The Intersection of M&A and Cyber – The Importance of Cyber Due Diligence in Your Deals

Today's Program – April 4, 2017
Facilitator Biographies

Michele Maney is a partner in Venable's Corporate Group with significant experience negotiating and implementing mergers and acquisitions, private equity and venture capital transactions, LBOs, divestitures and joint ventures. Ms. Maney also provides general corporate counseling. She represents a broad range of clients in connection with U.S. and cross-border business and investment transactions, with a focus on private equity, venture capital, strategic and institutional investors in private financings. Among her recent deals, Ms. Maney, with co-presenter Philip von Mehren, advised Canada-based online dating site, PlentyOfFish Media, Inc. in the $575 million sale to the Match Group, a subsidiary of IAC. The team won the "Technology Deal of the Year Award" from The Association for Corporate Growth (ACG) New York for their role on the deal.

A leading voice in national cybersecurity policy with over two decades of government and nonprofit experience, **Ari Schwartz** is Venable's Managing Director of Cybersecurity Services. Mr. Schwartz oversees Venable's cybersecurity consulting services and assists organizations in developing risk management strategies, including implementing the National Institute of Standards and Technology (NIST) Cybersecurity Framework, to help minimize risk. Prior to joining Venable, Mr. Schwartz was a member of the White House National Security Council, where he served as Special Assistant to the President and Senior Director for Cybersecurity.

Jami Mills Vibbert is a member of Venable's Privacy and Data Security practice, andadvises and counsels clients on matters related to data security, data protection, and data risk management. She conducts comprehensive data security risk assessments and gap analyses, and develops and implements data risk solutions and comprehensive breach prevention and incident response programs. She also assists clients on a wide variety of complex litigation, including incident response investigations and litigation.

Philip von Mehren is the co–chair of Venable's New York Corporate Group. He routinely handles cross-border and domestic acquisitions and dispositions – for strategic and financial buyers and sellers – including family office and private equity and venture capital funds. He also advices his corporate, family office and private equity fund clients in matters of corporate governance and compliance.

Mr. von Mehren is outside counsel for the Latin American Private Equity and Venture Capital Association (LAVCA), the leading international association for Latin American-focused GPs and LPs.

VENABLE

The Intersection of M&A and Cyber – The Importance of Cyber Due Diligence in Your Deals

Michele Maney
Partner, Corporate / M&A

Ari Schwartz
Managing Director of Cybersecurity Services

Jami Mills Vibbert
Counsel, Privacy and Data Security

Philip von Mehren
Partner, Corporate / M&A

Our Road Map

- Introduction
- Cyber Threats
- The Impact for Deals
- The Cyber Audit
- Q&A

Cyber Due Diligence Strategy

- Purchasers: develop strategy to ensure target meets or exceeds the purchaser's standards and target is priced appropriately
- Sellers: reexamine policies, programs, and controls before entering market to maximize value

The Four Phases of Cyber Due Diligence for the Purchaser

1. Preliminary risk assessment
    a. Polling target on its cybersecurity practices
2. Detailed interview with target's management
    a. Analysis of policies and procedures, types of data, hacking history
3. Full assessment
    a. Review of policies, procedures, controls, employee interviews, technical vulnerability testing, compliance practices
4. Written report

PHOTO: SHUTTERSTOCK

Questions?

Michele Maney
Partner, Corporate / M&A
Venable LLP
New York
mmaney@Venable.com
212.503.0678

Ari Schwartz
Managing Director of Cybersecurity Services
Venable LLP
Washington, DC
aschwartz@Venable.com
202.344.4711

Jami Mills Vibbert
Counsel, Privacy & Data Security
Venable LLP
New York
jvibbert@Venable.com
212.370.6288

Philip von Mehren
Partner, Corporate / M&A
Venable LLP
New York
ptvonmehren@Venable.com
212.503.0679

Notes:

VENABLE LLP

Cybersecurity Alert

March 27, 2017

Cyber Diligence and Practical Advice for Managing Cyber Risk in the Deal Context

AUTHORS

Michele Maney
Jami Mills Vibbert
Philip T. von Mehren

RELATED PRACTICES

Privacy and Data Security
Corporate
Mergers and Acquisitions

RELATED INDUSTRIES

Cybersecurity Risk Management Services

ARCHIVES

2017 2013 2009
2016 2012 2008
2015 2011 2007
2014 2010

Not a day goes by without news of a new cyberattack or data loss, across all industries and all sizes of organizations. The consequences of those attacks for the company can be dire—reputational harm, C-Suite turnover, and material diminution of shareholder equity. Although cyber issues are omnipresent for most companies, the period in and around an acquisition/divestiture transaction can be an especially sensitive moment for both purchasers and sellers. As neither data breaches nor deals are going anywhere, both purchasers and sellers need to develop a strategy to address this issue in the context of acquisitions. To maximize value, sellers should reexamine their cyber policies, programs, and controls and make sure they are as robust as is practical before embarking on a sales process. Purchasers should develop a cyber due diligence strategy to ensure that the target meets or exceeds the purchaser's standards and to ensure the appropriate price is paid for the target.

As a seller prepares itself for a sale, it must make a hard-headed determination of what policies, procedures, and controls it has in place to protect its data as well as the data of its customers. A well-constructed cybersecurity program will reassure potential buyers that the company is not a potential reputational and liability trap and help the target to maximize its sale price. Making sure that management has thought through how it will respond to a purchaser's requests on cybersecurity can help a seller maximize its value and shorten the sales process.

Purchasers should, similarly, focus on cybersecurity audits of targets to ensure that both the technology being purchased and the customer and employee data have been well protected. The extent of the due diligence will depend on a number of factors, including (i) the type of sensitive customer data the company uses and stores; (ii) whether the IP used by the company is a likely data breach target, and, if so, whether competitors could use such IP to undermine the company's business plans, including through misappropriation; and (iii) the types of cybersecurity policies, procedures, and controls the company has used historically and whether those were reasonable and risk-based. Each of these factors should be viewed on a continuum—the more emphatic the response is to any of these factors, the more a deep dive into the target's cyber program is warranted.

A purchaser should not rely only on standard contractual protections, as they relate only to a narrow definition of "losses," and then only if a specific representation can be shown to have been be breached. Quantifying losses for enormous reputational harm, C-suite turnover, and competitive disadvantage or misappropriation of proprietary IP may far exceed the actual legal liabilities suffered by a target post-closing that are recoverable under the transaction agreement through indemnification.

In this resource-constrained world, however, organizations need to be able to make determinations of how much cybersecurity due diligence they should conduct and when. The scale of cybersecurity due diligence ranges from simple to extensive. How a company should determine the amount of cyber diligence depends on several factors. A company should estimate the extent of the reputational harm that would come from the revelation of a data breach at the company, the financial harm that may arise from a data breach (whether because of litigation or because of loss of valuable information), and any liability to which the company would be exposed from regulators or others. For example, a healthcare company subject to the data security rules in HIPAA may weigh the regulatory risk higher than a non-regulated company, such as a non-consumer-facing company; but that company may still face enormous losses from a due loss of reputation.

Purchasers will also want to consider the implications of a latent breach or security vulnerabilities on issues specifically related to the target company. While it is clear that if the target company is being acquired for the data itself, the confidentiality, integrity, and availability of that data are of paramount importance, other types of targets may have other considerations. For example, a target company with specific intellectual property may not be worth purchasing if the IP has been compromised by a hacker (either because of the misappropriation of that IP or because of the competitive disadvantage of others with that IP). Similarly, the purchaser needs to understand the classes of information held by the target that are different from the classes of information that the acquiring company possesses and assess whether the purchaser's policies will need to be altered to integrate the new business. Sometimes purchasers fail to realize that the target might be subject to a different regulatory framework than the

purchaser, which can lead the purchaser to underappreciate the risks and expense attendant with an acquisition.

Once a purchaser has considered the potential impact of a breach and the cyber vulnerabilities of a target, the purchaser should use that knowledge to begin the due diligence process on the target. The first phase consists of a preliminary risk assessment. In this phase, the purchaser polls the target on its cybersecurity practices. The target's responses help to identify any major issues the target may have on security practices. Ending due diligence at this stage may be appropriate if, for example, the target does not maintain personal data on customers or patients and has a limited number of employees.

In most circumstances, this first phase review will be insufficient to address adequately the risk. The second phase in the due diligence process will be to have a call or meeting with the management at the target, asking detailed questions concerning the company's security posture and policies. This is a relatively cost-effective way to conduct diligence and have access to additional information that may raise or allay significant concern. This information then needs to be analyzed to decide whether more significant due diligence is prudent. If any yellow flags appear because of the target's existing policies and procedures, types of data, historical experience with hacking, or sensitive IP, more due diligence is likely warranted in order to make an informed decision of whether the purchaser should move forward with the transaction, request a price reduction, or simply walk away from the transaction.

If any yellow flags exist after the first and second phases of the cyber due diligence, a third phase should be initiated. A full cybersecurity assessment includes a thorough review of the policies, procedures, and controls of the company, interviews of employees and management, technical vulnerability testing, and an assessment of the company's compliance practices with the industry's best standards and any relevant regulatory requirements. These cybersecurity assessments are best conducted by a combined legal and technical team that can discuss with the purchaser the extent of the vulnerabilities in the cyber program and how those vulnerabilities mesh with the risk tolerance of the acquiring company. The assessment should provide a verification of the responses received during the first two phases.

This phase should explore such issues as whether and how often a target has been attacked, the adequacy of written policies and programs, how personnel are trained in such policies and programs and compliance with same, whether the cybersecurity program at the target is appropriately resourced and accountable, access controls, encryption practices, data location, data use and transfer issues, change control management, physical security, back-up practices, vendor due diligence programs, software acquisition practices, efforts to stay informed of the latest threats, and the target's auditing scheme. This type of assessment would attempt to uncover latent breaches and provide insight into other vulnerabilities and risks. If the target operates in multiple jurisdictions globally, the purchaser and its advisors will need to conduct a risk-benefit analysis of the level of diligence that should be conducted in foreign jurisdictions where standards and penalties may differ substantively from those in the United States.

After a review of the target's cybersecurity practices, a written due diligence report would normally be prepared. The report would summarize the security practices of the target, attempt to discover whether a latent breach has occurred, assess overall strengths and weaknesses, and attempt to determine whether valuable IP has been hacked. Based on the report, the purchaser can decide how to respond to what it has uncovered through the due diligence process, including whether to renegotiate the price, continue with the deal on the agreed-upon terms, or, in egregious situations, terminate negotiations. The report also serves another function of helping the purchaser better integrate the target company into the purchaser's overall cybersecurity program.

While purchasers will want to rely as much as possible on their own diligence to gain comfort around potential liability for cybersecurity matters, the use of thorough representations and warranties in transaction documents serves as a secondary means of confirming diligence and provides some protection through indemnification. While, as noted above, it is difficult to provide security to a purchaser for potential reputational losses through customary indemnification provisions for breaches of representations and warranties, purchasers that have particular sensitivities in this area may structure direct indemnities, that do not require a breach for recovery of a loss, to protect the purchaser from a consequential business loss due to a cybersecurity breach. These provisions can be specifically tailored to address the particular factors and concerns of a given transaction. However, they may also be constrained by both parties' desire to avoid creating a road map for any regulatory authority or other third-party claimant that may have a claim against the target. As an alternative, a purchaser may choose to rely simply on breach of representations and warranties, with an agreement that the customary deductibles and caps on recovery would not apply and that the survival period would be longer than standard representations and warranties. These representations and warranties are more likely to be drafted without "knowledge" or "materiality" qualifiers, as a standard of strict liability is an increasingly common framework for cybersecurity matters.

As more companies suffer economic and reputation losses related to cybersecurity lapses, the importance of cybersecurity due diligence becomes more apparent. A thorough risk assessment not only has a benefit in terms of better assessing the target's risk and appropriately pricing that risk; the assessment itself is a testament to the purchaser's own cybersecurity maturity. This factor may be extremely important if, after closing, the target or the purchaser suffers a security incident. Regulators (and shareholders) may assess whether a company was reasonable in its data security practices by reference to the amount of diligence that the company did on the target. It is often said that it is not a question of if you will be breached, but when. In this dangerous environment, making sure that processes are sound is the best way to protect the company and its reputation. Conducting cybersecurity

due diligence decreases the likelihood of an attack in the future, decreases likelihood of liability in the event of an attack, and increases the ability of the purchaser to ensure the overall soundness of its cybersecurity practices.

VENABLE LLP

Cybersecurity Alert

February 27, 2017

New York's Department of Financial Services Finalizes Cybersecurity Requirements for Financial Institutions

AUTHORS

Ari Schwartz

Jami Mills Vibbert

RELATED PRACTICES

Privacy and Data Security

Banking and Financial Services Regulatory

Risk and Compliance (RCOM)

RELATED INDUSTRIES

Cybersecurity Risk Management Services

Financial Services

ARCHIVES

2017 2013 2009

2016 2012 2008

2015 2011 2007

2014 2010

On March 1, 2017, the New York State Department of Financial Services' (DFS) mandatory **cybersecurity requirements** for financial services entities will become effective, with implementation to occur within 180 days (or by September 1, 2017). The requirements broadly cover all entities operating under or required to operate under DFS licensure, registration, or charter, or which are otherwise DFS-regulated, as well as, by extension, unregulated third-party service providers to regulated entities. This not only includes state-chartered banks, licensed lenders, private bankers, service contract providers, trust companies, and mortgage companies, but also foreign banks licensed to operate in New York and any insurance company doing business in New York. It does exempt small companies, though, including those with fewer than 10 employees, less than $5 million in gross annual revenue for three years, or less than $10 million in year-end total assets.

The regulation delineates various minimum standards and requires a risk-based cybersecurity program tailored to each company's specific risk profile. Significantly, the regulation requires covered entities to file an annual certification of compliance with the regulation; Certifications of Compliance will commence February 15, 2018.

As discussed in a **prior alert**, DFS proposed similar regulations on September 13 of last year, but that set of regulations elicited significant feedback. Still, the regulations require potentially significant changes and focus on cybersecurity for many institutions.

Requirements

Generally, the regulation's requirements are focused on steps to increase security awareness and to encourage a risk-based, holistic, and robust security program at covered entities. To ensure compliance, covered entities must implement the following:

1. *Risk Assessments:* Periodic risk assessments that consider threats, particular risks to the entity, and an examination of existing controls in the context of identified risk.

2. *Cybersecurity Program:* The creation of a cybersecurity program based on the periodic risk assessments and designed to identify and assess risks; protect information systems and nonpublic information; detect, respond to, and recover from cyber events; and fulfill all reporting obligations. The program must include annual penetration testing and biannual vulnerability assessments. The cybersecurity program referenced here follows the general mandates of those delineated in the NIST Cybersecurity Framework.

3. *Cybersecurity Policies:* The creation and maintenance of written policies and procedures for the protection of information systems and nonpublic information and based on the risk assessment. These must include a written incident response plan.

4. *CISO:* The designation of a chief information security officer to oversee the cybersecurity program.

5. *Minimum Standards:* Implementation of minimum cybersecurity standards, including systems designed to recover material financial transactions following an event and audit trails to detect events, the institution of appropriate access privileges, procedures for evaluating and testing the security of applications, multifactor authentication, data disposal, mandatory cybersecurity awareness training, and encryption measures.

6. *Third-Party Risk Management:* Implementation of a third-party risk management program, including a review of the cybersecurity practices of those providers and periodic assessment and audit thereof.

These new requirements, which are the first of their kind, signal an increased focus on risk-prioritized and managed cybersecurity.

Save the Date: On April 4, the article's authors will lead a discussion in **Venable's New York City office** concerning conducting cybersecurity due diligence in M&A deals. Sellers and purchasers subject to this regulation should consider such due diligence an important aspect of maintaining an appropriate cybersecurity program. Please email **tfacey@Venable.com** for more information on the program.

NEW YORK STATE
DEPARTMENT OF FINANCIAL SERVICES
23 NYCRR 500

CYBERSECURITY REQUIREMENTS FOR FINANCIAL SERVICES COMPANIES

I, Maria T. Vullo, Superintendent of Financial Services, pursuant to the authority granted by sections 102, 201, 202, 301, 302 and 408 of the Financial Services Law, do hereby promulgate Part 500 of Title 23 of the Official Compilation of Codes, Rules and Regulations of the State of New York, to take effect March 1, 2017, to read as follows:

(ALL MATTER IS NEW)

Section 500.00 Introduction.

The New York State Department of Financial Services ("DFS") has been closely monitoring the ever-growing threat posed to information and financial systems by nation-states, terrorist organizations and independent criminal actors. Recently, cybercriminals have sought to exploit technological vulnerabilities to gain access to sensitive electronic data. Cybercriminals can cause significant financial losses for DFS regulated entities as well as for New York consumers whose private information may be revealed and/or stolen for illicit purposes. The financial services industry is a significant target of cybersecurity threats. DFS appreciates that many firms have proactively increased their cybersecurity programs with great success.

Given the seriousness of the issue and the risk to all regulated entities, certain regulatory minimum standards are warranted, while not being overly prescriptive so that cybersecurity programs can match the relevant risks and keep pace with technological advances. Accordingly, this regulation is designed to promote the protection of customer information as well as the information technology systems of regulated entities. This regulation requires each company to assess its specific risk profile and design a program that addresses its risks in a robust fashion. Senior management must take this issue seriously and be responsible for the organization's cybersecurity program and file an annual certification confirming compliance with these regulations. A regulated entity's cybersecurity program must ensure the safety and soundness of the institution and protect its customers.

It is critical for all regulated institutions that have not yet done so to move swiftly and urgently to adopt a cybersecurity program and for all regulated entities to be subject to minimum standards with respect to their programs. The number of cyber events has been steadily increasing and estimates of potential risk to our financial services industry are stark. Adoption of the program outlined in these regulations is a priority for New York State.

Section 500.01 Definitions.

For purposes of this Part only, the following definitions shall apply:

(a) *Affiliate* means any Person that controls, is controlled by or is under common control with another Person. For purposes of this subsection, control means the possession, direct or indirect, of the power to direct or cause the direction of the management and policies of a Person, whether through the ownership of stock of such Person or otherwise.

(b) *Authorized User* means any employee, contractor, agent or other Person that participates in the business operations of a Covered Entity and is authorized to access and use any Information Systems and data of the Covered Entity.

(c) *Covered Entity* means any Person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law.

(d) *Cybersecurity Event* means any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an Information System or information stored on such Information System.

(e) *Information System* means a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems.

(f) *Multi-Factor Authentication* means authentication through verification of at least two of the following types of authentication factors:

(1) Knowledge factors, such as a password; or

(2) Possession factors, such as a token or text message on a mobile phone; or

(3) Inherence factors, such as a biometric characteristic.

(g) *Nonpublic Information* shall mean all electronic information that is not Publicly Available Information and is:

(1) Business related information of a Covered Entity the tampering with which, or unauthorized disclosure, access or use of which, would cause a material adverse impact to the business, operations or security of the Covered Entity;

(2) Any information concerning an individual which because of name, number, personal mark, or other identifier can be used to identify such individual, in combination with any one or more of the following data elements: (i) social security number, (ii) drivers' license number or non-driver identification card number, (iii) account number, credit or debit card number, (iv) any security code, access code or password that would permit access to an individual's financial account, or (v) biometric records;

(3) Any information or data, except age or gender, in any form or medium created by or derived from a health care provider or an individual and that relates to (i) the past, present or future physical, mental or behavioral health or condition of any individual or a member of the individual's family, (ii) the provision of health care to any individual, or (iii) payment for the provision of health care to any individual.

(h) *Penetration Testing* means a test methodology in which assessors attempt to circumvent or defeat the security features of an Information System by attempting penetration of databases or controls from outside or inside the Covered Entity's Information Systems.

(i) *Person* means any individual or any non-governmental entity, including but not limited to any non-governmental partnership, corporation, branch, agency or association.

(j) *Publicly Available Information* means any information that a Covered Entity has a reasonable basis to believe is lawfully made available to the general public from: federal, state or local government records; widely distributed media; or disclosures to the general public that are required to be made by federal, state or local law.

(1) For the purposes of this subsection, a Covered Entity has a reasonable basis to believe that information is lawfully made available to the general public if the Covered Entity has taken steps to determine:

(i) That the information is of the type that is available to the general public; and

(ii) Whether an individual can direct that the information not be made available to the general public and, if so, that such individual has not done so.

(k) *Risk Assessment* means the risk assessment that each Covered Entity is required to conduct under section 500.09 of this Part.

(l) *Risk-Based Authentication* means any risk-based system of authentication that detects anomalies or changes in the normal use patterns of a Person and requires additional verification of the Person's identity when such deviations or changes are detected, such as through the use of challenge questions.

(m) *Senior Officer(s)* means the senior individual or individuals (acting collectively or as a committee) responsible for the management, operations, security, information systems, compliance and/or risk of a Covered Entity, including a branch or agency of a foreign banking organization subject to this Part.

(n) *Third Party Service Provider(s)* means a Person that (i) is not an Affiliate of the Covered Entity, (ii) provides services to the Covered Entity, and (iii) maintains, processes or otherwise is permitted access to Nonpublic Information through its provision of services to the Covered Entity.

Section 500.02 Cybersecurity Program.

(a) Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems.

(b) The cybersecurity program shall be based on the Covered Entity's Risk Assessment and designed to perform the following core cybersecurity functions:

(1) identify and assess internal and external cybersecurity risks that may threaten the security or integrity of Nonpublic Information stored on the Covered Entity's Information Systems;

(2) use defensive infrastructure and the implementation of policies and procedures to protect the Covered Entity's Information Systems, and the Nonpublic Information stored on those Information Systems, from unauthorized access, use or other malicious acts;

(3) detect Cybersecurity Events;

(4) respond to identified or detected Cybersecurity Events to mitigate any negative effects;

(5) recover from Cybersecurity Events and restore normal operations and services; and

(6) fulfill applicable regulatory reporting obligations.

(c) A Covered Entity may meet the requirement(s) of this Part by adopting the relevant and applicable provisions of a cybersecurity program maintained by an Affiliate, provided that such provisions satisfy the requirements of this Part, as applicable to the Covered Entity.

(d) All documentation and information relevant to the Covered Entity's cybersecurity program shall be made available to the superintendent upon request.

Section 500.03 Cybersecurity Policy.

Cybersecurity Policy. Each Covered Entity shall implement and maintain a written policy or policies, approved by a Senior Officer or the Covered Entity's board of directors (or an appropriate committee thereof) or equivalent governing body, setting forth the Covered Entity's policies and procedures for the protection of its Information Systems and Nonpublic Information stored on those Information Systems. The cybersecurity policy shall be based on the Covered Entity's Risk Assessment and address the following areas to the extent applicable to the Covered Entity's operations:

(a) information security;

(b) data governance and classification;

(c) asset inventory and device management;

(d) access controls and identity management;

(e) business continuity and disaster recovery planning and resources;

(f) systems operations and availability concerns;

(g) systems and network security;

(h) systems and network monitoring;

(i) systems and application development and quality assurance;

(j) physical security and environmental controls;

(k) customer data privacy;

(l) vendor and Third Party Service Provider management;

(m) risk assessment; and

(n) incident response.

Section 500.04 Chief Information Security Officer.

(a) Chief Information Security Officer. Each Covered Entity shall designate a qualified individual responsible for overseeing and implementing the Covered Entity's cybersecurity program and enforcing its cybersecurity policy (for purposes of this Part, "Chief Information Security Officer" or "CISO"). The CISO may be employed by the Covered Entity, one of its Affiliates or a Third Party Service Provider. To the extent this requirement is met using a Third Party Service Provider or an Affiliate, the Covered Entity shall:

(1) retain responsibility for compliance with this Part;

(2) designate a senior member of the Covered Entity's personnel responsible for direction and oversight of the Third Party Service Provider; and

(3) require the Third Party Service Provider to maintain a cybersecurity program that protects the Covered Entity in accordance with the requirements of this Part.

(b) Report. The CISO of each Covered Entity shall report in writing at least annually to the Covered Entity's board of directors or equivalent governing body. If no such board of directors or equivalent governing body exists, such report shall be timely presented to a Senior Officer of the Covered Entity responsible for the Covered Entity's cybersecurity program. The CISO shall report on the Covered Entity's cybersecurity program and material cybersecurity risks. The CISO shall consider to the extent applicable:

(1) the confidentiality of Nonpublic Information and the integrity and security of the Covered Entity's Information Systems;

(2) the Covered Entity's cybersecurity policies and procedures;

(3) material cybersecurity risks to the Covered Entity;

(4) overall effectiveness of the Covered Entity's cybersecurity program; and

(5) material Cybersecurity Events involving the Covered Entity during the time period addressed by the report.

Section 500.05 Penetration Testing and Vulnerability Assessments.

The cybersecurity program for each Covered Entity shall include monitoring and testing, developed in accordance with the Covered Entity's Risk Assessment, designed to assess the effectiveness of the Covered Entity's cybersecurity program. The monitoring and testing shall include continuous monitoring or periodic Penetration Testing and vulnerability assessments. Absent effective continuous monitoring, or other systems to detect, on an ongoing basis, changes in Information Systems that may create or indicate vulnerabilities, Covered Entities shall conduct:

(a) annual Penetration Testing of the Covered Entity's Information Systems determined each given year based on relevant identified risks in accordance with the Risk Assessment; and

(b) bi-annual vulnerability assessments, including any systematic scans or reviews of Information Systems reasonably designed to identify publicly known cybersecurity vulnerabilities in the Covered Entity's Information Systems based on the Risk Assessment.

Section 500.06 Audit Trail.

(a) Each Covered Entity shall securely maintain systems that, to the extent applicable and based on its Risk Assessment:

(1) are designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the Covered Entity; and

(2) include audit trails designed to detect and respond to Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operations of the Covered Entity.

(b) Each Covered Entity shall maintain records required by section 500.06(a)(1) of this Part for not fewer than five years and shall maintain records required by section 500.06(a)(2) of this Part for not fewer than three years.

Section 500.07 Access Privileges.

As part of its cybersecurity program, based on the Covered Entity's Risk Assessment each Covered Entity shall limit user access privileges to Information Systems that provide access to Nonpublic Information and shall periodically review such access privileges.

Section 500.08 Application Security.

(a) Each Covered Entity's cybersecurity program shall include written procedures, guidelines and standards designed to ensure the use of secure development practices for in-house developed applications utilized by the Covered Entity, and procedures for evaluating, assessing or testing the security of externally developed applications utilized by the Covered Entity within the context of the Covered Entity's technology environment.

(b) All such procedures, guidelines and standards shall be periodically reviewed, assessed and updated as necessary by the CISO (or a qualified designee) of the Covered Entity.

Section 500.09 Risk Assessment.

(a) Each Covered Entity shall conduct a periodic Risk Assessment of the Covered Entity's Information Systems sufficient to inform the design of the cybersecurity program as required by this Part. Such Risk Assessment shall be updated as reasonably necessary to address changes to the Covered Entity's Information Systems, Nonpublic Information or business operations. The Covered Entity's Risk Assessment shall allow for revision of controls to respond to technological developments and evolving threats and shall consider the particular risks of the Covered Entity's business operations related to cybersecurity, Nonpublic Information collected or stored, Information Systems utilized and the availability and effectiveness of controls to protect Nonpublic Information and Information Systems.

(b) The Risk Assessment shall be carried out in accordance with written policies and procedures and shall be documented. Such policies and procedures shall include:

(1) criteria for the evaluation and categorization of identified cybersecurity risks or threats facing the Covered Entity;

(2) criteria for the assessment of the confidentiality, integrity, security and availability of the Covered Entity's Information Systems and Nonpublic Information, including the adequacy of existing controls in the context of identified risks; and

(3) requirements describing how identified risks will be mitigated or accepted based on the Risk Assessment and how the cybersecurity program will address the risks.

Section 500.10 Cybersecurity Personnel and Intelligence.

(a) Cybersecurity Personnel and Intelligence. In addition to the requirements set forth in section 500.04(a) of this Part, each Covered Entity shall:

(1) utilize qualified cybersecurity personnel of the Covered Entity, an Affiliate or a Third Party Service Provider sufficient to manage the Covered Entity's cybersecurity risks and to perform or oversee the performance of the core cybersecurity functions specified in section 500.02(b)(1)-(6) of this Part;

(2) provide cybersecurity personnel with cybersecurity updates and training sufficient to address relevant cybersecurity risks; and

(3) verify that key cybersecurity personnel take steps to maintain current knowledge of changing cybersecurity threats and countermeasures.

(b) A Covered Entity may choose to utilize an Affiliate or qualified Third Party Service Provider to assist in complying with the requirements set forth in this Part, subject to the requirements set forth in section 500.11 of this Part.

Section 500.11 Third Party Service Provider Security Policy.

(a) Third Party Service Provider Policy. Each Covered Entity shall 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. Such policies and procedures shall be based on the Risk Assessment of the Covered Entity and shall address to the extent applicable:

(1) the identification and risk assessment of Third Party Service Providers;

(2) minimum cybersecurity practices required to be met by such Third Party Service Providers in order for them to do business with the Covered Entity;

(3) due diligence processes used to evaluate the adequacy of cybersecurity practices of such Third Party Service Providers; and

(4) periodic assessment of such Third Party Service Providers based on the risk they present and the continued adequacy of their cybersecurity practices.

(b) Such policies and procedures shall include relevant guidelines for due diligence and/or contractual protections relating to Third Party Service Providers including to the extent applicable guidelines addressing:

(1) the Third Party Service Provider's policies and procedures for access controls, including its use of Multi-Factor Authentication as required by section 500.12 of this Part, to limit access to relevant Information Systems and Nonpublic Information;

(2) the Third Party Service Provider's policies and procedures for use of encryption as required by section 500.15 of this Part to protect Nonpublic Information in transit and at rest;

(3) notice to be provided to the Covered Entity in the event of a Cybersecurity Event directly impacting the Covered Entity's Information Systems or the Covered Entity's Nonpublic Information being held by the Third Party Service Provider; and

(4) representations and warranties addressing the Third Party Service Provider's cybersecurity policies and procedures that relate to the security of the Covered Entity's Information Systems or Nonpublic Information.

(c) Limited Exception. An agent, employee, representative or designee of a Covered Entity who is itself a Covered Entity need not develop its own Third Party Information Security Policy pursuant to this section if the agent, employee, representative or designee follows the policy of the Covered Entity that is required to comply with this Part.

Section 500.12 Multi-Factor Authentication.

(a) Multi-Factor Authentication. Based on its Risk Assessment, each Covered Entity 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.

(b) Multi-Factor Authentication shall be utilized for any individual accessing the Covered Entity's internal networks from an external network, unless the Covered Entity's CISO has approved in writing the use of reasonably equivalent or more secure access controls.

Section 500.13 Limitations on Data Retention.

As part of its cybersecurity program, each Covered Entity shall include policies and procedures for the secure disposal on a periodic basis of any Nonpublic Information identified in section 500.01(g)(2)-(3) of this Part that is no longer necessary for business operations or for other legitimate business purposes of the Covered Entity, 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.

Section 500.14 Training and Monitoring.

As part of its cybersecurity program, each Covered Entity shall:

(a) 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 such Authorized Users; and

(b) provide regular cybersecurity awareness training for all personnel that is updated to reflect risks identified by the Covered Entity in its Risk Assessment.

Section 500.15 Encryption of Nonpublic Information.

(a) As part of its cybersecurity program, based on its Risk Assessment, each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest.

(1) To the extent a Covered Entity determines that encryption of Nonpublic Information in transit over external networks is infeasible, the Covered Entity may instead secure such Nonpublic Information using effective alternative compensating controls reviewed and approved by the Covered Entity's CISO.

(2) To the extent a Covered Entity determines that encryption of Nonpublic Information at rest is infeasible, the Covered Entity may instead secure such Nonpublic Information using effective alternative compensating controls reviewed and approved by the Covered Entity's CISO.

(b) To the extent that a Covered Entity is utilizing compensating controls under (a) above, the feasibility of encryption and effectiveness of the compensating controls shall be reviewed by the CISO at least annually.

Section 500.16 Incident Response Plan.

(a) As part of its cybersecurity program, each Covered Entity shall establish a written incident response plan designed to promptly respond to, and recover from, any Cybersecurity Event materially affecting the confidentiality, integrity or availability of the Covered Entity's Information Systems or the continuing functionality of any aspect of the Covered Entity's business or operations.

(b) Such incident response plan shall address the following areas:

(1) the internal processes for responding to a Cybersecurity Event;

(2) the goals of the incident response plan;

(3) the definition of clear roles, responsibilities and levels of decision-making authority;

(4) external and internal communications and information sharing;

(5) identification of requirements for the remediation of any identified weaknesses in Information Systems and associated controls;

(6) documentation and reporting regarding Cybersecurity Events and related incident response activities; and

(7) the evaluation and revision as necessary of the incident response plan following a Cybersecurity Event.

Section 500.17 Notices to Superintendent.

(a) Notice of Cybersecurity Event. Each Covered Entity shall notify the superintendent as promptly as possible but in no event later than 72 hours from a determination that a Cybersecurity Event has occurred that is either of the following:

(1) Cybersecurity Events impacting the Covered Entity of which notice is required to be provided to any government body, self-regulatory agency or any other supervisory body; or

(2) Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity.

(b) Annually each Covered Entity shall submit to the superintendent a written statement covering the prior calendar year. This statement shall be submitted by February 15 in such form set forth as Appendix A, certifying that the Covered Entity is in compliance with the requirements set forth in this Part. Each Covered Entity shall maintain for examination by the Department all records, schedules and data supporting this certificate for a period of five years. To the extent a Covered Entity has identified areas, systems or processes that require material improvement, updating or redesign, the Covered Entity shall document the identification and the remedial efforts planned and underway to address such areas, systems or processes. Such documentation must be available for inspection by the superintendent.

Section 500.18 Confidentiality.

Information provided by a Covered Entity pursuant to this Part is subject to exemptions from disclosure under the Banking Law, Insurance Law, Financial Services Law, Public Officers Law or any other applicable state or federal law.

Section 500.19 Exemptions.

(a) Limited Exemption. Each Covered Entity with:

(1) fewer than 10 employees, including any independent contractors, of the Covered Entity or its Affiliates located in New York or responsible for business of the Covered Entity, or

(2) less than $5,000,000 in gross annual revenue in each of the last three fiscal years from New York business operations of the Covered Entity and its Affiliates, or

(3) less than $10,000,000 in year-end total assets, calculated in accordance with generally accepted accounting principles, including assets of all Affiliates,

shall be exempt from the requirements of sections 500.04, 500.05, 500.06, 500.08, 500.10, 500.12, 500.14, 500.15, and 500.16 of this Part.

(b) An employee, agent, representative or designee of a Covered Entity, who is itself a Covered Entity, is exempt from this Part and need not develop its own cybersecurity program to the extent that the employee, agent, representative or designee is covered by the cybersecurity program of the Covered Entity.

(c) A Covered Entity that does not directly or indirectly operate, maintain, utilize or control any Information Systems, and that does not, and is not required to, directly or indirectly control, own, access, generate, receive or possess Nonpublic Information shall be exempt from the requirements of sections 500.02, 500.03, 500.04, 500.05, 500.06, 500.07, 500.08, 500.10, 500.12, 500.14, 500.15, and 500.16 of this Part.

(d) A Covered Entity under Article 70 of the Insurance Law that does not and is not required to directly or indirectly control, own, access, generate, receive or possess Nonpublic Information other than information relating to its corporate parent company (or Affiliates) shall be exempt from the requirements of sections 500.02, 500.03, 500.04, 500.05, 500.06, 500.07, 500.08, 500.10, 500.12, 500.14, 500.15, and 500.16 of this Part.

(e) A Covered Entity that qualifies for any of the above exemptions pursuant to this section shall file a Notice of Exemption in the form set forth as Appendix B within 30 days of the determination that the Covered Entity is exempt.

(f) The following Persons are exempt from the requirements of this Part, provided such Persons do not otherwise qualify as a Covered Entity for purposes of this Part: Persons subject to Insurance Law section 1110; Persons subject to Insurance Law section 5904; and any accredited reinsurer or certified reinsurer that has been accredited or certified pursuant to 11 NYCRR 125.

(g) In the event that a Covered Entity, as of its most recent fiscal year end, ceases to qualify for an exemption, such Covered Entity shall have 180 days from such fiscal year end to comply with all applicable requirements of this Part.

Section 500.20 Enforcement.

This regulation will be enforced by the superintendent pursuant to, and is not intended to limit, the superintendent's authority under any applicable laws.

Section 500.21 Effective Date.

This Part will be effective March 1, 2017. Covered Entities will be required to annually prepare and submit to the superintendent a Certification of Compliance with New York State Department of Financial Services Cybersecurity Regulations under section 500.17(b) of this Part commencing February 15, 2018.

Section 500.22 Transitional Periods.

(a) Transitional Period. Covered Entities shall have 180 days from the effective date of this Part to comply with the requirements set forth in this Part, except as otherwise specified.

(b) The following provisions shall include additional transitional periods. Covered Entities shall have:

(1) One year from the effective date of this Part to comply with the requirements of sections 500.04(b), 500.05, 500.09, 500.12, and 500.14(b) of this Part.

(2) Eighteen months from the effective date of this Part to comply with the requirements of sections 500.06, 500.08, 500.13, 500.14 (a) and 500.15 of this Part.

(3) Two years from the effective date of this Part to comply with the requirements of section 500.11 of this Part.

Section 500.23 Severability.

If any provision of this Part or the application thereof to any Person or circumstance is adjudged invalid by a court of competent jurisdiction, such judgment shall not affect or impair the validity of the other provisions of this Part or the application thereof to other Persons or circumstances.

APPENDIX A (Part 500)

(**Covered Entity Name)**

February 15, 20_____

Certification of Compliance with New York State Department of Financial Services Cybersecurity Regulations

The Board of Directors or a Senior Officer(s) of the Covered Entity certifies:

(1) The Board of Directors (or name of Senior Officer(s)) has reviewed documents, reports, certifications and opinions of such officers, employees, representatives, outside vendors and other individuals or entities as necessary;

(2) To the best of the (Board of Directors) or (name of Senior Officer(s)) knowledge, the Cybersecurity Program of (name of Covered Entity) as of_____(date of the Board Resolution or Senior Officer(s) Compliance Finding) for the year ended__(year for which Board Resolution or Compliance Finding is provided) complies with Part ___.

Signed by the Chairperson of the Board of Directors or Senior Officer(s)

(Name)_____ Date: _____

[DFS Portal Filing Instructions]

APPENDIX B (Part 500)

(**Covered Entity Name)**

(Date)_____

Notice of Exemption

In accordance with 23 NYCRR § 500.19(e), (Covered Entity Name) hereby provides notice that (Covered Entity Name) qualifies for the following Exemption(s) under 23 NYCRR § 500.19 (check all that apply):

- ☐ Section 500.19(a)(1)
- ☐ Section 500.19(a)(2)
- ☐ Section 500.19(a)(3)
- ☐ Section 500.19(b)
- ☐ Section 500.19(c)
- ☐ Section 500.19(d)

If you have any question or concerns regarding this notice, please contact:

(Insert name, title, and full contact information)

(Name)_____ Date: _____

(Title)

(Covered Entity Name)

[DFS Portal Filing Instructions]

VENABLE LLP

Cybersecurity Alert

January 18, 2017

NIST Releases Update to Cybersecurity Framework

AUTHORS

John Banghart
Ari Schwartz

RELATED INDUSTRIES

Cybersecurity Risk Management Services

ARCHIVES

2017 2013 2009
2016 2012 2008
2015 2011 2007
2014 2010

On January 10, the National Institute of Standards and Technology (NIST) released the long-awaited draft of the Cybersecurity Framework (CSF), draft version 1.1.

Since its initial release, the CSF has gained remarkable recognition in both the public and private sectors as a shared foundation for cybersecurity risk management. The CSF is comprised of three component parts: the Framework Core, the Framework Implementation Tiers, and the Framework Profiles. The Framework Core is comprised of five Functions: Identify, Protect, Detect, Respond, and Recover. Each function is further divided into Categories, Subcategories, and Informative References. The Framework Implementation Tiers and Framework Profiles are tools that help organizations tailor their application of the Framework Core to their particular business model or sector.

The revisions in CSF draft version 1.1 focus on four key areas:

- **Framework Tiers**

  CSF draft version 1.1 clarifies the relationship between the Framework Implementation Tiers and the Framework Profiles. Specifically, CSF draft version 1.1 highlights how an organization can use Framework Tiers during implementation of the Framework. The Framework Tiers put an organization's cybersecurity practices in context within the greater cyber-ecosystem. This context helps organizations to improve their approach to cybersecurity risk management by allowing them to assess their position relative to other stakeholders.

- **Supply Chain Risk Management (SCRM)**

  In recent years, sensitivity to the security of organizational supply chains has become an area of increasing concern across most industry sectors, as the risk introduced through technical and process dependencies becomes better understood.

  To help improve the security of organizational supply chains, NIST has taken several steps in the CSF: adding a SCRM Category to the Framework Core; making several revisions and additions at the sub-category level across multiple categories; and adding SCRM as a criteria in the Implementation Tiers

- **Access Control Category**

  CSF draft version 1.1 modifies the Access Control Category, which falls within the Protect Function. The modified Access Control Category now encompasses authentication, authorization, and identity proofing. Accordingly, the Access Control Category was renamed "Identity Management and Access Control" (PR.AC) in CSF draft version 1.1. The Category was renamed to provide a more accurate characterization of the scope of the Category and Subcategories. To further support the refined Access Control Category, CSF draft version 1.1 includes an additional Subcategory that specifically addresses identity proofing.

- **Measurement**

  NIST is taking the first steps at providing guidance on how to develop metrics and measurement for organizations using the Framework. CSF draft version 1.1 includes a section titled "Measuring and Demonstrating Cybersecurity," which explains the relationship between business objectives and cybersecurity risk management metrics and measures. The updated framework draft also provides a summary of metrics and measures as they relate to the CSF.

The period for submitting comments and feedback to NIST on CSF draft version 1.1 will conclude on April 10, 2017. Following the comment period, NIST will convene a workshop for interested stakeholders to discuss CSF draft version 1.1. NIST stated that it plans to publish the final CSF version 1.1 around the fall of 2017.

Notes: