactions sufficient to support normal operations and include audit trails designed to detect and respond to cybersecurity events that are likely to harm or disrupt any materials relevant to operations for 5 years.

Why is this important:

Data breaches happen. With a proper audit trail, they can be remediated in a timely manner and business can resume as quickly as possible.

How to become compliant:

BriteProtect takes away the hassle, and much of the cost, associated with running a SIEM. Through our service Brite will tune the system to reduce noise, provide 24/7 monitoring of alerts and notify an organization of medium and high priority alerts within a guaranteed SLA. Now an organization's valuable IT resources can focus on your strategic projects and priority incidents.

Fasoo Enterprise DRM protects information itself persistently whether it is stored, being used, being transmitted or even after transmission, throughout the entire document lifecycle. This is the only complete and effective solution that protects you against unwanted information leaks from anyone.

Varonis DatAdvantage enables organizations to remove the risks associated with file permissions and auditing. Easily prove to regulators that IT controls are stringent and manage user

permissions efficiently, so the right people, and only the right people, have access to a company's data.

Check Point SandBlast Agent provides actionable forensics from continuously collected data on user systems to reveal a comprehensive view of the attack flow. This Accelerates remediation by empowering security teams with full understanding of root cause, entry points and scope of damage.

ACCESS PRIVILEGES

What this is:

Every institute must limit user access privileges to Information Systems that provide access to Nonpublic Information and shall periodically review such access privileges.

Why is this important:

Privileged account users have access to a great deal of critical information. When one of those privileged accounts are compromised, so is all of a company's critical data. By utilizing sophisticated privileged account management tactics, the risk of compromised credentials is greatly decreased.

How to become compliant:

CyberArk is the trusted expert in privileged account security. Designed from the ground up with a focus on security, CyberArk has developed a powerful, modular technology platform that provides the industry's most comprehensive Privileged Account Security Solution. Each product can be managed independently or combined for a cohesive and complete solution for operating systems, databases, applications, hypervisors, network devices, security appliances and more. The solution is designed for on premise, hybrid cloud and OT/SCADA environments.

HID is a fully CJIS Advanced Authentication compliant solution, assists organizations satisfy HIPAA, HITECH, EPCS, Positive ID, and PCI-DSS requirements; while at the same time makes lives easier for end-users by streamlining authentication processes and reducing the amount of passwords users have to enter and manage on a daily basis. HID does all of this and significantly increases the level of security throughout the organization.

RISK ASSESSMENTS

What this is:

Every institute shall conduct a periodic risk assessment, in accordance with written policies and procedures, of their information systems to guide the design of their cybersecurity program. Risk assessment should review information relevant to the security of information systems, nonpublic information or business operations. The risk assessment results should guide revisions of controls to respond to technological developments and evolving threats.

Why is this important:
Cyber threats change at an alarmingly quick rate. Without frequent risk assessments an organization will become vulnerable to the latest threats. Periodic risk assessments will expose potential problems for an organization before a breach occurs.

How to become compliant:
BriteAsess is a third party to perform periodic risk assessments. BriteAsess utilizes tools from multiple vendors to give companies a wholesome look at where potential risks in a network are. As a third party, BriteAsess brings an unbiased view into an organization and can help create a plan to better secure networks.

BriteProtect provides external vulnerability scans are scheduled through the Vulnerability Assessment portal. When the scans are executed our scanning infrastructure assesses the hosts identified in the scan criteria against our threat intelligence and signatures in order to identify any existing threats, vulnerabilities or weaknesses. The results are then recorded in our solution and available via the Vulnerability Assessment portal so that you can review remediation steps and take any necessary actions. Upon remediating you can rescan the hosts to determine the status of your security posture.

Rapid7 allows companies to prioritize risk by likelihood of use by an attacker, discovered through penetration testing, ensuring the most dangerous issues are fixed first. The entire vulnerability management process can be automated from scanning to report distribution, and set up dynamic asset groups with granular filters to ensure that team members get only the information relevant to them. Use live assessment and dynamic dashboards to get a constant scoreboard for how the penetration testing program is working.

CYBERSECURITY PERSONNEL AND INTELLIGENCE

What this is:
Either a qualified cyber security employee of the finical institute, an affiliate or third party security service provider must perform or oversee the performance of the core cybersecurity functions, which include those previously stated in the Cybersecurity Policy and maintain sufficient knowledge of current trends and training of how to address threats.

Why is this important:
No matter how much we automate the cyber security world, we will always need the human touch. An organization need knowledgeable people running its cybersecurity program for it to be successful.

How to become compliant:
BriteStar is a comprehensive manged IT service that helps companies protect and manage IT Infrastructures through a superior combination of people, process and technology. Let Brite's MSP support your organization and put our over 20 years of experience to work. From Frontline IT help desk to proactive support and strategic recommendations, BriteStar is the service for you.

Invest in Personal – People are the core of an organization. By having good hiring practices and encouraging continuous education, finical institute will maintain compliance with this section.

THIRD PARTY SERVICE PROVIDER SECURITY POLICY

What this is:

Each institution must implement written policies and procedures designed to ensure the security of information systems and nonpublic information that are accessible to, or held by, third party service providers. The policies and procedures should be based on the results of the Periodic Risk Assessments and include minimum cyber security practices required to be met, due diligence processes used to evaluate the adequacy of cybersecurity practices and should be periodically assessed to ensure adequacy of third party service providers cyber security practices. The policies and procedures shall include relevant guidelines for due diligence and/or contractual protections relating to Third Party Service Providers including the Third Party Service Provider's policies and procedures for access controls including its use of Multi-Factor Authentication to limit access to sensitive systems and Nonpublic Information, use of encryption and notice to be provided to the finical institute in the event of a cyber security event directly impacting the finical institute information systems or non-public information.

Why is this important:

Anyone with access to a network has can be a potential cyber security threat. A hacker can break into a Third Party Service Provider's network and then gain access to your network. By ensuring third party service providers are secure, organizations can secure their network.

How to become compliant:

Prevalent Vendor Risk takes the guesswork out of vendor assessment by creating a standard tiering structure within your organization, a standardized assessment workflow, shared assessments content, evidence collection, risk scoring, and reporting. The solution manages each vendor independently, offering you the ability to understand the impact of doing business with a particular vendor. Additionally, the solution can offer an aggregated view to understand vendor risk by tier or across all vendors.

ENHANCED MULTI-FACTOR AUTHENTICATION

What this is:

Each institute shall use effective controls, which may include Multi-Factor Authentication or Risk-Based Authentication, to protect against unauthorized access to nonpublic information or information systems. Multi-Factor Authentication must be utilized for any individual accessing the finical institute's internal networks from an external network, unless the CISO has approved in writing the use of reasonably equivalent or more secure access controls.

Why is this important:

Multi-Factor Authentication helps ensure that the person accessing the data is who they say they are. It is easy for an intruder to figured out a single method of entry, like just a password. It is far me difficult if the intruder needs multiple pieces of information to steal credentials.

How to become compliant:

HID is a fully CJIS Advanced Authentication compliant solution, assists organizations satisfy

HIPAA, HITECH, EPCS, Positive ID, and PCI-DSS requirements; while at the same time makes lives easier for end-users by streamlining authentication processes and reducing the amount of passwords users have to enter and manage on a daily basis. HID does all of this and significantly increases the level of security throughout the organization.

LIMITATIONS ON DATA RETENTION

What this is:

Each institute must have policies and procedures for the secure disposal of any nonpublic information identified on a periodic basis that is no longer necessary for business operations or for other legitimate business purposes, except where such information is otherwise required to be retained by law or regulation, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained.

Why is this important:

Just because data is no longer needed by the financial institute does not mean that there is not nonpublic information or sensitive information in it. Therefore, proper disposal is needed.

How to become compliant:

Varonis doesn't just show you where sensitive data lives, they show you where it's overexposed, who is accessing it, and how to lock it down. DatAdvantage will also identify stale data that is no longer accessed by actual humans – save disk space, lower cost and simplify your environment all at once. DatAdvantage uses machine learning and bi-directional cluster analysis to pinpoint users that have access to files they don't need to do their job. It's your single interface for managing permissions and security groups.

Fasoo Data Security Framework helps organizations discover, classify and protect sensitive data so that you control who can access it, regardless of location. It discovers and classifies sensitive files automatically and encrypts them as you create them on the desktop, localize them from databases or download them from information systems. Dynamic security policies travel with the files and apply permission controls that grant or deny users the right to View, Edit, Copy, Paste, Print or Decrypt the files. If any unauthorized user got access to the file, they could not read the information inside.

Check Point Data Loss Prevention (DLP) Software Blade combines technology and processes to revolutionize DLP, helping businesses to pre-emptively protect sensitive information from unintentional loss, educating users on proper data handling policies and empowering them to remediate incidents in real-time.

TRAINING AND MONITORING

What this is:

Each institute must implement risk-based policies, procedures and controls designed to monitor the activity of authorized users and detect unauthorized access or use of, or tampering with

nonpublic information by authorized users. Additionally, finical institutes need to provide for regular cyber security awareness training for all personnel that is updated to reflect risks identified by the finical institute in its Risk Assessment.

Why is this important:

Monitoring authorized user access will help catch improper use and prevent cyber breaches. If an organization is unaware that an authorized account has been compromised or is accesses databases it should not be, then it will not be able to stop the problem. Not all breaches of this kind are intentional-some happen unknowingly. Therefore, it is important to train and educate your employees on proper behaviors to maintain a secure environment.

How to become compliant:

CyberArk Privileged Threat Analytics, part of the CyberArk Privileged Account Security Solution, is a security intelligence system that allows organizations to detect, alert, and respond to cyber-attacks targeting privileged accounts. The solution is designed to identify an attack in real-time and automatically respond to stop an attacker from continuing to advance the attack.

Training It is important to have an updated employee cyber security policy and to educate them on it. This portion of the regulation can change based on an organization's needs.

ENCRYPTION OF NONPUBLIC INFORMATION

What this is:

All institutes, based on their Risk Assessment, must utilize encryption to protect nonpublic information that they hold or transmit, both in transit over external networks and at rest. The effectiveness of encryption shall be reviewed by the CISO at least annually.

Why is this important:

Data is everywhere and unprotected data creates significant vulnerabilities. It is important to protect data throughout its lifecycle; at rest, in motion, in use and also in the cloud.

How to become compliant:

Check Point Endpoint Data Protection combines data security, network security, threat prevention technologies and remote access VPN into one package for complete Windows and Mac OS X protection. Secure data at rest, data in use and data in transit on endpoint devices. Secure endpoint devices from threats. Simplify endpoint security with a unified endpoint security policy and reporting of events. This integrated suite allows users to manage security protection from a single console.

Fasoo Enterprise DRM protects, controls and traces sensitive files containing intellectual property, trade secrets, PII and more. It maintains file protection and prevents unintended information disclosure no matter where it is.

Varonis enables you to remove the risks associated with file permissions and auditing. Easily prove to regulators that IT controls are stringent and manage user permissions efficiently, so the right people, and only the right people, have access to data.

INCIDENT RESPONSE PLAN

What this is:

Every institute must create a written incident response plan designed to promptly respond to and recover from any cyber security event that affects the confidentiality, integrity or availability of the information systems or the continuing functionality of any aspect of the finical institute business or operations. The incident response plan shall address the following areas: the internal processes for responding to a cyber security event, the goals of the incident response plan, definition of clear roles, responsibilities and levels of decision-making authority, external and internal communications and information sharing, identification of requirements for the remediation of any identified weaknesses in information systems and associated controls, documentation and reporting regarding cyber security events and related incident response activities and the evaluation and revision as necessary of the incident response plan following a cyber security events.

Why is this important:

As the Marines say, "It is better to have and not need, then need and not have". It is better to be prepared for an incident and know how to recover and not use it, then to have an incident and not know how to respond.

How to become compliant:

Spend time creating and documenting proper incident response plan. Make sure to review and inform all involved parties of their role in the plan.

For more information on Brite's full line-up of cybersecurity tools and services, visit brite.com/cybersecurity.