



Security Basecamp: Cybersecurity Research & Insights

**For Broker-Dealers, Investment Companies,
and Investment Advisors**

*Utilizing Cybersecurity Risk Assessments to
Take Focused Action*

August 2015

(949) 330-0899

Table of Contents

EXECUTIVE SUMMARY	2
INTRODUCTION – THE NEED FOR ACTION	3
Your Threats – Cybercriminals Are Targeting Small to Mid-Sized Companies	3
Cybersecurity – The Regulation: What Are Broker-Dealers and Investment Advisors Required to Do.....	3
Cybersecurity – Your Business and Regulatory Exposure.....	4
Cybersecurity Insurance	4
The Need for Action – What You Don’t Know, Can Hurt You.....	5
CYBERSECURITY RISK ASSESSMENTS	6
Planning Your Cybersecurity Work.....	6
Executing the Work	8
Step 1: Inventory and Identify Critical Assets.....	8
Step 2: Assess Threats and Vulnerabilities	8
Step 3: Address Identified Risks – Implementing Controls.....	10
ABOUT SECURITY BASECAMP	12
AUTHOR INFORMATION	12

LIST OF FIGURES

Figure 1: Case Study - Cyber Threats from Firm Customers.....	4
Figure 2: Essential Elements of a Cybersecurity Program	6
Figure 3: Cybersecurity – Security Basecamp Project Intake Questionnaire Excerpt.....	7
Figure 4: Security Basecamp Cybersecurity Toolkit - Deliverables by Phase.....	7
Figure 5: Identification of Risks Questionnaires.....	8
Figure 6: Security Basecamp Basic Framework for Measuring and Reporting Cybersecurity Risk.....	9
Figure 7: Assessing Business & Regulatory Impact Severity Levels	9
Figure 8: Assessing Risk Likelihood Levels.....	9
Figure 9: Common Vulnerability Scoring System Calculator	10
Figure 10: Cybersecurity: Example Areas Firms May Want to Improve Controls to Reduce Cyber Risks	11

EXECUTIVE SUMMARY

- The menace of cybercrime is becoming more automated and sophisticated. Financial services firms such as brokers, dealers, asset managers, and investment advisors are high-value targets due to the sensitive information they are required to gather and maintain.
- Small to mid-sized companies are particularly vulnerable to attack and to the financial and reputational damage associated with cybercrime. According to Symantec, small to mid-sized companies - such as most independent broker-dealers (BDs) and investment advisors (IAs), experienced 60% of all attacks during 2014¹.
- Protecting your firm is less difficult than one might think given the constant barrage of information about cybersecurity threats and incidents. There are straight forward steps to be taken. A set of essential technical controls exists for broker-dealers and investment advisors to review for potential implementation.²
- The **regulators require** BDs and IAs to:
 - Adopt reasonably designed written policies and procedures addressing administrative, technical and physical safeguards for the protection of customer information and records; and
 - Protect against any anticipated threats or hazards to the security or integrity of customer records and information, and against unauthorized access to or use of customer records or information.
- In addition, entities registered with the SEC or CFTC (including broker-dealers or investment advisors) **must develop and implement** an Identity Theft Protection Program (ITPP) under Regulation S-ID.³
- Furthermore, **regulators recommend** that all BDs and IAs complete a **cybersecurity risk assessment**. FINRA calls these risk assessments a foundational tool⁴ - no matter a firm's size or business model.
- FINRA found that most BDs have completed a cybersecurity risk assessment, estimating that over 80 percent of firms had established cybersecurity risk assessment programs.⁵ That said, this indicates that a number near 20%, or 1 in 5 registered firms, have not taken a critical step in protecting its customer information. FINRA is concerned that the remaining firms either have no program in place or were only in the nascent stages of establishing a program.
- The effectiveness, quality, and depth of cybersecurity programs across the industry should be expected to be varied. To date, the regulators have been primarily focused on gathering information, assessing the existence of programs, and understanding current practices – not necessarily on assessing the quality and practical business effectiveness of a given cybersecurity program at a given firm.
- Ultimately, the motivations of cybercriminals, and their effectiveness in penetrating your firm's controls, will serve as the judge to the quality of your firm's cybersecurity program.
- Rigorous attention to detail tempered by good business acumen is necessary for a successful cybersecurity program. One size does not fit all. Organizations face varying levels of risk. Organizations have varying levels of time, money, and resources to dedicate to the critical need of protecting your business and customer interests. Cybersecurity programs should be tailored to the specific needs of your firm and your security risk profile.
- A professional, third-party cybersecurity risk assessment can be used to assess the specific vulnerabilities your firm faces. Assessments allow you to take focused actions to address your vulnerabilities and further control or mitigate your cybersecurity risks. Two methods of vulnerability analysis are highlighted in this paper. Both allow for the creation of a focused list of cybersecurity action steps.

¹ Symantec, *2015 Internet Security Threat Report*. The report defines small to mid-sized companies as those with fewer than 2,500 employees.

² Security Basecamp has formulated a list of actions it recommends all broker-dealers, asset managers, and investment advisors of any size consider (and implement as necessary) called its *Quick Hit Technical Controls Review*.

³ SEC, *Identity Theft Red Flags Rules*, <https://www.sec.gov/rules/final/2013/34-69359.pdf>, May 20, 2013; (web, August 2015)

⁴ FINRA, *Report on Cybersecurity Practices*, February 2015.

⁵ *Ibid*, page 14.

INTRODUCTION – THE NEED FOR ACTION

Your Threats – Cybercriminals Are Targeting Small to Mid-Sized Companies

Symantec stated that smaller firms experienced 6 out of 10 cyber-attacks during 2014⁶. Many were automated and programmed to search the web for unprotected computers or devices. The wealth-advisory industry has long been struggling with what security experts and advisers say has been an onslaught of fraudulent wire-transfer requests, many resulting from client email accounts being hacked. Fifty-four percent of broker-dealers, and 43% of RIAs said they had received fraudulent emails seeking to transfer client money.⁷

In February 2015, the SEC's Office of Compliance Inspections and Examinations (OCIE) issued a Risk Alert⁸ providing summary observations derived from the staff's sweep examinations performed of over 100 registered BDs and IAs that were undertaken to assess the cybersecurity practices and preparedness of such firms. The examinations found that 88% of broker-dealers and 74% of investment advisers reported cyber-attacks directly or through one or more vendors, the majority of which arose from malware and fraudulent e-mails.

Smaller firms may assume that only larger firms are at risk of cyber-attacks. Yet from the perspective of a hacker looking for the right opportunity, smaller to medium-sized financial firms are attractive targets. The assumption being fewer physical barriers, a larger degree of human vulnerabilities (i.e. less formal training, less technical monitoring of computer usage by employees), and less complex or sophisticated IT environments (i.e. less money to spent on cybersecurity). Even if these characteristics do not apply to your firm, attackers may assume they do. That alone can make your firm a target. *If an attacker is targeting your firm today, would you know?*

According to regulators and cybersecurity professionals, an effective way to get started in developing an appropriate plan for your firm is to undertake a guided, risk assessment. Then, after completing the risk assessment, your firm focuses its resources on remediating the vulnerabilities highlighted. Performing the risk assessment and taking informed action to implement necessary controls is both a prudent regulatory and business step.

Cybersecurity – The Regulation: What Are Broker-Dealers and Investment Advisers Required to Do

As stated previously, it is estimated that 1 in 5 firms has not taken the recommended action of performing a documented risk assessment. NASD (n/k/a FINRA) Rules of Fair Practice have always required confidential treatment of customer information. Regulation S-P⁹ further strengthened this requirement specifically with Section 30. Brokers, dealers, investment companies, and investment advisers registered with the SEC are **required** to:

1. Adopt reasonably designed written policies and procedures addressing administrative, technical and physical safeguards for the protection of customer information and records; and
2. Protect against any anticipated threats or hazards to the security or integrity of customer records and information, and against unauthorized access to or use of customer records or information.¹⁰

In addition, any entity registered with the SEC or CFTC (including broker-dealers or investment advisers) which holds transaction accounts for its clients must develop and implement an Identity Theft Protection Program (ITPP) under Regulation S-ID.¹¹

⁶ *Ibid*, 1, page 6.

⁷ *Most Brokerages and Advisory Firms Targeted by Cybercriminals*, Wall Street Journal, February 2015 (Web August 2015).

⁸ Cybersecurity Examination Sweep Summary, U.S. Securities and Exchange Commission, National Exam Program Risk Alert, Vol. 4, Issue 4 (Feb. 2, 2015), available at <http://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf> (the Risk Alert).

⁹ Morrison & Foerster LLP, *Broker-Dealer Cybersecurity: Protect Yourself or Pay the Price*, January 10, 2014: Regulation S-P became effective in November 2000, and compliance with the rules and regulations has been mandatory since July 1, 2001. The requirement that policies and procedures be written has been in place since 2005.

¹⁰ *Ibid*, 1, page 1.

¹¹ *Ibid*, 3.

Cybersecurity – Your Business and Regulatory Exposure

Financial services firms, such as broker-dealers, investment companies, and investment advisors are high value targets for cyber criminals. The nature of a financial services firm involves managing sensitive information about clients that can be used to perpetuate fraud, including the unauthorized transfer of money from a client's account. When it comes to unauthorized transfers, consumers are protected with liability limits, but, companies have no such protection. A customer reporting fraud within 48 hours cannot be liable for more than \$50.¹² Yet businesses don't have liability limits and so the potential exposure and financial impacts are worthy of consideration.

Consider a former Morgan Stanley Smith Barney adviser—whose client's email had been hacked—resulting in 4 fraudulent wire requests totaling \$521,500 over two months during 2014. Also, a former Wells Fargo adviser failed to confirm two wire transfers for a total of \$67,532 over two months in 2012 that turned out to be from an impostor. FINRA suspended and fined both advisors. Neither admitted or denied the allegations, and their firms fired them.

Of the broker-dealers that reported losses from fraudulent emails, 25% said the losses were the result of employees not following the firms' authentication procedures. The case study below, further illustrates a range of risks and vulnerabilities facing a typical firm.

Figure 1: Case Study - Cyber Threats from Firm Customers¹³

In one instance where FINRA took enforcement action, hackers used an SQL injection attack on a firm's database server to obtain confidential customer information of more than 200,000 customers, including names, account numbers, social security numbers, addresses and dates of birth. The firm stored the data on a computer with an Internet connection and did not encrypt the information. The firm only became aware of the breach when hackers attempted to extort money from the firm. In fact, however, those breaches had been visible on the firm's web server logs.

The case illustrates governance failures in several respects. Most broadly, the firm failed to implement adequate safeguards to protect customer information. More specifically, the firm stored unencrypted confidential customer data on a database connected to the Internet without effective password protection. Although the firm performed penetration testing, it did not include an asset with sensitive customer information as part of that test. In addition, the firm did not establish procedures to review the web server logs that would have revealed the theft of data. And, the firm did not respond to an earlier auditor recommendation that it acquire an intrusion detection system. Finally, the firm also failed to have written procedures in place for its information security program designed to protect confidential customer information.

Cybersecurity Insurance

The SEC has also found that 58% of broker-dealers, but only 21% of RIAs are insured against losses from cyberattacks. In a separate review, FINRA reported that 61% of the brokerages polled have a separate cybersecurity insurance policy, and 11% have a cybersecurity rider with other insurance, such as errors and omissions policies. 28% of those surveyed said they have no cyber insurance coverage at all.

Firms have another consideration in the wake of cyber-attacks - that being the costs associated with reputational damage associated with an incident. Although not in our industry, the well-publicized Target stores data breach in 2013 is estimated to have cost the company \$200 million dollars as of earlier this year. When all is said and done, the costs of that single breach could reach upwards toward \$1 billion. Companies need to make security a top priority by completing the most basic steps and also addressing insider threats, which is how many breaches are happening today.¹⁴

¹² Investment News, *Cybercrime: a challenge firms and advisers must face*, May 2015: Federal Deposit Insurance Corporation (FDIC) Law, Regulations, Related Acts, 6500 - Consumer Protection, PART 205—ELECTRONIC FUND TRANSFERS, Web 2015

¹³ *Ibid*, 4, page 8.

¹⁴ Security Week: *Target Data Breach Tally Hits \$162 Million in Net Costs*, <http://www.securityweek.com/target-data-breach-tally-hits-162-million-net-costs> (Web, August 2015)

The Need for Action – What You Don't Know, Can Hurt You

FINRA and the SEC have been actively communicating cybersecurity guidance to its firms. Recently, they have specifically recommended that firms do the following:

1. Document your technology environments and cybersecurity programs.
2. Perform a risk assessment.
3. Implement cybersecurity controls.
4. Develop, implement and test incident response plans.
5. Perform 3rd party vendor due diligence and manage related cybersecurity risks.
6. Train your staff to identify and mitigate cybersecurity risks.

A cybersecurity risk assessment identifies your potential vulnerabilities. Simultaneously, a good process benchmarks your organization's cybersecurity practices against regulatory requirements and guidance. Further, a risk assessment also defines your potential for exposure. This allows you to understand the pros and cons of implementing various technical controls. Most importantly, an effective risk assessment focuses your effort and spending on the highest impact controls. In other words, when done from a business perspective, a risk assessment maximizes your return on investments made on cybersecurity controls.

The subsequent section of this analysis communicates an approach to completing a risk assessment and then highlights ways in which it can be utilized to create a focused plan of action.

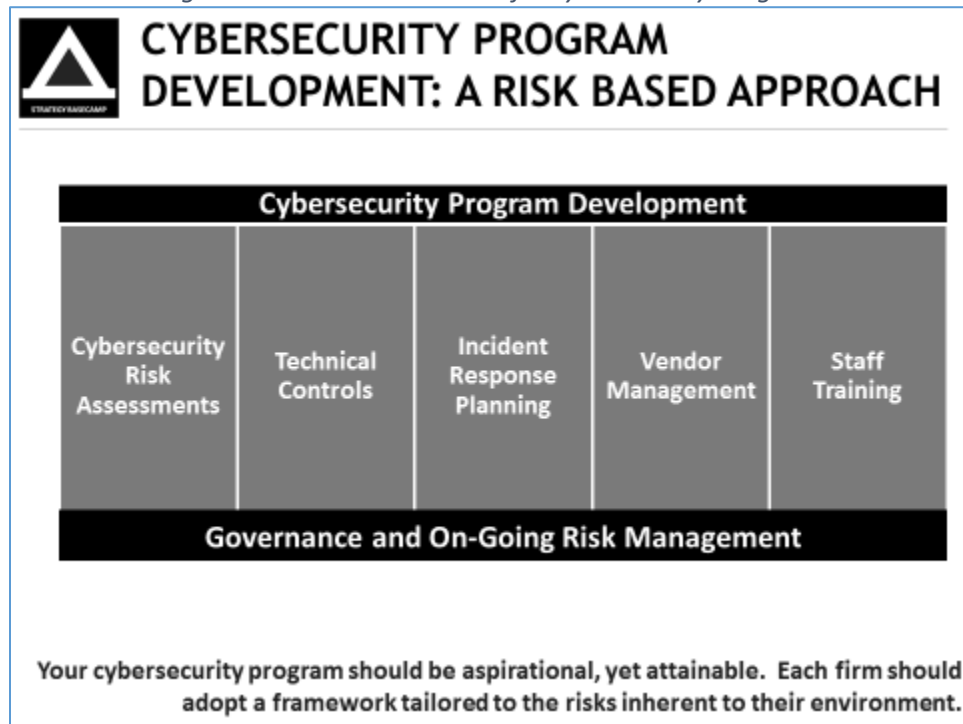
CYBERSECURITY RISK ASSESSMENTS

Planning Your Cybersecurity Work

Below is a depiction of the key elements of an overall cybersecurity program. The risk assessment, and related documentation, drive the plan and communicate the actions needed. The risk assessment defines the problems in need of solutions (whether they be related to technology controls, process improvements, and/or staff training).

Effective planning and risk management also helps to ensure that time, money, and efforts are targeted on the highest priorities.

Figure 2: Essential Elements of a Cybersecurity Program



Before starting the risk assessment, take time to think about your firm and similar work previously completed (e.g. documenting your systems / applications / networks, previous cybersecurity incidents, etc.). These items will serve as inputs to the process. For example, gather and review documents such as your existing information security plans, system application diagrams, a list of devices connected to your network, etc.

Documentation of your current technology environment and related processes serves other useful purposes. This documentation serves as the foundation for any major technology (e.g. better integrating your technology applications or selecting a new software vendor) or process improvement initiative.

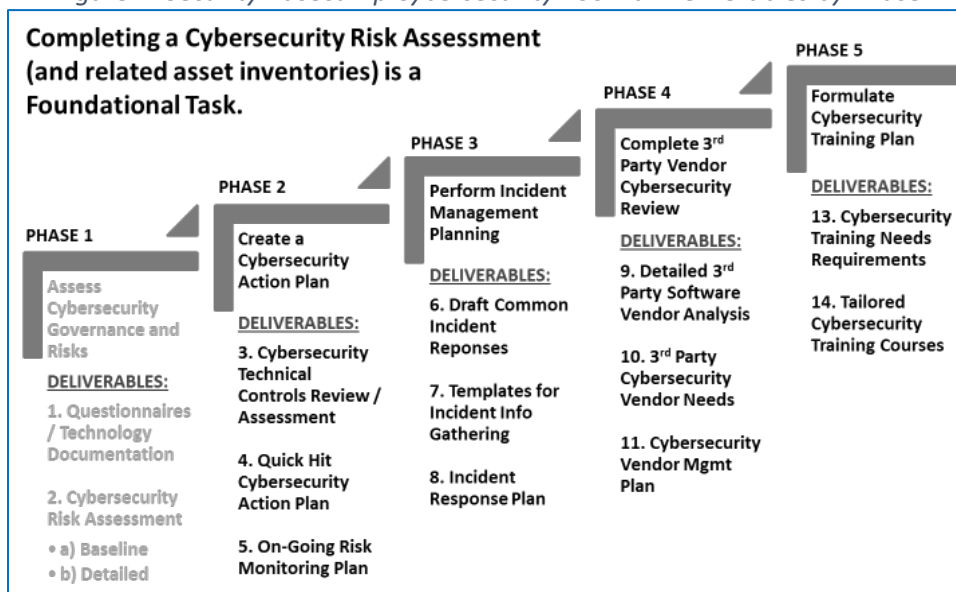
Tailor your cybersecurity project to the particular needs and resources of your firm. Consider the skills and capabilities of your team in order to better plan “who does what by when” and to determine if and when you need to bring in external resources. See the figure below for an illustration of the types of information evaluated during Phase 1 of the *Security Basecamp Cybersecurity Toolkit* methodology. A key point of our value is understanding what questions should be posed and answered in completing the process.

Figure 3: Cybersecurity – Security Basecamp Project Intake Questionnaire Excerpt

PHASE	TASKS / DELIVERABLES	COMPLETE (YES / NO)	NOTES
PHASE 1: ASSESS CYBERSECURITY GOVERNANCE AND RISKS			
CREATE CYBERSECURITY RISK ASSESSMENT:			
Cybersecurity Governance Risk Assessment:			
	Assess firm's written information security policy		
	Evaluate most recent periodic cybersecurity risk assessments (if performed) and related findings		
	Evaluate cybersecurity roles and responsibilities for the firm and third-party stakeholders		
	Evaluate written business continuity plans and plans that address mitigation of effects of cybersecurity incidents and/or recovery of from such incidents		
	Evaluate cybersecurity insurance policies (if in existence)		
Protection of Firm Networks and Information:			
	Evaluate firm's written guidance and periodic training to employees concerning information security risks and responsibilities		
	Evaluate controls to prevent unauthorized creation/escalation of user privileges and lateral movement among network resources		
	Evaluate controls to restrict users to those network		

Attention to detail tempered by business acumen is necessary for a successful cybersecurity program. Senior leadership involvement and an effective governance structure increases the likelihood of success. Day to day execution of a well-organized set of deliverables and tasks, monitoring progress, and leveraging questionnaires that guide the process drive better outcomes efficiently. Finally, it is important to have a diverse set of functional team members. This work is not just to be owned by technology or driven by compliance. Cybersecurity is a team effort.

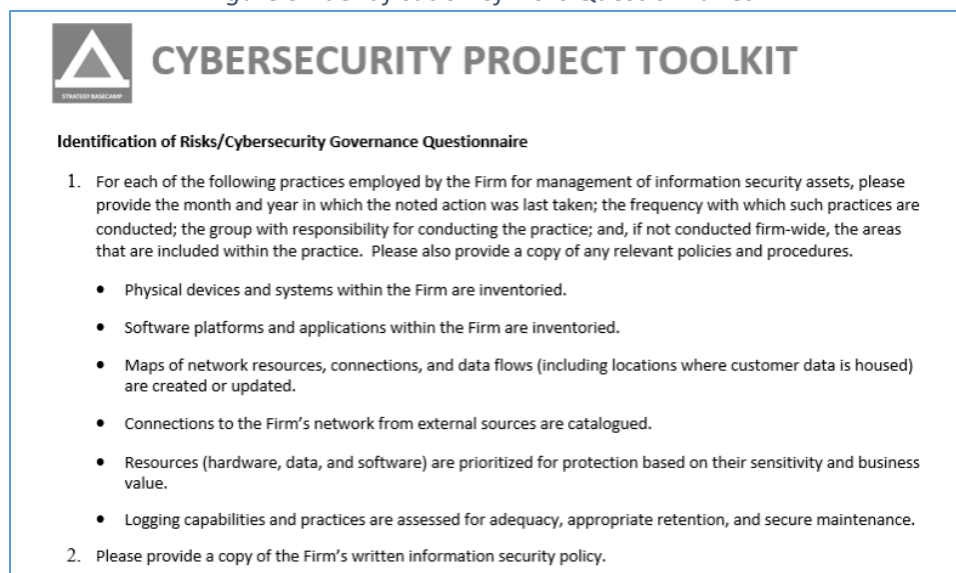
Figure 4: Security Basecamp Cybersecurity Toolkit - Deliverables by Phase



Executing the Work

As illustrated above, the initial phase of cybersecurity program development involves the completion of questionnaires¹⁵ and asset inventories, documentation of critical assets, and the completion of a formal cybersecurity risk assessment report. Security Basecamp completes this risk assessment report for its clients.

Figure 5: Identification of Risks Questionnaires¹⁶



CYBERSECURITY PROJECT TOOLKIT

Identification of Risks/Cybersecurity Governance Questionnaire

- For each of the following practices employed by the Firm for management of information security assets, please provide the month and year in which the noted action was last taken; the frequency with which such practices are conducted; the group with responsibility for conducting the practice; and, if not conducted firm-wide, the areas that are included within the practice. Please also provide a copy of any relevant policies and procedures.
 - Physical devices and systems within the Firm are inventoried.
 - Software platforms and applications within the Firm are inventoried.
 - Maps of network resources, connections, and data flows (including locations where customer data is housed) are created or updated.
 - Connections to the Firm's network from external sources are catalogued.
 - Resources (hardware, data, and software) are prioritized for protection based on their sensitivity and business value.
 - Logging capabilities and practices are assessed for adequacy, appropriate retention, and secure maintenance.
- Please provide a copy of the Firm's written information security policy.

Step 1: Inventory and Identify Critical Assets

Asset inventories are a key component of a risk assessment. Assets, in terms of a cybersecurity risk assessment, are defined as: people, hardware, business applications and other software, and data on the firm's network. In order to assess risks, firms need to know what assets they have, what assets are authorized to be on their network and what assets are most important to protect. Both the NIST Framework and SANS Top 20 identify inventories as foundational activities, and the NIST Framework also underscores the importance of identifying critical assets.¹⁷

For broker-dealers, one consideration in identifying critical assets is the firms' obligations under Regulation S-P to protect customers' personally identifiable information (PII). Therefore, databases containing personal client data and business applications containing this data would normally be considered critical assets. In addition, firms may establish a variety of other criteria to prioritize assets, for example, their importance to the firm's business operations (such as trading systems), whether clients or others have online access to initiate transactions, whether there is an impact to order routing, whether the asset could allow client statements to be altered, whether the asset allows for delivery of securities or cash—e.g., wire transfers—and whether the asset is designed to fill a critical regulatory need.

Step 2: Assess Threats and Vulnerabilities

Firms use a variety of inputs for their risk assessment process. With respect to threats, these inputs include **past cybersecurity incidents** either at the firm or noted in the industry, threat intelligence identified from other organizations or through security organizations such as the Financial Services Information Sharing and Analysis Center (FS-ISAC). These

¹⁵ Security Basecamp's approach leverages a sample list of requests for information that the U.S. Securities and Exchange Commission's Office of Compliance Inspections and Examinations (OCIE) may use in conducting examinations of registered entities regarding cybersecurity matters. Some of the questions track information outlined in the "Framework for Improving Critical Infrastructure Cybersecurity," released in February 2014 by the National Institute of Standards and Technology.

¹⁶ *Ibid*

¹⁷ See NIST Framework, ID.AM-1, ID.AM-2, ID.AM-5, p. 20, and SANS Top 20. SANS is an organization that provides security training / certification.

threats can include both internal threats—e.g., threats from employees—or external threats, such as hackers or organized crime groups.

Another important component of the risk assessment process is **vulnerability analysis**—that being the process of identifying, quantifying and prioritizing potential vulnerabilities within a system. Firms' approaches will differ regarding assessing threats and vulnerabilities in producing an overall risk assessment. For example, in some cases it is helpful to develop proprietary risk assessment methodologies while in others, to use vendor products tailored to the firm's needs. The sophistication of vulnerability analysis varies across firms. Judgement should be used to determine what is appropriate.

One relatively simple, yet pragmatic approach to performing vulnerability analysis is shown in the figure below. Informational assets are given a value of critical, high, medium, or low. The risk level of those informational assets is also given a rating of critical, high, medium, or low. The final level of risk depends on actions taken by the broker-dealer or investment advisor.

Figure 6: Security Basecamp Basic Framework for Measuring and Reporting Cybersecurity Risk

Informational Asset (From the Assets Identified During Step #1)	Severity Value (Critical / High/Medium/ Low)	Risk Level (Critical / High/Medium/ Low)	Vulnerability Score (Severity Value + Risk)	Notes / Actions
Informational Asset X	See below	See Below	Vulnerability = Impact + Likelihood	
Informational Asset Y	“ “	“ “	Vulnerability = Impact + Likelihood	

Severity values and risk levels may be assigned based upon the following classifications (and can be tailored as needed):

Figure 7: Assessing Business & Regulatory Impact Severity Levels

Severity Level	Score	Definition (Tailed to Client Engagement)
Critical	4	Unmanageable impact on financial performance (e.g. bankruptcy or loss of income that impairs the firm), brand damage, clear violation of privacy or regulatory compliance
High	3	Measurable impact on financial performance, potential loss of clients / accounts, potential violation of privacy or regulatory compliance
Medium	2	Minor impact on financial performance, minimal impact on clients / accounts, no violation of privacy or regulatory compliance
Low	1	No financial / reputational / compliance impacts

Figure 8: Assessing Risk Likelihood Levels

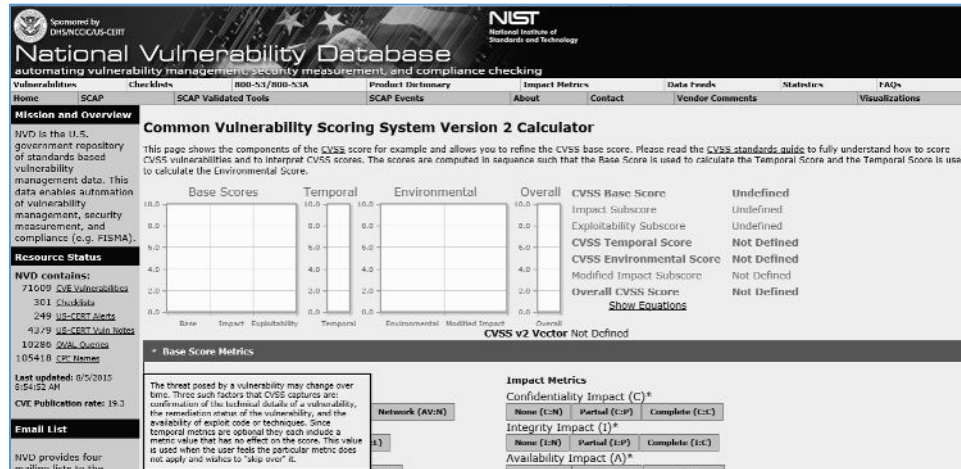
Risk Level	Score	Definition (Tailed to Client Engagement)
Critical	4	Known vulnerability / known intrusion / difficult to detect cyber incidents
High	3	Probable intrusion / vulnerability in the absence of a control / difficult to detect intrusion or cyber incidents
Medium	2	Possible, but not probable intrusion / difficult to exploit vulnerability / easy detection of intrusion or cyber incident
Low	1	Known controls to prevent risk / Easy detection of intrusion or cyber incident

These ratings feed into the firm's cybersecurity governance process and play a key role in driving a firm's risk remediation efforts. Asset vulnerabilities are ranked, prioritized, and discussed. This level of information allows the organization to decide where to focus its effort and action planning. Typically, ratings of critical or high risk require remediation or approval through a risk acceptance process. **One challenge noted in this process is maintaining visibility**

on assets that evolve from low to high risk. This may occur, for example, if an application is not updated or if it handles new types of data.

Another, more complex approach used to assess vulnerabilities is the Common Vulnerability Scoring System (CVSS). CVSS is an industry open standard for assessing the severity of vulnerabilities and prioritizing their remediation.

Figure 9: Common Vulnerability Scoring System Calculator



The Common Vulnerability Scoring System (CVSS) approach is significantly more complex than what would typically be used for a small to mid-sized company such as an independent broker-dealer or investment advisor. That said, reviewing the approach, leveraging elements of it, and incorporating key concepts to your firm is attainable. Other helpful tools and resources (e.g. the OWASP Risk Rating Methodology¹⁸ upon which the *Security Basecamp Basic Framework* above is modeled) exist and Security Basecamp, as business and technology consultants, can help you tailor an approach to measuring risks and vulnerabilities to your organization's needs and risk profile.

In the context of the enforcement case study cited earlier, a database containing unencrypted confidential customer information without effective password protection and exposed to the Internet would be considered a critical risk. A risk assessment process coupled with vulnerabilities analysis could have identified the firm's exposure before the firm's data was stolen. The firm would have then been in better position to implement the requisite controls.

Step 3: Address Identified Risks – Implementing Controls

The primary purpose of a risk assessment and associated vulnerability analysis is to determine what technical controls need to be implemented or enhanced in order to mitigate the identified risks. The controls can take several forms:

- **Preventive**—these are controls to stop or prevent harm from taking place in the first place; these include, for example, anti-malware, anti-virus software and privilege management tools.
- **Detective**—these are controls a firm uses to identify potential threats that may have occurred, for example, through the detection of data leakage or email content analysis.
- **Corrective**—these are controls that restore a system or process back to the state prior to the detrimental occurrence, for example, a business recovery process that could restore a system to its original state after a system outage.
- **Event Predictive**—these are controls that would predict a detrimental event happening, such as notification that a specific type of hack has been occurring at similar firms.

¹⁸ OWASP Risk Rating Methodology, https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology (Web, August 2015)

Some smaller firms that are at an earlier stage of maturity in their cybersecurity program do not have the in-house expertise to conduct risk assessments, assess vulnerabilities, and decide which controls would be most effective. For that reason, many broker-dealers outsource the process, or elements of it, to a vendor or 3rd party offering professional services.

Security Basecamp has drawn heavily on guidance from the SEC, FINRA, Securities Industry and Financial Markets Association (SIFMA), and the National Institute of Standards and Technology (NIST). We work with your compliance, operations, and technology team to plan and monitor the work done within your technical environment. Your team executes the detailed technical tasks using our methodology and planning as a guide. Security Basecamp also plays a critical role in assisting to guide the work, document the work, manage progress, and by including applicable industry best practices throughout your project.

There are numerous controls that can be considered. Below is a simple list presented for illustrative purposes. Depending upon the severity and likelihood of a particular attack, firms are wise to consider a layered (e.g. “castled”) approach to controls. Envision a series of defenses similar to the construct of castle – i.e. multiple controls all designed to protect the firm. Should one layer fail (e.g. a firewall), then another set (e.g. passwords, data encryption, employee training, etc.) may prove sufficient in thwarting an attack.

Figure 10: Cybersecurity: Example Areas Firms May Want to Improve Controls to Reduce Cyber Risks

Data storage at vendors	Privilege management	Software development lifecycle
Employee training	Wi-Fi protection	Web/URL filtering
Data encryption	Email content filtering	Staff skillset matching
Employee access controls	Customer access controls	Vendor access controls
Patch and software updates	Hand-held device protection	Software patch management

Regardless of a firm’s ability to perform a risk assessment and to take action based upon its results, FINRA notes that what is important from an effective practice perspective is that firms have defined escalation processes to address risks identified as not appropriately mitigated. Typically, the more significant the risk, the higher the level of management approval required to accept that risk (i.e. to ignore it). If making a decision to accept a risk at a higher level than the firm would like, it is important to have a plan of action for addressing and mitigating that risk. It is also important to set due dates for implementation of all risk mitigation actions. All firms indicated that high or critical risks dealing with customer PII or critical firm information without adequate mitigation controls were unacceptable. Assess controls in need of immediate action and also identify a process for on-going risk monitoring and improvement.

In the end, protecting yourself might not be as hard as you think – there are straight forward steps to be taken. It does take time and effort. There are a set of essential controls all broker-dealers and investment advisors should review for potential implementation¹⁹. Reasonable approaches exist to formulating your firm’s cybersecurity program. Most importantly, firms should decide to take measured action beginning with a risk assessment that creates a tangible set of focused controls.

¹⁹ Security Basecamp has formulated a list of actions it recommends all broker-dealers and investment advisors of any size review (and implement as necessary) called its *Quick Hit Technical Controls Review*.

ABOUT SECURITY BASECAMP

Security Basecamp is a consulting firm focused exclusively in the financial services industry. We partner with executives and managers to facilitate effective business planning and help you competitively leverage technology for profitable growth. Our mission is to help financial services firms solve their most challenging strategic business issues through critical thinking, rigorous project management, and/or the savvy use of practical technologies.

Collectively, our consultants have managed hundreds of strategy, operations, technology, compliance, and business development projects over the past 25 years. We bring a business oriented approach to completing cybersecurity projects and the technical acumen to work effectively with your internal IT staff. We help you manage the cybersecurity analysis, action planning, and execution that your busy management team doesn't have the time or resources to lead.

To learn more, visit our website (securitybasecamp.com) or call (949) 330-0899.

AUTHOR INFORMATION

Paul Osterberg
(949) 330-0899 or (800) 276-8423
posterberg@securitybasecamp.com