Bloomberg BNA

Privacy and Security Law Report®

Third Party Vendors

What protections are necessary for companies, and what concessions third party vendors are willing to make in order to secure such companies as customers, will depend on the circumstances, but companies won't get something they don't ask for, so it's vital for companies to know what its ''asks'' should be as they consider negotiating contracts with third party vendors in light of material cybersecurity considerations, the author writes.

Protecting the Data That Matters: Negotiating Third Party Vendor Contracts in an Age of Material Cybersecurity Concerns

By Russell M. Franklin

Introduction

In an age where digitalization is necessary to corporate survival, and public and private institutions are being hacked on what seems to be a daily basis, much has been written on what a company can do to reduce the probability that its sensitive information is compromised as a result of a direct intrusion. However, what is discussed far less frequently is what a company can do to protect the same information when providing all, or a portion of, such sensitive information to third party vendors is necessary for such company's business functions. In reality this circumstance applies to most companies, whether it be in connection with purposes that are tightly tailored to the company's business or something as general as a contract with a cloud storage provider. Regardless of the specifics, in such a situation, a company should be particularly vigilant about the language that appears in its contracts with vendors that will have access to all or part of its sensitive information. The intention of this article is to shed some light on the big picture items that a company should consider as it negotiates a contract with a vendor if cybersecurity issues are a material consideration.

Russell M. Franklin is a partner in Boies, Schiller & Flexner LLP's corporate group in New York and, among other things, has experience in negotiating contracts in light of cybersecurity concerns.

As is the case with any contract, what considerations are deemed material will vary (in nature and significance) depending on the type of engagement, the identity of the vendor, what information the vendor will have access to and how that information will be accessed. Accordingly, what concepts are reflected in such a contract, and how, has to be determined on a case-by-case basis with a particular eye towards the circumstances. That said, if cybersecurity issues are a material concern, there are a few concepts that are important enough (and general enough) to warrant consideration regardless of the specific circumstances surrounding a vendor contract. These concepts include:

1. an ironclad confidentiality provision;

 ISSN 1538-3423

2. appropriate representations and covenants with respect to the existence of, and maintenance of, sufficient security protocols;

3. the company having a right to effect a physical audit on the vendor's property to confirm how such company's sensitive information is being used and what security protocols are in place to protect it;

4. the company having a right to terminate the contract upon a material data breach (even if such data breach does not expose any of the company's information);

5. an appropriate indemnity to make the company whole in the event that the company is harmed as a result of a data breach; and

6. restrictions on publicity.

Each of the aforementioned considerations are discussed in more detail below.

Material Considerations

An ironclad confidentiality provision that limits the use of ''confidential information'' to those purposes that are absolutely necessary for the vendor to provide the applicable services.

Although some consider confidentiality provisions to be ''boilerplate,'' substantial thought should be given to the language contained therein if cybersecurity concerns are present. For example, in this case, the language has to be drafted such that both a voluntary and involuntary (i.e. a forceful intrusion) sharing of confidential information would result in a breach of the confidentiality provision.

A company should strive to use vendors that do not have to provide a company's sensitive information to yet another third party in order to provide the requisite services.

When it's necessary for a company to provide its sensitive information to a vendor in order for such vendor to provide services, a company should strive to use vendors that do not have to provide a company's sensitive information to yet another third party in order to provide the requisite services. In the event that everything is handled in house, the contract should expressly state that, subject to legally required disclosures, confidential information will not be provided to a third party without the company's consent.

If a vendor must provide certain sensitive information to a third party in order to provide the services in question, the company should be certain that it understands (and the contract expressly states) who such information will be provided to and for what purpose. Given that each additional entity that has access to such information translates into additional risks, the objective is to limit access as much as possible.

If a vendor must share a company's sensitive information with a third party in order to provide the requisite services, each applicable third party should be subject to a confidentiality obligation that is at least as restrictive as the one between the company and the vendor. If possible under the circumstances, it is also worth considering if the company should be an express third party beneficiary of such confidentiality obligation. Leaving aside what the confidentiality provision between the vendor and its related parties says, the vendor always should be directly liable for any breach of the confidentiality provision that appears in the contract between the vendor and the company, even if one of the vendor's related parties is the entity that is ultimately responsible for such breach.

Regardless of if the vendor is a one-stop-shop, or one that leverages a network of other entities to provide the requisite services, a company's sensitive information only should be viewable by employees of such vendor (or related parties) that need to access such information in order for the vendor to provide the services in question—and such sensitive information only should be used in connection with the provision of such services. Both of these requirements should be express in the contract, as, if they are not, it is often the case that any employee of the vendor (or of a related party), whether working on the engagement or not, could view such company's sensitive information and, so long as such information is not provided to a third party, use such information for a myriad of purposes (for example, internal marketing research purposes), all without being in breach of the terms of the contract.

Inclusion of material representations about the security protocols the vendor currently uses to prevent data breaches, and covenants that ensure that, as technologies advance, the vendor appropriately updates its security protocols.

Every company with cybersecurity concerns does some homework on a potential vendor's security protocols prior to engaging such vendor. However, reviewing the security protocols that a vendor advertises on its website or includes in its pitch materials is an insufficient method of ensuring that the vendor's security protocols are adequate. If particularly sensitive information will be shared with the vendor, it may be fruitful to visit the vendor's facilities to see firsthand what security protocols are being utilized at the time and how they are being implemented. Yet, even if the nature of the information that will be shared does not merit a site visit, a vendor should have no objection to formally representing, in one form or another, in the relevant agreement that it utilizes and appropriately maintains the security protocols that it advertises it uses. The existence of this representation and warranty provides the company with a remedy if it is later revealed that, at the time the representation was made, the vendor did not actually conduct its business in the manner it advertised.

  PVLR ISSN 1538-3423

An audit right is a particularly difficult right to acquire, but if a company can negotiate for such a right, it always will provide a company with more information than it would have access to in its absence.

Because vendor contracts can survive indefinitely, the aforementioned representation is necessary but not sufficient since representations are made as of a fixed point in time. Accordingly, a company also would want contractual assurances (in the form of covenants) that the vendor's cybersecurity measures will advance with the times as the relationship progresses. In both cases, the remedy associated with a breach of the representation or the covenant will be vital. Indeed, if noncompliance is severe enough, the company should have the right to immediately sever the relationship (without penalty) and promptly receive its sensitive data back[1].

The inclusion of an ''audit right'' that allows the company to visit the vendor's premises and inspect the security protocols that are being implemented at the time.

Assuring that sensitive information doesn't fall into the wrong hands has monetary value to every company. Yet, in the case of a company that provides sensitive information to a vendor, there is no contractual provision that can provide real time insight into (i) how a vendor is actually using such company's sensitive information or (ii) what measures the vendor is utilizing to ensure that such information doesn't fall into the wrong hands. If a company needs to know this information, only an audit right can provide it. That said, an audit right provides little value to a company if it isn't coupled with an appropriate remedy. In this case as well, if noncompliance is severe enough, the company should have the right to immediately sever the relationship (without penalty) and promptly receive its sensitive data back.

Because an audit right requires entering another company's physical space, if an audit can be conducted at all, there are always material restrictions on how and when they can be conducted. Typically there are also restrictions on the frequency in which they may be conducted (generally once a year).

[1] Although beyond the scope of this article, it is worth noting that there are often situations in which it is not possible for a vendor to return (or destroy) all of a company's sensitive information. This may be due to the fact that a copy must be kept for compliance reasons, because of logistical challenges associated with how such data was stored and/or used, etc.

In the event of a material data breach, the company should be able to immediately terminate the vendor contract (without penalty) and promptly receive its sensitive data from the vendor.

An audit right is a particularly difficult right to acquire. That said, if a company can negotiate for such a right, regardless of how restrictive the audit right ends up being in final documentation, it always will provide a company with more information than it would have access to in its absence.

The ability to terminate the contract in the event that the vendor is the subject of a material data breach, even if such breach does not impact the company's data.

In today's ultra-competitive environment, many vendors have to provide services for some minimum term (usually 12 months) in order to make a profit. With that in mind, in an effort to ensure that such contracts are not easily terminable, such contracts generally are only terminable upon a material breach. Typically what counts as a ''material breach'' isn't specifically defined.

Although quite common, this construct is particularly problematic from a cybersecurity perspective for at least two reasons. First, it often takes a material amount of time to uncover exactly what data has been exposed in the case of a data breach. Second, even after a company that is a client of a vendor that is the subject of a material data breach can confirm that a portion of its data has been exposed, in order to terminate the contract pursuant to its terms, the company still must successfully demonstrate that such a breach amounts to a ''material breach'' of the contract.

For reputational reasons, any company that has shared sensitive information with a vendor that is the subject of a material data breach (whether or not such breach exposed all, or any portion of, the company's sensitive information) would prefer to be able to tell its clients that it promptly severed ties with such vendor to maintain (or begin the process of rebuilding) client confidence. This simply is not possible if the company must demonstrate a material breach of the contract before it can distance itself from such vendor.

Accordingly, a company should look to clearly define what will count as a ''material data breach'' and ensure that the company is privy to a specific remedy in the event that the vendor becomes the subject of a material data breach. Ideally, in the event of a material data breach, the company should be able to immediately terminate the vendor contract (without penalty) and promptly receive its sensitive data from the vendor.

An appropriate indemnity to make the company whole in the event that a data breach does expose the company's sensitive information.

In an effort to keep their pricing as competitive as possible (which requires being able to reasonably predict the financial exposure associated with each contract), most vendors include a blanket limitation of liability with no exceptions in their contracts. However, there are a number of exceptions to a blanket limitation

on liability that are appropriate, and a breach of the confidentiality provision is one.[2] Vendors are quick to remind a company that, regardless of what precautions the vendor takes, there is nothing it can do to ensure that its systems will not be compromised. This, of course, is irrefutable. However, from an allocation of risks standpoint, it is also most appropriate for the vendor to assume all, or a material portion of, that risk since the vendor determines what checks and balances it imposes with respect to the protection of its systems. Ultimately, in the case of a breach of the confidentiality provision (whether as a result of a data breach or otherwise), the indemnity should allow the company to recover its losses from dollar one without a cap.

Restrictions on Publicity

Vendors like to promote who their clients are in an effort to encourage other notable companies to use them as well. Vendors are often granted the right to do so pursuant to a publicity provision. As a general matter, material thought should be given to this provision as, sensitive data aside, most companies would like to approve how their name and logo are used, and under what circumstances. Yet, companies should be particularly wary of letting vendors use such company's name for advertising purposes if such vendor possess any of the company's sensitive information as, from a cybersecurity prospective, having a vendor publish who its clients are provides hackers who are looking to exploit a particular company's sensitive information with a road map as to where to look to do so. This is particularly true if the company's security protocols are superior to those of the vendor in question. In such a case, a direct attack may be less attractive than an indirect one.

Conclusion

Although it is impossible for a company that shares sensitive information with vendors to ensure that such sensitive information will remain confidential under all circumstances, there are steps that a company can take to minimize the probability of an indirect data breach and, in the event that a vendor that such company uses becomes the subject of a data breach, ensure that it can quickly mitigate the damage and recover any and all losses it may incur as a result of such data breach. This article has touched upon some of the more generally applicable ways to do so.

Ultimately, what protections are necessary for the company, and what concessions the vendor is willing to make in order to secure such company as a customer, will depend on the circumstances. However, since a company won't get something it doesn't ask for, it's vital for a company to know what its ''asks'' should be as it considers negotiating contracts with third party vendors in light of material cybersecurity considerations.

[2] Another exception that is particularly important relates to intellectual property. If the vendor misappropriates the company's intellectual property, losses associated with that breach should be excluded from the limitation of liability. Similarly, if it turns out that the vendor's product infringes on the intellectual property rights of a third party, any losses that the company incurs in connection therewith also should be excluded from the limitation of liability.

  PVLR ISSN 1538-3423

HUNTON& WILLIAMS

April 2016

Overview of the EU General Data Protection Regulation

Background

- **The existing law:** Current EU data protection law is based on Directive 95/46/EC (the "**Directive**"), which was introduced in 1995. Since that time, there have been significant advances in information technology, and fundamental changes to the ways in which individuals and organisations communicate and share information. In addition, the various EU Member States have taken divergent approaches to implementing the Directive, creating compliance difficulties for many businesses.
- **The changes:** The EU's legislative bodies have reached a political agreement on an updated and more harmonised data protection law (the "**Regulation**"). The Regulation will significantly change EU data protection law, strengthening individual's rights, expending the territorial scope, increasing compliance obligations and expanding regulator enforcement powers. The formal adoption is expected in Spring 2016, with the Regulation applying from Spring 2018. Organisations will have two years to implement changes to their data protection compliance programmes, business processes, and IT infrastructure to reflect the Regulation's new requirements.

Impact of the Regulation on Businesses

Key:  **This change is broadly positive for most businesses**  **This change is broadly negative for most businesses**  **This change is broadly neutral for most businesses**

 **Some concepts will change:** The Regulation will introduce ***a number of new concepts and approaches***, the most significant of which are outlined below. The Regulation is also designed to be more future-proof and forward looking than the Directive, and as technology-agnostic as possible.

 **Some concepts will stay the same:** ***Many of the existing core concepts under the Directive will*** broadly similar in both the Directive and the Regulation. These concepts are not addressed further below.

 **Increased enforcement powers:** Currently, fines under EU Member State law vary, and are comparatively low (e.g., the UK maximum fine is £500,000). The Regulation will significantly increase the ***maximum fine to €20 million, or 4% of annual worldwide turnover***, whichever is greater. In addition, national data protection supervisory authorities will be co-ordinating their supervisory and enforcement powers across the EU Member States, likely to lead to a more pronounced enforcement impact and risk for businesses.

 **Greater harmonisation:** The Regulation introduces a single-legal framework that applies across all EU Member States without the need for national implementation. This means that businesses will face a ***more consistent set of data protection obligations*** from one EU Member State to the next, which should aid overall compliance. However, harmonisation will not be complete and some differences will persist across the EU Member States.

 **Expanded territorial scope:** Non-EU businesses will be subject to the Regulation if they: (i) offer goods or services to EU residents; or (ii) monitor the behaviour of EU residents. Many non-EU businesses that were not required to comply with the Directive ***will be required to comply with the Regulation***.

 **Consent, as a legal basis for processing, will be harder to obtain:** Under the Regulation, individuals' consent must be freely given, specific, informed and unambiguous. Consent may not be valid if it is bundled with other matters, part of the general terms of conditions, or there is a "clear imbalance" between the parties. Organisations will be required to demonstrate that consent was given. Mere acquiescence (e.g., failing to un-tick a pre-ticked box) does not constitute valid consent

under the Regulation. Businesses that rely on consent to process personal data will need to carefully review their existing practices.

The risk-based approach to compliance: The Regulation acknowledges a risk-based approach to compliance, under which businesses would bear responsibility for assessing the degree of risk that their processing activities pose to individuals. ***Low-risk processing activities face a reduced compliance burden.*** On the other hand, documented ***data protection impact assessments*** will be required for high-risk processing activities. These compliance steps will need to be integrated into future product cycles.

The 'One-Stop Shop': Currently, a Data Protection Authority ("**DPA**") may exercise authority over businesses established in its territory or otherwise falling within its jurisdiction. Under the Regulation, where a business is established in more than one EU Member State, the supervisory authority ("**SA**") of the main establishment of the business will act as the lead authority for data processing activities that have an impact throughout the EU and will co-ordinate its work with other SAs. In addition, each SA will have jurisdiction over complaints and possible violations of the Regulation in their own Member State.

Data protection by design and by default: Businesses will be required to implement data protection ***by design*** (e.g., when creating new products, services or other data processing activities) and ***by default*** (e.g., by implementing data minimisation techniques). They will also be required to perform data protection impact assessments to identify privacy risks in new products.

Data Protection Compliance Programmes — Internal processing records and Data Protection Officer: Organisations will have to implement and be able to demonstrate to the SA that they have comprehensive data protection compliance programmes, with policies, procedures and compliance infrastructure. For example, instead of registering with a SA, the Regulation will require businesses to ***maintain a record*** of processing activities. Also, organisations must appoint a data protection officer ("**DPO**") where (1) they are a public authority or body; (2) the core activities of the controller or processor require regular and systematic monitoring of individuals on a large scale; (3) the core activities of the controller or processor include processing certain types of data on a large scale, including data relating to criminal convictions and offences; or (4) required by Member State law. Businesses should: (i) review their existing compliance programmes, and ensure that those programmes are updated and expanded as necessary to comply with the Regulation; (ii) ensure that they have clear records of all of their data processing activities, and that such records are available to be provided to SAs upon request; and (iii) consider appointing a DPO.

New obligations of processors: The Regulation introduces ***direct compliance obligations for processors***. Under the Directive, processors generally are not subject to fines or other regulatory penalties. In an important change, under the Regulation processors may be liable to pay ***fines of up to €20 million, or 4% of annual worldwide turnover***, whichever is greater. The Regulation also requires detailed provisions in third-party processing contracts. This will have an impact on both controllers and processors, as they identify their processor agreements, review their commercial and legal positions for future agreements and renegotiate existing agreements.

Strict data breach notification rules: The Regulation will require businesses to notify the SA of data breaches ***within 72 hours***. If the breach has the potential for serious harm, individuals will have to be notified without undue delay. Businesses will need to develop and implement a data breach reporting and response plan (including designating specific roles and responsibilities, training employees, and preparing template notifications) enabling them to react promptly in the event of a data breach. The breach notification rule is likely to increase the risk profile for businesses, as their security breaches may get into public domain and attract attention of regulators and media.

Overview of the EU General Data Protection Regulation

Pseudonymisation: The Regulation introduces a concept of ***'pseudonymised data'*** (i.e., key-coded or enhanced data). Pseudonymous data will still be treated as personal data, but is likely to help organisations comply with the Regulation and reduce the risks of non-compliance. The 'key' necessary to identify individuals from the pseudonymised data must be kept separately and subject to technical and organisational measures to ensure non-attribution to an identified or identifiable person.

Binding Corporate Rules ("BCRs"): BCRs are binding data protection corporate policies and programmes that are used to lawfully transfer personal data globally within a group of companies. The Regulation formally recognises BCRs. They will still require SA approval, but the approval process should become ***less onerous than the current system***. BCRs are available to both ***controllers and processors***.

The 'right to be forgotten': Under the Regulation, individuals will have the ***right to request that businesses delete their personal data*** in certain circumstances (e.g., the data is no longer necessary for purposes for which it was collected). As a result, businesses will need to devote additional time and resources to ensuring that these requests are appropriately addressed. In particular, businesses should consider how they will give effect to the right to be forgotten, as deletion of personal data is not always straightforward.

The right to object to 'profiling': Under the Regulation, individuals will have the right to object to profiling on grounds relating to their particular situation. ***'Profiling'*** is defined broadly and includes most forms of online tracking and behavioural advertising, making it harder for businesses to use data for these activities. Businesses that regularly engage in profiling activities (e.g., in the advertising or social media context) will need to consider how to best implement appropriate consent mechanisms in order to continue these activities.

The right to Data Portability: Individuals will have ***the right to obtain a copy of their personal data from the controller in a commonly-used format and have it transferred to another controller.*** Consumer-based businesses (e.g., social media businesses, insurance companies, banks, telecommunication providers) should consider how they will give effect to these rights. Many new-to-market online businesses may welcome this new development as a way to improve competition in the sector while established providers will view it in less beneficial terms.

Contacts

Hunton & Williams

Bridget Treacy
+44 (0) 20 7220 5731
BTreacy@hunton.com

Wim Nauwelaerts
+32 (0)2 643 5814
WNauwelaerts@hunton.com

Hunton & Williams LLP

Lisa J. Sotto
+1 (212) 309 1223
LSotto@hunton.com

Aaron Simpson
+1 (212) 309 1126
ASimpson@hunton.com

Centre for Information Policy Leadership

Bojana Bellamy
+44 (0) 20 7220 5703
BBellamy@hunton.com

privacy@hunton.com

大成DENTONS

IREG Update

The NAIC takes on cybersecurity

May 26, 2016

- **Hot Topic: Key changes for ACA CO-OP boards: a look at new regulations taking effect this week**
- **ICYMI: Noteworthy links from the past two weeks**

The NAIC takes on cybersecurity

The subject of cybersecurity risks, which the National Association of Insurance Commissioners' Chief Security and Information Officer Frosty Mohn presented at NAIC's Insurance Summit in Kansas City, MO last week, has taken on greater significance as consumer financial and health information is increasingly being stored in electronic form. Cyber risks include identity theft or inadvertent disclosure; theft of digital assets, such as customer lists and trade secrets; business interruption from a network shutdown; introduction of malware; and damage to a business's reputation. In response to these relatively new risks, insurance regulators have begun urging businesses to secure cyber-liability insurance and pressing insureds to shore up their defenses against cyber attacks.

In April 2015, the NAIC's Cybersecurity (EX) Task Force adopted and issued **12 Principles for Effective Cybersecurity: Insurance Regulatory Guidance**. The NAIC Guidance encouraged insurers and regulators to join forces in identifying risks and adopting practical solutions to protect the critical information entrusted to them.

The Task Force also developed the **NAIC Roadmap for Cybersecurity Consumer Protections (Roadmap)**, which was adopted by the NAIC Executive (EX) Committee at the end of 2015. The NAIC Roadmap details what protections the NAIC believes consumers are entitled to expect from insurance companies, agents and other businesses following a data breach.

To gather financial performance information about insurers writing cyber-liability coverage, the Task Force also has worked with the NAIC's Property and Casualty Insurance (C) Committee and Financial Condition (E) Committee to develop a "Cybersecurity and Identify Theft Coverage

Key contacts

Matthew J. Gaul
Partner
New York
D +1 212 398 5835
matthew.gaul@dentons.com

Kara Baysinger
Partner
San Francisco/Oakland
D +1 415 882 2475
kara.baysinger@dentons.com

Bruce E. Baty
Partner
Kansas City
D +1 816 460 2495
bruce.baty@dentons.com

Supplement" to be included with insurer financial statements.

The NAIC also recommends that businesses secure a cyber-liability policy, noting that most standard commercial policies do not cover many of the cyber risks noted above. But cyber risks remain difficult for underwriters to quantify. The lack of actuarial data requires that insurers qualitatively assess the business's risk management procedures and culture, and insurers writing such coverage will want to know the business's risk-management techniques for protecting its network and assets, its antivirus and anti-malware software, how its employees and others are able to access data systems, and its data breach response plan.

Because cyber risk policies are more customized than many other types of risk that insurers take on, they tend to be more costly. Such policies might include one or more of the following types of coverage: liability for security or privacy breaches; the costs associated with a privacy breach, such as consumer notification, customer support and costs of providing credit monitoring services to affected consumers; and the costs associated with business interruption.

The NAIC, insurance companies and the world at large are becoming increasingly aware of the importance of cybersecurity issues. We will continue to stay at the forefront of these changes and publish updates as they arise.

ICYMI...

Noteworthy links from the past two weeks

General

- An environmental advocacy group claimed the insurance industry is overly exposed to energy investments that may be negatively impacted by climate change [**Bloomberg**]
- Federal Reserve Governor Turillo discussed upcoming risk based capital rules for Systemically Important Financial Institutions [***Law360***, **Business Insurance**, **Reactions**]

Property and Casualty

- The Federal Emergency Management Agency announced changes to the National Flood Insurance Program in response to Sandy [***Wall Street Journal***]
- The usage-based auto insurance business continued to grow [**Insurance Journal**]

Life and Health

- Minnesota sued some life insurers over unclaimed benefits [**CBS Minnesota**]
- The Supreme Court punted on its Affordable Care Act contraception case [***The New York Times***]

The IREG Update is edited by **Matt Gaul**

HUNTON& WILLIAMS

Lawyer Insights

July 19, 2016

The EU-US Privacy Shield: A How-To Guide

by Lisa J. Sotto and Christopher D. Hydak

Published in Law360

The EU safe harbor framework, unveiled in 2000, allowed certified U.S. companies to receive personal data of EU residents in compliance with EU cross-border data transfer rules. The safe harbor served as a popular data transfer mechanism for U.S. companies — more than 4,000 businesses had certified to the safe harbor, including many service providers whose ability to legally transfer data to the U.S. allowed thousands of other businesses to comply with EU data transfer restrictions. Despite its popularity, however, 15 years after the safe harbor was rolled out by European and U.S. regulators, it was declared invalid by the stroke of a pen held by the Court of Justice of the European Union. The CJEU's opinion was largely motivated by the belief that the safe harbor, and U.S. law in general, did not adequately protect the fundamental rights and freedoms of EU individuals whose information was transferred to the U.S. pursuant to the safe harbor because there were not sufficient restrictions on the U.S. government's ability to grab that data once in the hands of U.S. companies.

Four months after the CJEU invalidated the safe harbor, in February 2016, the European Commission released the EU-U.S. Privacy Shield. The Privacy Shield was designed to replace the safe harbor and cure the deficiencies identified by the CJEU. Following its issuance, a number of EU-based government bodies (including the Article 29 Working Party, European Parliament and European Data Protection Supervisor) and consumer privacy advocates criticized aspects of the shield. In an effort to address the concerns, EU and U.S. regulators renegotiated and revised a few sections of the Privacy Shield text, including those involving onward transfers and data retention. A revised version of the Privacy Shield was formally adopted on July 12, 2016, as a successor to the now-defunct safe harbor.

The U.S. Department of Commerce has indicated that it will begin accepting certifications from U.S. companies on Aug. 1, 2016. Commerce worked quickly to release in July 2016 a guide to self-certification and FAQs.

Purpose of the Privacy Shield

EU data protection law generally prohibits the transfer of personal data outside of the EU unless the transfer (1) is to a jurisdiction that is deemed by the EC to provide an "adequate" level of protection for EU personal data, (2) falls within one of the few exceptions, or (3) is made in accordance with one of a small number of legal data transfer mechanisms. There are few "adequate" jurisdictions globally and the U.S. is not one of them. The exceptions, which include consent of the relevant individual, are ill-suited to routine and systematic business transfers. With respect to legal mechanisms for transferring EU personal data, the Privacy Shield is one of the few methods available, along with standard contractual clauses and binding corporate rules, by which personal data can be legally transferred from the EU to the U.S. Unlike

standard contractual clauses and binding corporate rules, the Privacy Shield is available only to companies in the U.S. and applies only to data transfers from the EU to the U.S.

Privacy Shield Requirements

To use the Privacy Shield as a data transfer mechanism, similar to the safe harbor, U.S. companies must commit to comply with seven principles governing the handling of personal data received in the U.S. via the shield. The seven principles that comprise the Privacy Shield are comparable to those of the safe harbor. The names of the principles have changed slightly, more detail has been added to certain of the principles, and a few new items have been included. Generally, however, companies that previously were certified to the safe harbor will be able to transition to the Privacy Shield without an extensive review or alteration of their processes for handling personal data received from the EU.

The Privacy Shield principles, along with brief descriptions of each principle, are as follows:

1. Notice — Organizations must inform relevant EU data subjects of thirteen enumerated data handling practices, such as the types of personal data the entity collects and how it uses the data.

2. Choice — Companies must offer individuals the opportunity to opt out if their personal data is to be (a) disclosed to a third party (except agents) or (b) used for a purpose that is materially different from the purpose for which it was originally collected or subsequently authorized.

3. Accountability for Onward Transfer — Businesses must enter into written contracts with third parties to whom they transfer personal data received from the EU; those contracts must contain specific protections for the data.

4. Security — Organizations must take reasonable and appropriate measures to protect personal data from loss, misuse and unauthorized access, disclosure, alteration and destruction.

5. Data Integrity and Purpose Limitation — Entities must (a) limit personal information to that which is relevant for the purposes of the relevant processing, (b) take reasonable steps to ensure personal data is reliable for its intended use and is accurate, complete and current, and (c) retain personal data only for as long as it serves a purpose of the relevant processing.

6. Access — Companies must provide relevant EU individuals with access to the personal data the organization holds about them, as well as the ability to correct, amend or delete that information where it is inaccurate or has been processed in violation of the Privacy Shield.

7. Recourse, Enforcement and Liability — Businesses must implement robust mechanisms for assuring compliance with the Privacy Shield, including an independent recourse mechanism for complaints and procedures for verifying the privacy representations made to individuals.

The seven principles of the Privacy Shield are complemented by 16 supplemental principles that provide more detail regarding specific data transfer issues, such as the processing of human resources information or sensitive data. Because the principles are designed to reflect the protections for personal data and rights granted to data subjects under EU law, companies with operations in the EU should be familiar with the substance of the shield's requirements.

Why Certify?

Like the safe harbor, the Privacy Shield is expected to be popular among U.S. companies seeking to receive personal data from the EU. The Privacy Shield is more flexible, more convenient and less costly for companies to implement than other available data transfer mechanisms. For example, standard contractual clauses often are viewed as an administrative nightmare. All relevant legal entities may need to sign the clauses (including all data exporters and importers), certain EU member states require data exporters to submit the clauses, and other EU member states mandate regulatory approval of the clauses before transfers may commence. In addition, standard contractual clauses contain provisions that many data importers find onerous, such as the requirement to submit data processing facilities to audits by the data exporter and to obtain the exporter's consent to provide subcontractors with access to personal data. Binding corporate rules require the approval of EU data protection authorities and generally involve a lengthy and costly process. A large multinational organization could expect to spend well over a year and expend significant resources (both monetary and otherwise) to implement binding corporate rules.

Organizations that will derive the most benefit from the availability of the Privacy Shield are those that route the majority of their EU-originating personal data from the EU to the U.S. For example, a U.S.-based company whose Texas headquarters serves as the global hub for the organization's data will find the Privacy Shield particularly useful. If the company certifies to the shield, it can legally transfer EU personal data to the U.S. The company also will be allowed to transfer the personal data to third-party recipients who have signed an "onward transfer" agreement prepared by the company. Organizations that transfer their EU data directly to countries other than the U.S. generally will not be able to take advantage of the Privacy Shield.

To induce companies to certify early, the Privacy Shield contains a narrow nine-month grace period for organizations that certify within the first two months of the Privacy Shield's effective date. Businesses that certify during this two-month window will have a nine-month transition period to bring their existing contracts with onward transfer recipients into compliance with the Privacy Shield. Companies that certify more than two months after the effective date must have all of their shield-related onward transfer agreements in place on the date of certification.

Enforcement

Certifying to the Privacy Shield imposes a legal commitment to comply with the seven principles of the shield. The Federal Trade Commission and the U.S. Department of Transportation are authorized to enforce against violations of the Privacy Shield. Companies that certify and fail to comply with the shield are subject to enforcement by these regulators. The FTC, which is the principal U.S. enforcement agency with respect to the shield, brought nearly 40 enforcement actions for violations of the safe harbor. The FTC is expected to be even more active in enforcing compliance with the Privacy Shield. A company that violates the requirements of the shield likely would enter into a consent order imposing stringent data handling obligations for 20 years.

Future of the Privacy Shield

The EC's decision validating the Privacy Shield is based on Directive 95/46/EC, which is the current data protection regime in the EU. As has been widely publicized, Directive 95/46/EC is set to expire on May 25, 2018, when its successor framework, the General Data Protection Regulation will take effect. The GDPR will fundamentally transform the EU data protection regime. While deemed to provide adequate protection to personal data under Directive 95/46/EC, the Privacy Shield may not be found adequate under the GDPR.

A more likely risk, as evidenced by the demise of the safe harbor, is a CJEU decision to overturn the Privacy Shield's adequacy decision in response to a legal challenge. While such a challenge appears inevitable, and the CJEU's response to such a challenge is difficult to predict, the Privacy Shield is expected to fare better than the safe harbor because the shield's provisions were specifically drafted to address the inadequacies identified by the CJEU in the safe harbor.

There is reason to be optimistic about the future of the Privacy Shield. Unlike the safe harbor, the shield will undergo a joint annual review by EU and U.S. authorities. Should material concerns arise, they can be addressed through ongoing revisions to the text. The safe harbor framework was static and became stale over time. By its nature, the annual review process will ensure that the shield remains current.

Given the changes in technology and world events since 2000, an overhaul of the safe harbor was inevitable, particularly in light of the Snowden revelations and the upcoming revamp of the EU data protection regime. The Privacy Shield was the result of three years of negotiation by EU and U.S. authorities. The final product shows the significant efforts on the part of the negotiating team to address all outstanding concerns so as to leave little room for questions regarding the adequacy of the protections provided by the shield to EU residents' personal data. The text of the shield was carefully crafted to satisfy EU concerns about its predecessor regime's lack of rigor in key areas, such as the ability of U.S. law enforcement to access EU personal data, redress for EU residents, and the onward transfer of data to third parties. The European Commission's approval of the shield is a win for global commerce. The enhanced protections provided to EU data are a win for EU privacy rights. All in all, the new EU-U.S. Privacy Shield is a coup for all stakeholders.

Lisa J. Sotto is a partner and chair of the global privacy and cybersecurity practice at Hunton & Williams in New York. She assists clients in identifying, evaluating and managing privacy and information security law risks. She may be reached at (212) 309-1223 or lsotto@hunton.com. Christopher D. Hydak focuses his practice on privacy, data security and information management issues. He may be reached at (212) 309-1012 or chydak@hunton.com.

Bloomberg BNA

Privacy and Security Law Report®

EU-U.S. Privacy Shield

After a long and twisting diplomatic process, the EU-U.S. Privacy Shield formally became effective for companies to use on Aug. 1, 2016. The annual review process will inevitably result in further tweaks and improvements, and it cannot be excluded that the Privacy Shield will be challenged before regulators or courts, but despite these ongoing challenges, the Privacy Shield's recent adoption constitutes a step in the right direction for both businesses and their customers and employees, the authors write.

The Privacy Shield Gets the Green Light from the European Union

By Aaron Simpson and Anna Pateraki

After a long and twisting diplomatic process, the EU-U.S. Privacy Shield (Privacy Shield or Shield) formally became effective for companies to use on Aug. 1, 2016. The U.S. Department of Commerce has developed a website for the Privacy Shield framework and has announced that it will stop accepting new Safe Harbor framework (Safe Harbor) submissions as of Aug. 1, 2016 and re-certifications as of Oct. 31, 2016. In parallel, the European Commission has updated its website to include the Privacy Shield in its list of European Union adequacy decisions and has published a Guide for citizens explaining their rights and remedies in the context of the Privacy Shield.

Background

Similar to the Safe Harbor before it, the Privacy Shield is a legal mechanism that allows companies in the EU to comply with data transfer restrictions when they transfer personal data to entities in the U.S. that have publicly certified their adherence to the new framework. For a detailed description of Privacy Shield, see Aaron Simpson, ''*European Commission Presents EU-U.S. Privacy Shield*,'' Pratt's Privacy & Cybersecurity Law Report, May 2016.

The Privacy Shield is comprised of seven principles and 16 supplemental principles inspired by EU data protection law that organizations must publicly proclaim their compliance if they intend to certify. The *seven principles* are: (1) Notice; (2) Choice; (3) Accountability for Onward Transfers; (4) Security; (5) Data Integrity and Purpose Limitation; (6) Access; (7) Recourse, Enforcement and Liability. The *16 supplemental principles* are: Sensitive data; Journalistic Exceptions; Secondary Liability; Performing Due Diligence and Conducting Audits; The role of Data Protection Authorities; Self-Certification; Verification; Access; Human Resources Data; Obligatory Contracts for Onward Transfers; Dispute Resolution and Enforcement; Choice – Timing of Opt-Out; Travel Information; Pharmaceutical and Medical Products; Public Record and Publicly Available Information; Access Requests by Public Authorities.

When compared to its predecessor, the Privacy Shield imposes stricter obligations on companies with respect to onward transfers, redress mechanisms for individuals and data access by public authorities. The framework itself is also subject to enhanced supervision and is intended to result in more enforcement. In order to ensure the framework remains a living and breathing

 ISSN 1538-3423

construct, it also includes an annual joint review mechanism by the EU and the U.S. that allows for continual improvements to be made to the framework.

The Privacy Shield was adopted on July 12, 2016, following an adequacy decision by the European Commission (15 PVLR 1478, 7/18/16). The adequacy decision on the Privacy Shield replaces the EU-U.S. Safe Harbor adequacy decision which was invalidated by the Court of Justice of the EU on Oct. 6, 2015, primarily due to concerns in relation to law enforcement and judicial redress issues. The Privacy Shield is the result of an almost three-year negotiation process between EU and U.S. officials that was initiated in the aftermath of Edward Snowden's revelations in 2013.

The Article 29 Working Party will be focused on the necessity and proportionality of data access requests made by public authorities and the potential impact that such an assessment may have on other data transfer mechanisms.

The Statement of the Article 29 Working Party

On July 26, 2016, the Article 29 Working Party (Working Party) issued a short statement welcoming the improvements made on the Privacy Shield following its non-binding opinion from April 2016 and outlining its remaining concerns, which include the following:

- **Commercial aspects:** The Working Party believes that further improvements should be made to introduce more specific rules on automated decision-making and a general right to object (according to point 25 of the EU Commission implementing decision on the Privacy Shield, automated decision-making will be re-examined in the course of the first annual joint review). The Working Party also would like to see more clarification on how the Privacy Shield Principles apply to data processors, which was also an issue under the Safe Harbor.
- **Data access by U.S. authorities:** The Working Party states that it expected stricter guarantees concerning the independence and the powers of the Ombudsperson under the Shield. The Ombudsperson is a function intended to sit within the U.S. Department of State. Its mission is to handle complaints and inquiries received from EU individuals regarding access to their commercial data by U.S. intelligence authorities. Furthermore, the Working Party acknowledged the commitment of the U.S. Office of the Director of National Intelligence (ODNI) to avoid mass and indiscriminate personal data collection, but the Working Party remained skeptical given no assurances were provided that the practice would not occur.

Despite these remaining concerns, the Privacy Shield is officially a legally valid data transfer mechanism for EU-U.S. data transfers. Therefore, the statement of the Working Party did not impact the Privacy Shield's implementation as a practical matter. That being said, such statements from the Working Party do have political value, and they likely will impact the annual review process that will be undertaken in accordance with the Shield. In its recent statement, the Working Party committed to await next year's first EU-U.S. joint annual review to further assess the effectiveness of the Shield. In particular, the Working Party will be focused on the necessity and proportionality of data access requests made by public authorities and the potential impact that such an assessment may have on other data transfer mechanisms.

In addition, the regulators participating in the Working Party have committed to proactively assist individuals with lodging complaints against Privacy Shield-certified organizations. The Working Party stated that it will provide guidance to data controllers about their obligations under the Privacy Shield. It also will provide suggestions on the composition of the ''EU centralized body'' to be created by the Shield to review individuals' law enforcement complaints, as well as the modalities of the joint review mechanism.

Implications for Businesses

For many businesses, the news of the Privacy Shield's formal adoption is a welcome relief. As a practical matter, the obligations for companies wishing to certify to the Shield are similar to the Safe Harbor framework, with a few key differences as described below:

- **Privacy notices:** The Privacy Shield's Notice principle requires companies to provide a privacy notice that includes specifically prescribed content across a range of areas, including with respect to the company's data processing activities, available recourse mechanisms, onward transfers and potential data disclosure to public authorities for national security and law enforcement purposes. Therefore, organizations wishing to join the Privacy Shield should have their privacy policies reviewed and updated as needed.
- **Choice to opt out:** Companies must offer individuals the choice to opt out if they will share personal data with a third party controller or if they use the personal data for a purpose that is materially different from the purpose for which it was originally collected or subsequently authorized. Individuals must be provided with clear, conspicuous and readily available mechanisms to opt out. Note that the opt out requirement only applies when personal data is being disclosed to a third party who uses the data for its own purposes. It does not apply when personal data is disclosed to an agent processing the data on behalf of the controller as long as an appropriate contract is in place.
- **Onward transfer agreements:** The Privacy Shield requires adherents to implement appropriate onward transfer agreements when personal data received from the EU is transferred onward to either

  PVLR ISSN 1538-3423

agents (*i.e.*, data processors) or third-party controllers. Such agreements with data controllers should provide that EU personal data may only be processed for limited and specified purposes and that the third-party recipient will provide the same level of protection for the data as is provided by the Privacy Shield Principles. In addition, the Privacy Shield-certified organizations must conduct specific diligence when sharing EU personal data with agents and will need to be prepared to provide a summary or a copy of the relevant onward transfer agreements to the Department of Commerce upon request. Ultimately, the Privacy Shield adherent will remain liable if its agent processes personal data in a manner inconsistent with the Privacy Shield Principles. Therefore, businesses will need to review their onward transfer arrangements to ensure appropriate onward transfer provisions are in place.

- **Withdrawal:** An organization that certifies to the Privacy Shield and subsequently leaves the framework will continue to be bound by its Principles and will continue to be liable for the processing if it keeps and does not return or delete the personal data processed under the Privacy Shield. In such cases, the business is required to affirm to the Department of Commerce on an annual basis its commitment to continue to comply with the Privacy Shield Principles for the retained data for as long as it retains that data.

- **Redress mechanisms:** Organizations are required to establish redress mechanisms provided for in the Privacy Shield. For example, organizations will need to implement a process internally that allows them to review and respond to individuals' complaints within 45 days. In addition, organizations will need to set up an Alternative Dispute Resolution process which will be free of charge for individuals, and be prepared to bear additional costs when redress is sought by other means (such as when individuals lodge complaints with the regulator in their country which will then be forwarded to the Department of Commerce and the Federal Trade Commission in the U.S., or when the binding arbitration of the Privacy Shield Panel is triggered).

Although there is a significant effort that will go into a company's Shield certification to ensure the public representations can be made accurately, organizations that were previously certified to Safe Harbor will be in a relatively advanced position as a relative matter given the similarities between the two frameworks. These companies should be able to leverage their existing Safe Harbor compliance program to certify with the Privacy Shield without upending their current data practices.

Companies should be able to leverage their existing Safe Harbor compliance program to certify with the Privacy Shield without upending their current data practices.

The Role of EU Data Protection Authorities

The Privacy Shield contains a supplemental principle on ''The Role of the Data Protection Authorities,'' according to which companies can select to cooperate with the EU regulators instead of another Alternative Dispute Resolution mechanism. In such cases, the company is required to respond promptly to inquiries from the handling authority designated by the panel of EU Data Protection Authorities (DPAs). This will be an informal panel of EU DPAs created in an effort to ensure a harmonized approach. The EU panel will provide advice to the U.S. organizations concerning unresolved complaints from individuals. It is not yet clear what the composition of the EU panel will look like, however, failure to comply with the advice of the EU panel can trigger enforcement by the Federal Trade Commission.

Overall, EU DPAs will be substantially involved in the monitoring of the Privacy Shield and in assisting individuals with lodging complaints. Individuals can always complain directly to their national DPA who will cooperate with the Department of Commerce and the Federal Trade Commission. Also, the EU DPAs are expected to play a significant role in the context of the Ombudsperson mechanism for reviewing complaints relating to law enforcement operations. As complaints from individuals steadily increase in number, enforcement by EU DPAs will also most likely increase in the future. It is expected that organizations will be subject to significantly more scrutiny and enforcement in the context of the Privacy Shield than they experienced under Safe Harbor.

Outlook

Although further tweaks and improvements will inevitably result from the annual review process, the Privacy Shield is officially a valid legal mechanism for EU-U.S. data transfers. Despite the remaining concerns of the Working Party, depending on a company's data flows, the Privacy Shield can be implemented by companies subject to the Federal Trade Commission's unfair competition authority either alone or in combination with other data transfer mechanisms.

It cannot be excluded that the Privacy Shield will be challenged before regulators or courts, however, the same is true for other data transfer mechanisms. Taken together, the challenges to data transfer mechanisms appear more focused on the foundational questions associated with cross-border data transfers generally and less focused on the specifics of a particular data transfer mechanism. Despite these ongoing challenges, the Privacy Shield's recent adoption constitutes a step in the right direction for both businesses and their cus-

tomers and employees.

   ISSN 1538-3423

Deloitte.

Assessing cyber risk

Critical questions for the board and the C-suite

Risk powers performance.

Risk powers performance.

Risk has traditionally been viewed as something to be minimized or avoided, with significant effort spent on protecting value. However, we believe that risk is also a creator of value and, approached in the right way, can play a unique role in driving business performance.

Take the issue of cyber risk. Increased use of technology and globalization are key drivers of cyber risk, but they are also key sources of competitive advantage. Organizations that pull back from these drivers to try and protect value will likely fall behind, while organizations that find better ways to manage cyber risk can power superior performance through increased use of technology and globalization.

A key step on this journey is understanding the current state of your organization's cyber capabilities. This guide and self-assessment tool is designed to help leaders gauge their cyber maturity, build new cyber risk understanding, and answer key questions, including:

- Do we have the right leader and organizational talent?
- Are we focused on, and investing in, the right things?
- How do we evaluate the effectiveness of our organization's cyber risk program?

Today's leading organizations are those that have learned how to protect their value through risk management. Tomorrow's leaders will be those that recognize the opportunity for risk to also create value. Deloitte's Risk Advisory professionals around the world can guide you on that journey and help you transform your organization into a place where risk powers performance.

To learn more, please visit us at www.deloitte.com/risk.

Owen Ryan
Global Risk Advisory Leader

Risk responsibility

Cyber risk is an imperative for everyone within the enterprise—but ultimate responsibility for overseeing risk rests with top leaders.

Many board members and C-suite executives, however, are far removed from the day-to-day challenges of monitoring, detecting, and responding to evolving cyber risks. Those leaders who develop a deeper view into where their organization stands when it comes to cyber risk can gain critical understanding for better managing the business.

Effective cyber risk management starts with awareness at the board and C-suite level. Sharpening your ability to understand risk, manage performance, and move your organization closer to cyber maturity often begins with answering important questions—and should result in becoming a more secure, vigilant, and resilient business. All three traits are critically important today—although cyberthreat management traditionally has focused on "secure" while paying less attention to "vigilant" (comprehensively monitoring the extensive threat landscape) and "resilient" (responding to and recovering from attacks). Here's an in-depth look at 10 must-answer questions that can help top leaders better comprehend where they stand when it comes to "secure, vigilant, resilient."

1. Do we demonstrate due diligence, ownership, and effective management of cyber risk?
2. Do we have the right leader and organizational talent?
3. Have we established an appropriate cyber risk escalation framework that includes our risk appetite and reporting thresholds?
4. Are we focused on, and investing in, the right things? And, if so, how do we evaluate and measure the results of our decisions?
5. How do our cyber risk program and capabilities align to industry standards and peer organizations?
6. Do we have a cyber-focused mindset and cyber-conscious culture organization wide?
7. What have we done to protect the organization against third-party cyber risks?
8. Can we rapidly contain damages and mobilize response resources when a cyber incident occurs?
9. How do we evaluate the effectiveness of our organization's cyber risk program?
10. Are we a strong and secure link in the highly connected ecosystems in which we operate?

Boards and C-suite play a critical role in helping their organizations respond to the constantly evolving cyberthreat landscape.

Cyberthreats and attacks continue to grow in number and complexity—all while the business world grows increasingly connected and digital. Amid this new landscape, managing cyberthreats becomes a business and strategic imperative, with the stakes higher than ever. These days, cybercrime involves more than fraud and theft. As the domain of vast criminal networks, foreign government-sponsored hackers, and cyber terrorists, cybercrime extends across the risk spectrum—to involve disruption of services, corruption or destruction of data, and even "ransomware" activities that seek to extort money, access, or corporate secrets from victims.

Today, cyber risk and performance are more tightly intertwined. Tangible costs from cybercrime range from stolen funds and damaged systems to regulatory fines, legal damages, and financial compensation for affected parties. Intangible costs could include loss of competitive advantage due to stolen intellectual property, loss of customer or business partner trust, and overall damage to an organization's reputation and brand. Beyond the damage to individual organizations, the sheer scope of cyberattacks now has the potential to cause mass-scale infrastructure outages and potentially affect the reliability of entire national financial systems and the well-being of economies.

Top-tier issue

With so much at stake, the board and C-suite increasingly realize that cyber risk must be treated as a top-tier business risk, requiring a level of awareness deeply embedded in the culture of the enterprise. As every aspect of business today touches on some digital component, cyber risk concerns stretch well beyond IT and well beyond the walls of the enterprise—to every partner, to every customer, to every worker, and to every business process.

Realizing that at some point the organization will be breached, leaders should work to understand the most significant threats and how those threats can put mission-critical assets at risk. As boards and the C-suite take a more active role in protecting their organizations, many will struggle to ensure that their efforts are effective. What are their responsibilities? Which competencies should they be cultivating? What are the right questions to ask? Faced with such questions and an evolving threat landscape, preparing for every possibility can prove daunting. So planning for what's probable—not just possible—offers a prudent path forward for leaders.

There's no blanket solution to the challenge, but the board and C-suite leaders can begin developing a custom cybersecurity program or improve an existing one. The 10 key questions that we lay out in the following pages should promote boardroom discussions around management's ongoing cyber strategies, how leaders effectively address evolving challenges, how they mitigate cyber risks, and how they anticipate opportunities.

Assess your maturity level

This list of key cyber risk questions and accompanying range of responses should effectively guide organizations in assessing their cyber posture, challenge information security teams to ask the right questions and provide critical information, and help consistently monitor and improve cyber resilience going forward.

These questions are designed to help you identify specific strengths and weaknesses, as well as paths to improvement. Determine where your organization's responses to the following questions fall on the cyber maturity scale:

Cybersecurity maturity scale

High maturity

We have a strong cyber risk posture within the organization.

Moderate maturity

Cyber risk measures are in place; some work remains.

Low maturity

We are lagging on cyber risk management, with few measures in place and significant work to do.

What it means to be secure, vigilant, and resilient

Secure

Establish and continually maintain foundational security capabilities—by enhancing risk-prioritized controls to protect against known and emerging threats, while also complying with industry cyber standards and regulations.

Vigilant

Detect violations and anomalies through better situational awareness across the environment—within all areas of your ecosystem.

Resilient

Establish the ability to quickly return to normal operations and repair damage to the business following the inevitable cyberattack.

1 Do we demonstrate due diligence, ownership, and effective management of cyber risk?

Determining the right degree of accountability at the leadership level is essential. If oversight involves only a 5-minute update on cyber events every now and then, you're probably not doing enough to manage risk effectively.

High maturity

- ☐ Board and C-suite hold a C-level executive accountable for cyberthreat risk management—and are responsible for overseeing development of a cyber risk program as well as confirming its implementation
- ☐ Board and C-suite stay informed about cyberthreats and the potential impact on their organization
- ☐ Board has one or more members—or appropriately leverages strategic advisors—who understand IT and cyber risks
- ☐ An established senior management-level committee, or a hybrid committee consisting of management and board directors, that is dedicated to the issue of cyber risk—or an alternate senior management-level committee has adequate time devoted to the overall cyber program
- ☐ Due diligence is evident in regular updates, budget analysis, and challenging questions to management

Moderate maturity

- ☐ Leadership and board oversight are concerned with cyber issues, but stakeholder communications and oversight of specific structures remain largely high-level
- ☐ Board has a working knowledge of IT and cyber risks
- ☐ Cyber due diligence and the ability to challenge management on cyber issues is lacking
- ☐ Board intermittently assesses the cyber framework and strategic requirements

Low maturity

- ☐ Tone at the top lacks cyber focus and understanding of strategic issues
- ☐ Little engagement by leadership in specific IT security issues
- ☐ Board has no significant experience in IT and cyber risks, and cyber issues are left to those within IT to resolve
- ☐ Oversight of cyber risk and assessment of related budgetary requirements remains at a very high level

2 Do we have the right leader and organizational talent?

Everyone within an organization holds some responsibility for cyber risk. With everyone responsible and with many leaders busy performing their legacy duties, organizations can fail to designate an appropriate leader—the "right" leader—who will ultimately be accountable for cyber risk.

High maturity

- ☐ Cyber leader has the right mix of technical and business acumen to understand how the organization operates, to engage with the business, and to know where to prioritize efforts
- ☐ Teams of passionate and energized staff stay up-to-date on the latest cyber trends, threats, and implications for their business
- ☐ Cyber risk discussions take place at the board and C-suite level
- ☐ There is a sufficient number of skilled staff with relevant industry experience focused on the right areas
- ☐ Compensation and total reward programs are in-line with industry and risk profile/ importance to the organization

Moderate maturity

- ☐ Cyber leader is in place but is primarily focused on technical risks associated with cybersecurity
- ☐ Cyber leader has a working knowledge of the industry but does not fully understand and appreciate how the organization operates
- ☐ Cyber risk is a significant focus but remains relatively high-level
- ☐ Cyber risk issues often stall at the IT or management level
- ☐ Skilled staff is present in IT and some business areas, but with limited industry-specific threat knowledge

Low maturity

- ☐ Little focus on cyber risk from leadership
- ☐ Cyber knowledge and talent are compartmentalized in the IT function
- ☐ Ad hoc training programs are developed for specific new technologies
- ☐ High turnover of staff due to a lack of investment in talent strategy

3

Have we established an appropriate cyber risk escalation framework that includes our risk appetite and reporting thresholds?

Developing meaningful cyber-related messages for the broader organization can help foster the flow of information when there are cyber incidents or concerns. But clearly defining the triggers or threshold events, as well as the actual process for moving information up to management, can make the difference between functional and effective.

High maturity

- ☐ Clearly articulated risk appetite and cyber risks are incorporated into existing risk management and governance processes
- ☐ Established enterprise-wide cyber risk policy is approved and challenged, when necessary, by the board
- ☐ Clearly described and operationalized roles and responsibilities across the cyber risk program
- ☐ Key risk and performance indicators exist, and processes are in place to escalate breaches of limits and thresholds to senior management for significant or critical cyber incidents
- ☐ Incident management framework includes escalation criteria aligned with the cyber risk program
- ☐ Evaluation and monitoring of the value of cyber insurance is in place

Moderate maturity

- ☐ Established cyber risk policy is not fully implemented outside IT
- ☐ Cyber risks are addressed only generally in overall risk management and governance processes
- ☐ Risk appetite is not integrated into cyber risk framework
- ☐ Cyber risk response tends to be reactive rather than proactive
- ☐ An alternative senior management committee has adequate time devoted to the discussion of the implementation of the cyber framework

Low maturity

- ☐ No formalized cyber framework is in place
- ☐ Any risk escalation is ad hoc and only in response to incidents

4 Are we focused on, and investing in, the right things? And how do we evaluate and measure the results of our decisions?

With risk and performance tightly linked, leaders should know what they're expending on resources—and they should know that they're bringing the right resources to bear on cyber challenges. Failing to develop a people strategy, overpaying for services, and other drags on operating costs are all very real risks.

High maturity

- ☐ Cyber risk is considered in all activities—from strategic planning to day-to-day operations—in every part of the organization
- ☐ Investments are focused on baseline security controls to address the majority of threats, and strategically targeted funds are used to manage risks against the organization's most critical processes and information
- ☐ Organization has made an effort to identify their "black swan" risks and has a program to anticipate and avoid these unlikely, but potentially catastrophic, threats
- ☐ Organization's investments and budgets align to risk (clear business cases for investments exist) and are reflected within the cyber strategy
- ☐ Senior management provides adequate funding and sufficient resources to support the implementation of the organization's cyber framework
- ☐ A mechanism for credible challenge exists

Moderate maturity

- ☐ Cyber framework is internally focused without added industry-based processes
- ☐ Cyber strategy and investments are neither aligned nor supportive of one another
- ☐ Imbalance of security investment across baseline security controls and those required for highly sophisticated attacks
- ☐ Strong threat awareness is focused on enterprise-wide infrastructure and application protection
- ☐ Implementation of identity-aware information protection
- ☐ Automated IT asset vulnerability monitoring is in place
- ☐ No significant mechanism for anticipating "black swan" risks

Low maturity

- ☐ Lack of cyber strategy, initiatives, and investment plan
- ☐ Only basic network protection/traditional signature-based security controls exist, with minimal concern for new technologies and methodologies
- ☐ Occasional IT asset vulnerability assessments are performed
- ☐ Business case for cyber investment is rarely made

5 How do our cyber risk program and capabilities align to industry standards and peer organizations?

It's important to know if your organization is lagging—to know how you stand against businesses that are effectively addressing cyber risk. But what do you do if you discover you are lagging? If the board and the C-suite aren't actively in charge of the challenge, who is?

High maturity

- ☐ Comprehensive cyber program leverages industry standards and best practices to protect and detect against existing threats, remain informed of emerging threats, and enable timely response and recovery
- ☐ Adoption of an industry framework to establish, operate, maintain, and improve/adapt cyber programs
- ☐ Organization has conducted an external benchmarking review of its cyber program
- ☐ Organization periodically verifies internal compliance with policies, industry standards, and regulations
- ☐ Organization has formally certified critical and applicable areas of their business (e.g., ISO 27001:2013 certification)

Moderate maturity

- ☐ Cyber program implements a number of industry best practices and capabilities, including basic online brand monitoring, automated malware forensics, manual e-discovery, criminal/hacker surveillance, workforce/customer behavior profiling, and targeted cross-platform monitoring for internal users
- ☐ Compliance and other internal program reviews may be undertaken occasionally but not consistently

Low maturity

- ☐ Cyber measures are ad hoc, with little reference to industry standards and best practices
- ☐ May conduct intermittent high-level reviews in support of compliance and regulatory requirements

6 Do we have a cyber-focused mindset and cyber-conscious culture organization wide?

As they try to strengthen their posture to become more secure, vigilant, and resilient, many businesses focus on education and awareness. But the need runs deeper. How do you change behavior? Guidance on the answer should come from the board and the C-suite.

High maturity

- ☐ Strong tone at the top; the board and C-suite promote a strong risk culture and sustainable risk/return thinking
- ☐ People's individual interests, values, and ethics are aligned with the organization's cyber risk strategy, appetite, tolerance, and approach
- ☐ Executives are comfortable talking openly and honestly about cyber risk using a common vocabulary that promotes shared understanding
- ☐ Company-wide education and awareness campaign established around cyber risk (all employees, third parties, contractors, etc.)
- ☐ Awareness and training specific to individual job descriptions helps staff understand their cyber responsibilities
- ☐ People take personal responsibility for the management of risk and proactively seek to involve others when needed

Moderate maturity

- ☐ General information security training and awareness is in place
- ☐ Targeted, intelligence-based cyber awareness focused on asset risks and threat types is in place

Low maturity

- ☐ Acceptable usage policy is in place
- ☐ Little emphasis on cyber risk outside of IT
- ☐ Awareness and training issues are reactively addressed, in that training is given only after a breach or noncompliance is discovered, and only to a small subset of individuals

7

What have we done to protect the organization against third-party cyber risks?

The roots of many breaches have their origins with business partners, such as contractors and vendors. Cyber concerns extend far beyond the four walls of your business, requiring you to align with your partners, to understand what they are doing, and to ensure that you're comfortable with the risk factors those relationships present.

High maturity

- ☐ Cyber risks are seen as part of the due diligence process for critical outsourcing and subcontracting arrangements
- ☐ All third parties are engaged through a consistent process, and policies and controls are in place (e.g., right to audit), aligned to the organization's expectations and risk tolerance
- ☐ Third parties receive specific training on cyber issues, tailored to relevant needs and risks
- ☐ Risk management program includes profiling and assessing all material third-party relationships and information flows
- ☐ Processes are in place to ensure timely notification of cyber incidents from third parties
- ☐ Steps are taken to mitigate potential cyber risks from outsourcing arrangements based on third-party profiling and risk assessments

Moderate maturity

- ☐ Steps are taken to mitigate potential cyber risks from outsourcing arrangements
- ☐ Due diligence around outsourcing and subcontracting arrangements is encouraged but inconsistently applied
- ☐ Communication from third parties respecting cyber incidents is not contractually embedded
- ☐ Some correlation of external and internal threat intelligence

Low maturity

- ☐ Only basic network protection is in place
- ☐ Third-party due diligence and cyber risk protection measures are nonexistent

8 Can we rapidly contain damages and mobilize diverse response resources when a cyber incident occurs?

Even among highly secure businesses, it often can take days or weeks to discover a breach. What matters is confidence in your ability to respond—confidence in your processes—once you do detect the active threat. From leadership's perspective, critical incident response capabilities include a clear and current chain of command, a thorough communication plan (including back-up contacts), and a broad view of legal issues, public relations needs, brand implications, and operational impacts.

High maturity

- ☐ Clear reporting and decision paths exist for action and communication in response to a security failure or accident
- ☐ Cyber incident response policies and procedures are integrated with existing business continuity management and disaster recovery plans
- ☐ Crisis management and cyber incident response plans and procedures are documented and rehearsed through wargaming, simulations, and team interaction
- ☐ External and internal communications plans exist to address cyber incidents for key stakeholders
- ☐ Organization is actively involved in industry simulations and training exercises

Moderate maturity

- ☐ Basic cyber incident response policies and procedures are in place but not effectively integrated with existing business continuity management and disaster recovery plans
- ☐ IT cyberattack simulations are regularly undertaken
- ☐ Cyberattack exercises are implemented intermittently across the business

Low maturity

- ☐ Some IT business continuity and disaster recovery exercises occur
- ☐ Cyber incident policies, response plans, and communications are minimal or nonexistent

9 How do we evaluate the effectiveness of our organization's cyber risk program?

The answer to this question is simple. You evaluate from end to end. Execution is the difficult part. The other challenge: seeing beyond systems—to understand business wide implications and to examine business processes, not just IT, through a critical lens. They're challenges that demand leadership and involvement from the board and the C-suite.

High maturity

- ☐ Board and C-suite ensure that the cybersecurity program is reviewed for effectiveness and that any identified gaps are appropriately managed in line with risk appetite
- ☐ The board, or a committee of the board, is engaged on a regular basis to review and discuss the implementation of the organization's cybersecurity framework and implementation plan, including the adequacy of existing mitigating controls
- ☐ Regular internal and external assessments (health checks, penetration testing, etc.) of vulnerabilities are conducted to identify cybersecurity control gaps appropriate for the industry
- ☐ Oversight activities include regular cybersecurity budget evaluation, service outsourcing, incident reports, assessment results, and policy reviews/approvals
- ☐ Internal audit evaluates cyber risk management effectiveness as part of their quarterly reviews
- ☐ Organization takes time to absorb important lessons and modify the secure and vigilant aspects of the program to emerge stronger than before

Moderate maturity

- ☐ Basic cyber risk assessments take place on a fixed, unvarying schedule and are not industry-specific
- ☐ Internal audit evaluates cyber risk management effectiveness no more than once a year
- ☐ Lessons learned are sometimes, but inconsistently, applied to improve management of cyber risk

Low maturity

- ☐ Cyber assessments and internal audit evaluations are sporadic or nonexistent
- ☐ Cyber measures remain relatively static and any improvements lack an experiential basis

10

Are we a strong and secure link in the highly connected ecosystems in which we operate?

The cyber readiness of your partners influences your cyber posture. But cyber risk is a two-way street when it comes to partners. Are you a weak link? Are you a leader on cyber risk? Are you making a positive impact when it comes to cyber and the broader business landscape? Collaborating with peer organizations and partners to share intelligence on threats is just one example of how business leaders can develop a more relevant, more holistic approach to cyber risk.

High maturity

- ☐ Strong relationships are maintained with internal stakeholders, external partners, law enforcement, regulators, etc.
- ☐ Supportive of innovative sharing initiatives that do not compromise information security and privacy
- ☐ Knowledge and information sharing with industry sector, independent analysis centers, government and intelligence agencies, academic institutions, and research firms
- ☐ Expansion of sharing efforts and relationships, to include partners, customers, and end users
- ☐ Preference for vendors that support industry standards and cyber advancements
- ☐ Independently maintain mature programs to avoid being the weakest link

Moderate maturity

- ☐ Ad hoc threat intelligence sharing with peers, or active collaboration with government and private sector on threat intelligence

Low maturity

- ☐ Minimal external relationship development and no information or knowledge sharing with peers, government, or external groups

Setting higher goals, setting strategic goals

Whether you're building or revamping, it's important for organizational risk leaders to set a target state for cyber maturity. Effectively defining that target requires an understanding of the business context and resulting priorities, along with discussions between cyber leaders and decision-makers in the rest of the organization. While not all organizations need to be at the highest level in all areas of cyber maturity, the target state should support the organization in achieving its strategic goals—balanced with the cost and time of achieving it. In many instances, this approach drives the organization toward higher levels of maturity for areas in which cyber risk practices are deemed critical. Developing a mature, advanced cyber risk program is not just about spending money differently. It's about taking a fundamentally different approach—investing in an organization-specific balance of secure, vigilant, and resilient capabilities to develop a program unique to your needs.

Where do you stand?
Based on the results of your assessment, does your current state of maturity support or hinder your strategy and mission? If your maturity index is not aligned with your target state of maturity—or if you have not yet developed appropriate cyber goals—it's time to start enhancing your cyber risk posture.

Of course, it isn't possible for any organization to be 100 percent secure, but it's entirely possible to manage and significantly mitigate the impacts of cyberthreats, including theft, regulatory penalties, legal compensation, and reputational damage. By working collectively, we can minimize the growing potential for broad scale infrastructure outages and business disruption at the national, or even the global, level.

For more information, contact one of our leaders:

Ted DeZabala
Global Cyber Risk Services Leader
973-602-4926
tdezabala@deloitte.com

Nick Galletto
Americas Cyber Risk Services Leader
416-601-6734
ngalletto@deloitte.ca

Ed Powers
US Cyber Risk Services Leader
212-436-5599
epowers@deloitte.com

Kelly Bissell
EMEA Cyber Risk Services Leader
+44 20 7007 3669
kelbissell@deloitte.co.uk

James Nunn-Price
Asia Pacific Cyber Risk Services Leader
+61 2-9322-7971
jamesnunnprice@deloitte.com.au

Ash Raghavan
Global Cyber Center of Excellence Leader
212-436-2097
araghavan@deloitte.com

Al Raymond, CIPP/US/C, CISSP

Specialist Leader, Privacy & Data Protection at Deloitte

Privacy Risks: FinTechs & Startups at the Regulatory Crossroads

Oct 7, 2016

FinTechs and startups are now at a regulatory crossroad. Though they have largely existed in an environment of self-regulation, these halcyon days are almost over. State and Federal government voices are starting to express a need for more formal oversight. Regulators are struggling with the balance between protections of end users and not impeding the company's abilities to foster innovation.

Small companies like FinTechs and startups, either as a standalone entity or as a vendor/service provider to a larger firm, have historically had major challenges with their compliance controls specifically, and with attention to data privacy in general.

Large established firms, especially in highly regulated industries (e.g. financial service, life sciences, pharmaceutical, etc.) are sometimes reluctant to do business with these smaller firms as they represent considerable risk if their controls are not in order.

Because FinTech may not currently be directly subject to traditional regulators, compliance with established laws [e.g. anti-money laundering (AML), Know Your Customer (KYC)] is difficult to measure and monitor. Here is the essence of the regulatory concern: with no direct regulation per se, customers may not understand that the traditional consumer protections they have been accustomed to with larger firms may not apply, since those protection laws wouldn't be extended to consumers who might do business with that company.

Since this may be a new paradigm for these smaller firms, I want to call attention to six general trends in the privacy space that FinTechs and startups would be well advised to be aware of as they try to 'move up' into the big leagues and improve their visibility with brand name, world-class firms.

They are:

1. Shifting demographics (i.e. focus and emphasis on millennial's impact to your business) necessitate a new and different approach to the understanding of 'customer privacy.'

2. Customers are savvier than ever of their privacy rights and expectations. They are not reluctant to express their concerns – especially on social media.

3. The rise of class action law suits represents a continuous risk to companies of all sizes, but can be especially destructive to a small firm with limited capital and resources.

4. There has been a constant revision of what is considered "personal information" and the scope is getting wider. Almost any data collected by a small firm is likely subject to protection of some kind.

5. There has also been a constant revision or addition of increasingly restrictive state privacy and security legislation which threatens many small startups with potentially overwhelming compliance overhead. Most small firms either lack the in-house expertise to sufficiently deal with all that is required from a compliance perspective, or they may just not be aware of what is expected from them.

6. Most regulators are showing an increased attention on consumer protection. Even if companies are following the letter of the law, if there is evidence of customer harm, a regulator may take action.

The message here should not be construed as all doom and gloom. FinTechs represent major disruptive possibilities across many industries, and consumers will be the ultimate beneficiaries. However, companies need to be cognizant of their corporate citizen responsibilities. Sure, consumers love a sexy and easy to use interface, but features and user experience shouldn't override cyber security and privacy concerns and obligations.

Innovators in this space should devote reasonable time and resources to regulatory compliance. At the end of the day, good privacy is good business!

Al Raymond, CIPP/US/C, CISSP

Specialist Leader, Privacy & Data Protection at Deloitte

The Arms Race of Privacy & Security Laws

Jun 16, 2016

This past March Tennessee became the latest state to either introduce its own data breach notification law, or modify its present one. The Tennessee law 47-18-2107 is an update to the existing Tennessee breach law already on its books. The law is amongst the now 47+ disparate laws on the books that businesses in the U.S. must navigate and be expected to comply with if they do business in more than one state, or possess the information of a resident of more than one state. I imagine that this is the kind of convoluted (and expensive) business environment that companies in Europe had to deal with before the European Union codified most of their laws.

In the U.S., the complicating factor for large and small businesses alike is the inaction of Congress; that is, failure to act in passing a national law, superseding every state law. When states get impatient for the Fed to act they take matters into their hands. Many times, especially in the case of privacy and security laws, they do it with the best intentions. Unfortunately, we often get a morass of confusing and contradictory pronouncements that are either unbelievably overreaching in scope or just simply too complex and punitive for a small company to attempt to comply with. This 'arms race' of states passing their own laws sometimes results in laws so esoteric and narrow that it may lead a small company to just ignore, or rationalize that it is easier and cheaper to pay any fines associated with non-compliance than to try and comply with the law. (True)

And then sometimes you get laws that appear (at least to me) to be only knee-jerk reactions to high profile cultural events like texting while driving. Granted, this is a dangerous trend and equally dangerous activity that is a negative by-product of modern technology. It makes sense to not do it in practice, but to pass a law against prohibiting texting while driving is pure demagoguery. So, you can't text while driving, but you can still eat, drink coffee, change the stations on your radio, program your GPS sing, turn around to smack your kids, put on make-up, and on and on? What about the recent phenomenon of companies asking employees for their Facebook or other social media credentials? I am not sure about your company, but since when did this become such a national epidemic, like ZIKA, or Swine Flu? Is this 1950 and employers are asking employees if they are now or have ever been a member of the Communist

Party? Sure, I believe it happens and it is wrong, but do we need to create and pass *specific* laws against it? Isn't there anything more significant to legislate?!?

Yes, all of these activities generate press and show citizens that members of government are actually doing something. (I like to recall of Hemingway's great line here: "Don't confuse motion with action."). But the outcome is just another law layered on top of all the other laws that companies, large and small, must deal with to be in compliance. The real ARMS race of nuclear arms proliferation ended between the U.S. and Soviet Union ended in the 1970's with the SALT I and II Talks. Maybe lives aren't at stake here as they were with ICBM missiles, but maybe we can convince Congress that the situation for privacy and security law compliance is dire enough to warrant a SALT talk for the prevention and further proliferation of these one-off, ad-hoc laws and end this arms race too. Thank you, Comrades.

The SEC's Broken Windows Enforcement Policy: Is there Anything New Here?

Denver G. Edwards

Summary: This article examines the Commission's Broken Windows enforcement program and whether it should change how compliance professionals think about carrying out their duties. Historically, the Commission has been perceived as monitoring all areas of the securities markets. Broken Windows does not appear to be a significant shift. Instead, Broken Windows has intensified existing elements of the Commission's enforcement program. Compliance personnel need not overreact to the Commission rebranding as the tough cop on the beat, but they should remain vigilant of business practices within their organizations, leverage technology to monitor their organization's commercial activities, and think creatively about where and how violations may occur.

In the early 1990s, if you drove a car in New York City and were lucky, men carrying squeegees sprayed water on your windshield and demanded a tip. If you were unlucky, squeegee men, as there were known, merely spat on your windshield, wiped it off with a dirty rag, and then demanded a tip. Subway cars were "tagged" with graffiti and riders felt unsafe. Prostitution and peep shows littered Times Square, and up the street in Bryant Park, the drug trade flourished.

Former Mayor Rudy Giuliani and Police Commissioner Bill Bratton adopted a policing strategy in 1994 known as "Broken Windows" to combat "quality of life crimes." The theory is that "when a window is broken and someone fixes it, it is a sign that disorder will not be tolerated. But, when a window is not fixed, it is a signal that no one cares, and so breaking more windows cost nothing." Broken Windows aimed to avoid an environment of disorder that would encourage more serious crimes to flourish and to send a message of law and order. No infraction was too small to be uncovered and punished.

New York is markedly better today than it was in 1994. The squeegee-men have been banished. Subway cars are clean and safe day or night. Times Square is home to "Good Morning America," and Bryant Park hosts New York Fashion Week in the fall and movie screenings in the summer.

Securities and Exchange Chairwoman, Mary Jo White, was the United States Attorney for the Southern District of New York from 1993 through 2002, and she witnessed New York's transformation under Broken Windows. Chair White has sought to adapt the Broken Windows approach to regulation of the securities market.

In speech on October 9, 2013, Chair White said that the Commission's enforcement program intends to be perceived as being "everywhere, pursuing all types of violation of federal securities law, big and small." "Even the smallest infractions have victims, and the smallest infractions are very often just the first step toward bigger ones," which "can foster a culture where laws are increasingly treated as toothless guidelines." The Commission will be a strong cop on the beat and the Division of Enforcement will pursue not just the biggest frauds, but also violations such as control failures, negligence based offenses and strict liability offenses where intent is not required.

The Broken Windows Enforcement Program

The Broken Windows enforcement program is comprised of five elements:

- Streamline collaboration with the Department of Justice, Financial Industry Regulatory Authority (FINRA), and state securities regulators;
- Target gatekeepers;

- Leverage the Office of Compliance Inspections and Examinations (OCIE) to understand and monitor the latest risks and to provide effective oversight;
- Incentivize whistleblowers to report wrongdoing; and
- Marshal technology to analyze data efficiently.

Each of the first four elements has been a constant feature of the Commission's enforcement regime. The Commission routinely works with the Department of Justice to conduct parallel investigations, as evidenced by recent insider trading investigations. Similarly, the Commission works with SROs, such as FINRA, to conduct "sweeps" to target industry-wide behaviors that are detrimental to investors and could jeopardize the integrity of the financial markets. The Commission collaborates with the North American Securities Administrators Association and state securities regulators to get intelligence on developments in state securities markets so that it can target issues before they become systemic problems.

The Commission has increasingly targeted "gatekeepers," including attorneys and accountants since passage of the Sarbanes-Oxley Act (SOX), and more recently it has targeted broker-dealers who violate the market access rule.

OCIE has been the Commission's "boots on the ground" to monitor risks posed by registrants since its creation in May 1995. OCIE has been a source of referrals for the Division of Enforcement since its inception. A key difference today, however, is that OCIE examiners specialize in discrete areas and are able to better understand the businesses they are examining, and the Division of Enforcement now values investigating and bringing non-fraud enforcement actions as it does bringing insider trading cases.

The Commission's whistleblower bounty program has been effective since enactment of the Insider Trading and Securities Enforcement Act of 1988, which mandated payments for tips reporting insider trading. The Dodd-Frank Wall Street and Consumer Protection Act (Dodd-Frank) provides a 10% - 30% bounty for reporting violations of the securities laws in SEC or CFTC enforcement actions that result in monetary sanctions greater than $1 million.

The Commission's investment in technology is the new feature of its enforcement program and may have the most significant impact on broker-dealer compliance functions. The Commission created the Center for Risk and Quantitative Analytics (CRQA) with a mandate to develop quantitative methods to monitor signs of potential wrongdoing and high risk behaviors. CRQA will feed its findings to the Division of Enforcement to investigate and prevent conduct that harm investors. The Commission has also developed the Advanced Bluesheet Analysis Program to analyze relationship among market participants to identify suspicious trading which may not be readily apparent. It also uses predictive analyses to spot trends, identify aberrational performance, and analyze data from new data sources, such as Form PF. On the examination side, the National Examination Analytics Tool (NEAT) enables the examiners to analyze millions of transaction documents accurately within a short time, and enables OCIE to do more precise and sophisticated examination.

More information about the long-term effectiveness of the Commission's analytics tools is needed. Based on recent releases from the Commission, the tools are working as intended, and have increased the Commission's ability to devise sophisticated surveillances of broker-dealer activities. For example, the Staff conducts link analyses, which looks for relationship between two disparate data sources, in insider trading cases. Link analysis has been used to analyze phone records and trading data to determine if two suspects had a phone call with the same person. In another example, the Staff has used link analysis to analyze large volumes of brokerage firm data to identify instances when a corporation allegedly purchased and sold its own stock, with no significant gain or loss, to create fictitiously high trading volume in order to obtain bank financing. The Staff has also used analytics to detect aberrational performance of a hedge fund that

fraudulently claimed it performed better than its peers throughout good and bad markets. These analyses use to take the Staff weeks or months to perform and were subject to human error. Today, these analyses can be completed within days. As a result of the Commission's zero-tolerance for technical violations or control failures, and their willingness to bring enforcement actions for non-fraud cases, compliance officers will need to rethink how they fulfill their roles to protect their institutions.

Broken Windows Presents Opportunities for Compliance

Broken Windows presents two potential opportunities for compliance: (1) a chance for more assertiveness with business units in instituting rigorous controls and testing those controls more frequently; and (2) an opening to negotiate for more resources to respond to the regulatory environment and greater cooperation from other areas of the firm.

Broker-dealers are required by statute/regulations to have written supervisory policies and procedures (WSPs) regarding their activities. Compliance is a partner to a firm's business units. However, the goal of the firm is to make money for clients, shareholders and employees, and onerous and overly restrictive WSPs may be perceived as limiting legitimate commercial activities for which buy-in from business units is necessary. Broken Windows presents an opportunity to tighten existing WSPs to limit supervisory gaps, require increased cooperation between compliance personnel and line supervisors, offer more training on codes of conduct and ethics for employees and management, and obtain more certifications or attestations regarding a supervisor's fulfilling his or her supervisory obligation.

Moreover, Broken Window policies may help compliance obtain more resources and organizational support. Currently, compliance initiatives are balanced against interests of the firm, including for example, technology and operations projects that drive the firm's commercial success. Compliance can cite penalties/fines as evidence of the Commission's aggressive approach to demonstrate that lack of resources, including personnel or proper technology, create enterprise-wide legal, regulatory, and reputational risks that may have far-reaching consequences for clients, counterparties, shareholders, and may cause personal liability to supervisors and management.

The intensity around the Broken Windows enforcement policy arms compliance with tools to make the case to employees to report violations to compliance in order for the organization to avoid regulatory scrutiny, fines, and penalties. Compliance must balance encouraging employees to report violations internally while not undermining the employee's right (and perhaps the Commission's expectation) to report securities violations externally. As a starting point, compliance could appeal to the shared responsibility of each employee to root out bad actors that violate the securities laws, jeopardize investors, and threaten the integrity of the market. It could also promote methods within the organization to facilitate reporting violations, such as toll-free hotlines, an ombudsman position, anonymous e-mail websites to accept tips, and drop-boxes to submit tips regarding violations.

Without suggesting employees should not report externally, compliance could point out to employees that reporting outside (1) does not guarantee an award due to the high threshold (voluntarily providing original information and $1 million sanction), and (2) may have an impact on the organization. For example, in fiscal year 2014, the Commission received 3620 tips of which 139 (3.8%) received the designation of Notice of Covered Action ("NoCA") and therefore eligible for an award. Since the inception of the program in August 2011, only 5.6% of tips (570 out of 10,193) have received the NoCA designation. The impact of non-qualifying tips include business disruption, lost productivity, costs to retain legal counsel to defend against regulatory investigations, and potential damage the firm's reputation, and client or counterparty relationships. Compliance should reiterate to employees that external reporting remains an option if the

employee reports a violation internally to a designated person and the violation is not addressed timely. This approach balances the firm's goal of operating in an efficient, ethical and commercially reasonable manner with the Commission's interest in protecting investors and the market.

Considerations for Compliance Professionals

Compliance personnel who actively work with a business unit to implement WSPs risks being labeled a supervisor and may be subject to liability for aiding and abetting or failure to supervise. Compliance personnel may minimize the risk of being labeled a supervisor by establishing in meetings with business supervisors that although he or she is an integral part of the business unit's operations, the business supervisor is the designated supervisor. Compliance personnel must document the supervisory reviews of the business that the supervisor is responsible for overseeing, and should periodically obtain certifications or attestations from supervisors indicating that she or he understands his or her supervisory role and is undertaking his or her supervisory obligations. More generally, compliance should ensure that the firm's supervisory manual states that compliance personnel are solely responsible for activities within the compliance department.

Compliance personnel should have a predetermined process to investigate, track and document red flags. They must act decisively when red flags surface or if red flags are brought to their attention. Compliance personnel should document each red flag, which business supervisors will address the red flag, and what corrective action will be taken. Compliance personnel must take reasonable steps to follow up with the business supervisor to ensure the issue has been resolved and then must monitor the issue to ensure it does not recur. Compliance personnel should also share information with firm management (particularly if a red flag involves a senior manager), and should be prepared, and have a process in place, to escalate matters to the Board of Directors if management fails to take corrective action.

Membership on firm committees is also an area of concern for compliance personnel. As evidenced in In the Matter of Theodore Urban, membership on certain firm committees may cause the Commission to determine that compliance personnel who, as a member of a committee, learn critical information about a violation have a duty to ensure that corrective action is taken. The Commission's approach exposes compliance personnel to personal liability that could potentially jeopardize careers and, as a result, may cause qualified candidates to avoid compliance roles.

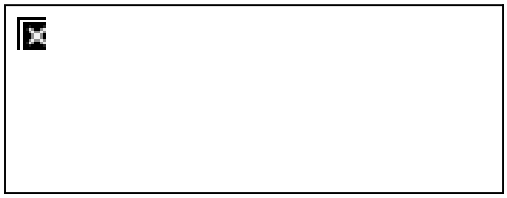
The Commission's use of data analytics tools has increased the pressure on compliance personnel to ferret out fraud, technical violations, and control failures. One approach is to conduct surveillances similar to those performed by the SEC's analytics teams. Some reliable off-the-shelf surveillance may be available, but compliance may have to leverage internal information technology resources and get buy-in from business units to build surveillance tools to counter the SEC. The associated costs may be significant since the Commission's data analytics program is continuously evolving and broker-dealers would need to keep pace. However, since repeated violations could lead to increasingly severe fines, create the impression that there is a lack of institutional control at firms, personal liability, and could jeopardize firms' reputation and client relationships, firm may have limited choice.

The other alternative is for compliance personnel to rely on the traditional approach, which is based on developing strong policies and procedures that match the firm's business and the regulatory environment, and diligent oversight. This approach requires frequent monitoring and testing of the adequacy of business units' compliance with polices and procedures. It also requires compliance personnel regularly ask where issues could occur, what controls are in place to prevent or detect problems, and what residual risks remain unmitigated by such controls?

Broken Windows has helped the Commission become more efficient in how it implements its enforcement program. Yet, Broken Windows does not represent a substantive change in the Commission's enforcement policy. SOX and Dodd-Frank reiterated to compliance personnel the need to establish strong controls and vigilance to protect their firms, investors, and the integrity of the market. Responsible compliance personnel have heard that message and approach their roles with professionalism and integrity. Broker-dealers should continue to prioritize implementing existing regulations, monitor controls, and thoughtfully consider where violations may occur within their organizations, rather than overreact to the Commission's efforts to rebrand itself as a tough cop on the beat.

Get Ready for the Next Phase in Cyberattacks

The National Law Journal
Michael J. Gottlieb and Matthew L. Schwartz, October 5, 2015



The threat to cybersecurity has evolved more rapidly than the technologies and processes available to defend our most sensitive information, and the speed with which new threats are emerging is leaving the legal framework that governs data privacy and security in the dust.

When data breaches began to seep into general public consciousness some time in 2013, the incidents garnering public attention tended to fall into one of two categories. The first and most widely appreciated category was breaches obviously motivated by financial gain. The poster child for this category is the large-scale retailer breach, including the attacks on The Home Depot Inc., Target Corp., Neiman Marcus Group Ltd. LLC and others. Hackers penetrated these retailers' networks to steal financial and other personally identifying information and subsequently sell that information on the black market.

The second category involves breaches of U.S. government organizations orchestrated chiefly by foreign governments (along with state-affiliated criminal networks) in order to steal government secrets for military, intelligence, economic or other foreign policy gains. The most recent example of this type of breach was the brazen attack on the networks of the U.S. Office of Personnel Management, likely launched by hackers employed by or affiliated with the Chinese government, which compromised the personnel security files, including fingerprint records, of millions of current and former federal employees.

A third type of breach — cyberextortion — entered the limelight when North Korean hackers launched a coordinated cyberattack against Sony Pictures Entertainment Inc. in late 2014. The purpose of the Sony attack was to intimidate the company into scrapping the release of its movie, "The Interview," by threatening to disclose publicly all of the company's most sensitive documents if it failed to comply. The Sony breach is the most visible example of cyberextortion designed to intimidate by threatening to reveal private information unless the victim agrees to certain demands. Both the Sony breach and the more recent attack on Ashley Madison have underscored that hackers may be motivated by political or ideological objectives.

These three categories do not represent an exhaustive taxonomy of cybersecurity threats, but they can help us understand both the diversity of hackers' targets and the creativity

of their methods. Recent attacks, particularly in the category of breaches motivated by financial gain, demonstrate the inadequacy of traditional approaches to cybersecurity, which have focused overwhelmingly on the protection of personally identifying information and, to a lesser extent, proprietary information such as trade secrets. Although such efforts remain important, it is clear that a data security program that focuses exclusively on these types of information is likely to fail.

THE PRESS -RELEASE SCHEME

An illustration of how hackers have evolved is the scheme to hack corporate press releases recently uncovered by the U.S. Department of Justice and Securities and Exchange Commission (SEC). The press-release scheme involved a conspiracy in which traders paid hackers — who developed sophisticated organizational and marketing tools, and even took orders from their customers about which press releases to target — to obtain thousands of press releases from PR Newswire, Business Wire and Marketwired prior to their release. The traders then used early access to those releases to execute profitable trades on companies such as Radio Shack Inc. and Panera Bread Co.

The conspiracy to steal press releases is significant for a number of reasons. First, the hackers did not seek out one particular target based upon a perceived vulnerability. Instead, they targeted a group of companies that collectively creates, stores and disseminates a particular and specialized type of information — corporate press releases — of great value to those willing to disregard the insider-trading laws. That is to say, the hackers targeted the news services not because of their vulnerability, but simply because of wealth of information they stored. Second, the press-release scheme involved a large-scale enterprise in which traditional financial fraudsters joined with hackers-for-hire to achieve a common objective. As these types of enterprises become more common, nearly all types of crime will become easier to commit and conceal.

One obvious lesson to draw from the press-release cases is that any organization that holds material nonpublic information relating to public companies is likely to become a target for hackers. This includes public companies, but also — and perhaps especially — entities that are likely to hold material nonpublic information concerning multiple public companies, such as professional-services firms, private-equity funds and news organizations. Any entity that collects or holds material nonpublic information should perform risk assessments that examine access, storage and retention policies that apply to such data.

Attention must also be given to the policies and procedures that define the entity's relationships with third parties, such as vendors and contractors that have access to systems that store such information. Furthermore, such information should be clearly identified as a separate category in incident-response plans, and table-top exercises should be structured to test identification, mitigation and notification procedures in the event of a breach.

For SEC-regulated entities, such as brokerage and advisory firms, this type of planning has become mandatory. The SEC's Office of Compliance Inspections and Examinations recently launched its second round of cybersecurity examinations of registered entities.

The commission's first sweep, which began in the spring of 2014, established clear areas of SEC concern, including the need for firms to conduct risk assessments; the importance of developing a written information-security policy appropriately tailored to the business; and appropriate cybersecurity governance, including board and senior executive participation, employee training and third-party controls. The new round of

inspections is likely to bring with it a more aggressive brand of enforcement, including the possibility of enforcement actions similar to those that the Federal Trade Commission has brought over the past several years.

Perhaps the most important message is that prevention and preparedness efforts must assess all of an organization's data, rather than simply the data that initially appear to be high risk based upon past breaches. All of a company's data could be transferred in one attack, and innovative hackers will continue to find new buyers for new types of stolen data. Thus, sound preparation should begin with a thorough data mapping and risk assessment exercise that considers not just how a company uses its data, but how others might misuse them.

Although no amount of preparation will eliminate the risk of a breach, beginning with the appropriate inquiry may help decrease the risk of relying upon information security policies that are stuck in the past.

Related Practice: Privacy, Cybersecurity & Technology

External Link: Read article here

Stop the Data Feeding Frenzy

Our laws are not built to protect victims of ideologically-driven data hacking.

Who is coming for your data?

By Michael Gottlieb | Feb. 23, 2015 | 10:25 a.m. EST + More

Imagine someone breaks into your home and steals a box that contains some of your bank and tax records, and perhaps some of your personal mementos such as pictures and letters. They then give the box away to a stranger and disappear. If you find that stranger in possession of your box, you will be able to recover it, because the law does not allow the stranger to keep, copy or use your property simply because he had no role in stealing it.

Now imagine, instead of a box taken from your home, a hacker breaks into your computer network. The hacker steals your bank and tax records, your pictures and correspondence, but all in digital form. The hacker disappears, but not before handing over all of your data to an Internet file sharing site, which in turn makes the data available all over the world. Not only does the file sharing site refuse to return your data, but soon thereafter, individuals are disseminating your private pictures, emails and tax returns via their Twitter accounts. Indeed, they claim a constitutional right to do so.

This is the dilemma faced by data breach victims: Data are not, and perhaps cannot be, subject to the same set of legal protections as tangible, physical property. Our laws have failed to keep pace with the ways in which our privacy depends on the security of electronic data. This problem is not well understood or widely discussed. Indeed, at the recent White House cybersecurity summit at Stanford University, the challenge of containing the spread of stolen data was not on the agenda.

[**SEE:** Editorial Cartoons on Chinese Hacking]

Until we develop a clear framework for addressing the problem of stolen data, efforts to improve cybersecurity will be incomplete. Data breaches are inevitable. For most organizations, it is a question of when, not if, they will be struck. That unfortunate reality means that an effective approach to cybersecurity cannot focus solely on prevention. To be prepared, organizations must treat breaches as a certainty, take steps to minimize risks wherever possible, and make plans to contain the damage that is caused when breaches take place.

These difficulties are compounded by the evolving nature of data breaches. Traditionally, hackers have targeted companies such as Anthem, Target, Home Depot and Neiman-Marcus to make money. The hackers break into corporate networks and steal data, such as credit card or Social Security numbers, which they then sell on the black market. Our current laws are directed at this kind of breach. We have imperfect, but strong, state and federal laws prohibiting identity theft, rapidly-improving encryption practices, and improving international law enforcement cooperation against criminal networks that trade in personally identifying information.

The 2014 cyber-attack on Sony Pictures Entertainment unleashed a new kind of threat: data breaches motivated by ideology rather than financial gain, but aimed at private rather than governmental entities. Today, both non-profit and for-profit organizations around the world face the prospect of having all of their data released to the public by hackers who disagree with their speech, work or political activities. The chief objective of this new breed of hackers is to take private information and make it public in order to intimidate or embarrass the victim. To succeed in that endeavor, the hackers depend on the witting or unwitting assistance of others to disseminate, spread and publish the stolen information as widely as possible.

[**SEE:** Editorial Cartoons on the Sony Hack]

Our laws are not designed to address these challenges. Data breaches are generally followed by an open season on the victim's most sensitive information. Some of that information concerns purely corporate interests; some of it concerns the privacy of employees, customers or third parties. Unfortunately, once hackers hand such data off to a third party, it may be impossible to recover or contain. There are stolen property laws in many states, but there are questions about whether such laws apply to information rather than physical property. There are trade secrets laws, but a trade secret may be lost forever if it is revealed (even involuntarily) to the public. And even where a law does apply, the First Amendment may still protect those who decide to publish the information.

If data breaches are indeed inevitable, the current situation is untenable. If we are serious about helping the individuals and organizations who are victims of data breaches, we can and must do better than a system that throws up its hands the moment information is stolen.

An effective regime against this new form of data breach will require updating and rationalizing a set of overlapping and often contradictory laws relating to stolen property, consumer privacy, identity theft, copyright, trade secrets and more. That effort must find a way to balance cherished First Amendment

Op Ed

Expert commentary on leading issues.

The Price of Appeasement

Stop the Data Feeding Frenzy

Breaking a Bad Business

The Audacity of Jeb

Q&As

Thoughtful discussions on critical questions.

Tracing the Path to Freedom

Historian Eric Foner dispels the myths about the Underground Railroad.

Just a Feel-Good Exercise?

Sociology professor **Caroline Lee** explains the power and pitfalls of public engagement.

values against the legitimate privacy interests that individuals have in the information that organizations hold about them, as well as the interests those organizations have in keeping their own information confidential.

[**READ:** Hacking Our Economy]

This project, however, cannot be limited to our laws. The robust protections that the First Amendment affords require that media organizations themselves consider what self-imposed restraints can be applied in the aftermath of a breach. Such self-policing is destined to be imperfect, and will no doubt be difficult given the demands of the 24-hour news cycle. But it is necessary. After all, it is only a matter of time until hackers steal, and someone attempts to release in public, the confidential sources of a major news organization.

The reforms described above will not be easy. But unless we find ways to address the feeding frenzy that inevitably follows data breaches, our best efforts to improve cybersecurity will continue to fall short.

TAGS: cybersecurity,

+ More

Michael J. Gottlieb is a partner in the Washington office of Boies, Schiller & Flexner LLP, specializing in cybersecurity and data privacy issues. He served as associate White House counsel during the first term of the Obama administration.

You Might Also Like

President Obama Cartoons

Gun Control Cartoons

Obamacare Cartoons

Susan Rice Calls Prime Minister Netanyahu's Visit 'Destructive'

By Rachel Brody | Feb. 25, 2015

The Price of Obama's Nuclear Appeasement Toward Iran

By Harold Evans | Feb. 24, 2015

Mother Jones Says Fox's Bill O'Reilly Embellished Falklands War

A Private Trauma in the Public Eye

Biographer **Barbara Learning** explores Jackie Kennedy's struggles after her husband's assassination.

Most Popular

Jon Stewart and Stephen Colbert Helped Bury MSNBC

United Steelworkers Say Safety, Not Wages, Behind Refinery Strike

The Price of Obama's Nuclear Appeasement Toward Iran

New Dietary Guidelines Call for Less Meat and Sugar

Experience

By Adriana Scott | Feb. 20, 2015

Rudy Giuliani Says Obama Doesn't Love America

By Rachel Brody | Feb. 20, 2015

Combat Human Trafficking By Disrupting Its Profit Cycle

By Charles C. Krulak | Louis Freeh | Feb. 19, 2015

Obama Won't Link Islamic State Extremism to Religion

By Rachel Brody | Feb. 19, 2015

Underground Railroad Legacy Is an Example of Interracial Cooperation

By Michael Morella | Feb. 19, 2015

Oklahoma Republicans Vote to Eliminate Funds for AP U.S. History Course

By Rachel Brody | Feb. 18, 2015

Texas Judge Temporarily Stalls Obama's Executive Actions on Immigration

By Rachel Brody | Feb. 17, 2015

Rand Paul, the Hawks and the Lack of 2016 Debate on Iraq and Syria

By Jill Lawrence | Feb. 17, 2015

Will Hillary Clinton Run Unopposed in 2016? Don't Bet On It.

By Robert Schlesinger | Feb. 17, 2015

Obama Has Lost His Nerve in the Battle Against a Nuclear Iran

By Mortimer B. Zuckerman | Feb. 13, 2015

Jon Stewart Will Leave 'The Daily Show,' Pundits React

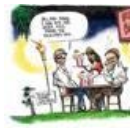
By Rachel Brody | Feb. 11, 2015

Vaccination Debate Shows Health Illiteracy Is a Real Danger

By Shannon Galvin | Juliet Sorensen | Feb. 11, 2015

David Axelrod Says Obama Lied in 2008 About His Gay Marriage Views

By Rachel Brody | Feb. 10, 2015



Editorial Cartoons on Brian Williams

Feb. 9, 2015

U.S. Supreme Court Allows Alabama Gay Marriage Despite Judge's Protests

By Rachel Brody | Feb. 9, 2015

Obama's Course to a Nuclear-Capable Iran

By Mortimer B. Zuckerman | Feb. 6, 2015

Obama's Prayer Breakfast 'Crusades' Comments Enrage the Right

By Rachel Brody | Feb. 6, 2015

Congress Must Be Involved in the ICANN-IANA Internet Transfer of Power

By Simon Rosenberg | Feb. 6, 2015

See More

In Cyber-Insurance Every Word Matters

Published on June 4, 2016

Denver G. Edwards
Principal at Bressler, Amery & Ross, P.C.

On April 22, I posted that the 4th Cir. Court of Appeals found that a cyber breach was covered under a GL policy. I wrote that "[t]he take away for the insured is to read your policies closely. Your policy may cover certain costs and expenses for a cyber incident. For the insured, use clear language to identify what is covered and what is not covered under a GLP. After all, a GLP is nothing more than a contract and courts will follow the Eight Corner's Rule – four corners of the contract and four corners of the policy."

On Tuesday, the U.S. District Court in Phoenix in *P.F. Chang's China Bistro Inc. v. Federal Insurance Co.*, ruled that P.F. Chang's GL policy did not cover costs associated with its data breach. Once again the court closely analyzed the terms of the cyber-insurance policy and, in this instance, found that the party claiming injury was not covered

under the policy. Even though the cases reached different results, the take-away remains the same: companies must closely review their cyber-insurance policies to determine what is covered and what is excluded in order to avoid gaps in coverage. Assuming there is coverage in place when none exists could be costly.

Practical tip: One way to gain certainty is to invite the cyber insurer and the GL insurer to the company's tabletop simulations or pen testing sessions and specifically ask if a particular scenario would be covered under existing cyber-insurance policy or GL policy.

Think the SEC is Soft on Cyber? Think Again.

Published on February 24, 2016

Denver G. Edwards
Principal at Bressler, Amery & Ross, P.C.

The cybersecurity discussion at SEC Speaks 2016 should not be mistaken for a lack of commitment. Besides enforcement actions by the Enforcement Division (and FINRA), the Commission's Investment Management and Corporate Finance Divisions have issued guidance in 2015 and 2011, respectively, which fleshes out the Commission's expectations. OCIE has interpreted the Market Access Rule to include a cybersecurity requirement, and Regulation SCI 's requirement that entities' maintain operational capabilities and promote fair and orderly markets clearly includes disruptions due to cybersecurity (e.g., DDoS attacks).

Below ae some points that public companies, broker-dealers, investment advisers, and other SEC-regulated entities keep in mind:

Public Companies - Governance

- Cybersecurity assessment and monitoring are part of a director's fiduciary duties. Directors must oversee management to ensure that adequate systems and procedures are in place to limit cyber intrusions. Elevate cybersecurity to enterprise risk status.
- Directors must understand the risk, the potential benefits (and costs) of prevention.
- Raise cybersecurity at board meetings, including retaining independent consultants to evaluate the firm's risk profile and provide specific recommendations. Learn what the firm is doing in the area of cybersecurity. Directors will likely receive benefit of the business judgment rule if a data breach occurs.
- Understand your regulator and the standards that the agency expects to be met.
- Have a plan to respond if preventative efforts fail. Select the response team (external counsel, forensics, PR, etc.) in advance, identify their roles, and the chain of command.

Broker-Dealers, Investment Advisers, and other parties

SEC and FINRA have disciplined firms for:

- Failing to have robust cybersecurity procedures, failing to follow existing cybersecurity procedures, and failing to establish appropriate controls to enforce existing cybersecurity procedures.

- Failing to perform sufficient periodic assessments of cybersecurity procedures and failing to respond to deficiencies detected through such assessments prior to a breach.
- Failing to protect networks containing non-public customer information with appropriate technology (encryption, antivirus software and firewalls) and reasonable procedures (user access restrictions).
- Failing to respond appropriately to cybersecurity breaches, including how firms enhance their systems and procedures with a view toward preventing the recurrence of similar data breaches.

Guidance from Investment Management Division

Create a strategy designed to prevent, detect and respond to cybersecurity threats, including regular audits focused on:

- Access control, authentication and authorization methods, firewalls or perimeter defenses, tiered access to sensitive information and network resources, network segregation and system hardening.
- Data backup and retrieval.
- Data encryption.
- Protect against loss or exfiltration of sensitive data; limit use of removable storage media; deploy software that monitors for unauthorized intrusions, loss or exfiltration of sensitive data, or other unusual events.
- Gather information related to cyber threats from outside resources, such as vendors, third-party contractors specializing in cybersecurity and technical standards, topic-specific publications

and conferences, and participating in the Financial Services – Information Sharing Analysis Center.

- Develop an incident response plan, including having a cybersecurity team in place before the accident occurs.