Cybersecurity Requirements Kit

Instructional Template for Compliance
of U.S. Investments Firms with
SEC OCIE Cybersecurity Initiative[1]

[1] *SEC OCIE's* September 15, 2015 *Cybersecurity Examination Initiative*

Table of Contents quick.link

This ***Cybersecurity Requirements Kit*** is designed to outline the cybersecurity points an investments firm must contemplate and determine, in order to satisfy the *SEC OCIE's* September 15, 2015 *Cybersecurity Examination Initiative*[1]. **Intersource Consulting Group LLC ("Intersource")** has developed this instructional document for your financial services firm, in its efforts to comply with the *SEC*'s cybersecurity regulations.

This *9/15/2015 SEC Initiative*[1] strongly recommends[2] that the following cybersecurity *areas of focus*[20] be addressed by financial firms:

- Governance and Risk Assessment
- Access Rights and Controls
- Data Loss Prevention
- Vendor Management
- Training
- Incident Response

Intersource provides this *Cybersecurity Requirements Kit* as a basis for financial firms to establish their own customized set of *Written Information Policies & Procedures* ("*WISP")*[3], tailored to the specific business and information control environment of each firm.

[2] In 2016 **Intersource** has consistently observed that the SEC has been treating *OCIE's* September 15, 2015 *Cybersecurity Examination Initiative* as ***Regulation***, as opposed to a set of strong recommendations.

[3] The *WISP (Written Information Policies & Procedures)* for an investments firm have been promulgated in the *Governance and Risk Assessment* cybersecurity area of the *SEC OCIE Cybersecurity Examination Initiative*[1].

Table of Contents quick.link

Intersource Consulting Group LLC is a financial services consulting firm, specializing in compliance with securities regulation for *FINRA/SEC*-registered *broker-dealers* and *investment advisers*.

Ernie D. Kappotis, the *Chief Financial Officer* ("*CFO*") of **Intersource**, is a 2001 graduate of ***Boston College****'s Carroll School of Management*, one of the most prestigious universities in the United States, currently ranked 22nd nationally by *Forbes* magazine. He is also a 15-year member of the *Boston College Club*, the university's downtown Boston alumni networking social organization. Mr. Kappotis is the author of this *Cybersecurity Requirements Kit.*

A 9-year ***FINOP*** **(*FINRA* Series 27**-registered *Financial and Operations Principal*), Mr. Kappotis is a net capital expert, providing securities firms with Remote CFO services and represents his clients during the financial portions of their examinations administered by *FINRA* (the *Financial Industry Regulatory Authority*) and/or the *SEC* (*U.S. Securities and Exchange Commission*).

Mr. Kappotis, a lifetime resident of Peabody, Massachusetts (slightly northeast of Boston) served as a *FINRA Sales Practice Examiner* at the regulator's Boston District from 2011-15, specializing in financial and net capital examinations of broker-dealers.

Prior to Kappotis' tenure at *FINRA*, he held the post of *In-House FINOP* for 4 years at Boston equity research firm *Detwiler Fenton & Co.*, a landmark of Boston's financial district since 1962.

Table of Contents quick.link

Donald R. Pollard, the *Senior Managing Partner* of **Intersource** holds his Management degree from ***St. Joseph's College*** on Long Island. With over 25 years in the securities industry, including a presence on Wall Street, Mr. Pollard has vast regulatory experience, featuring tenure at *E*Trade*, *Oppenheimer*, and *Smith Barney*.

Mr. Pollard was an integral driver in constructing the 1990s on-line trading platform at *Quick & Reilly*, navigating and maintaining the required compliance for that digital arena.

Donald Pollard serves as **Intersource's** *Chief Compliance Officer ("CCO")* for its broker-dealer & investment adviser clients. He holds ***FINRA's* Series 24**, 7, 4, 8, and 63 Licenses.

Table of Contents quick.link

Cybersecurity Requirements Kit
Table of Contents:

Table of Contents quick.link

I. Customer Data:

Expanding upon terminology from the U.S. Department of Commerce's National Institute of Standards and Technology (*NIST*), your financial firm can categorize Customer Data into the following 3 primary categories (*Table 1*):

PII	Personally Identifiable Information
NPPI	Non-Public Personal Information
RNPPI	Restricted Non-Public Personal Information

Using the *NIST* guideline, *PII (Personally Identifiable Information)* can be quantified as the following:

- Name
- Social security number
- Passport number
- Driver's license number (or state-issued identification number)
- Residential address
- E-mail address
- Personal characteristics (photograph, fingerprints, handwriting, eye color, hair color, height, weight, facial geometry, voice recording, etc.)

Cybersecurity concerns are paramount for financial firms versus other industries because investments companies, by the nature of the services provided, inherently possess a wide range of *PII*.

PII Data should be separated into *Public PII* and *Non-Public PII ("NPPI")*.

A common measurement to determine if *PII* is *Public* is the *Google* test. If you perform a *Google*-search on an individual's name, the results would be considered to be *Public PII*. If the individual discloses his/her place of employment, and you can access information about that person from the employer's website, that data is also *Public PII*.

Most of the types of information listed above (the majority of which are held by financial firms) are forms of *Non-Public PII, or NPPI*, and investments companies have an obligation to protect both their customers' *PII* and *NPPI*.

RNPPI (Restricted Non-public Personal Information) is even more highly sensitive customer data, such as dates of birth, annual gross income figures, and medical information. If compromised, both *NPPI* and *RNPPI* could materially damage an individual's finances, reputation, and/or well-being. *RNPPI* could also identify an individual or family as high-net worth, potentially targeting that individual/family to hackers. Your financial firm obviously has a *material* obligation to safeguard

Table of Contents quick.link

customers' *RNPPI*, and is expected by the *U.S. Securities and Exchange Commission (SEC)* to enforce an information flow environment with effective controls and safeguards over all three forms of Customer Data – *PII, NPPI,* and *RNPPI*. That system of controls and safeguards over the information environment of a financial firm is called the *Written Information Security Policies & Procedures ("WISP")*[2].

A lot of broker-dealers, investment advisors, and dual broker-dealers/investment advisory firms don't know where, or what in what context, their *WISPs* exist. The *WISP* may be present within the firm's overall set of Written Supervisory Procedures ("*WSPs*"). If this is the case, such a *WISP* is often represented, or documented, in the form of a separate appendix or exhibit; because the specified responsibilities and workflows inherent under the *WISP* are often too complex and/or detailed to logically fit within the confines of the *WSPs* (similar to several *AMLCPs* "Anti-Money Laundering Compliance Programs").

> Some firms have a *Data Protection Policy* and/or a set of *Information Privacy Procedures*. The *WISP* should be a combination of those policy manuals, and should also include, in detailed fashion, the tasks that will be executed in order to safeguard customers' information and records.

Some U.S. States have specific laws outlining levels of protection that companies must take over customer data. For example, the Commonwealth of Massachusetts goes further than the *SEC* in its jurisdiction over enterprises' safeguards over customer information, stating the following:

Commonwealth of Massachusetts 201 CMR 17 Data Protection Law (March 1, 2010):

> *The objectives of this regulation are to insure (sic) the security and confidentiality of customer information*
> *in a manner fully consistent with industry standards;*
>
> *protect against anticipated threats or hazards to the security or integrity of such information;*
>
> *and protect against unauthorized access to or use of such information that may result in substantial harm or inconvenience to any customer.*

Table of Contents quick.link

In the United States, most cybersecurity lawmakers, consultants, and regulators can agree that –

A financial firm needs to assess:

- The *types* of information it has possession over (both proprietary & customer)
- *How* each information type needs to be safeguarded.

A data type matrix, using the references identified in *Table 1*, is an optimal method for firms to categorize their data.

Communications:

When electronically sharing customer data, it is advisable to use secured, encrypted means to do so. Secure encryption is often confused with password-protection, which is altogether different. Simply linking a file password to a *Microsoft*, *Adobe*, or any other software file does not encrypt that data. While linking the password has added security to that file, it has by no means encrypted the file or its underlying data.

In no way diminishing the password-protection feature in certain instances (which can be beneficial), customer data really should be transmitted in a secured, encrypted means. Various on-line companies provide secure, encryption resources. *AppRiver*[3] and *ShareFile* are two such vendors.

Using a secured, encryption vendor enables users to transmit customer (or otherwise sensitive) data through an on-line portal, to which the other users (customers, vendors, third-parties, consultants) are securely *invited* through a vendor e-mail. With some vendors, such as *AppRiver*[3], a recipient first has to be invited to become a user, before becoming eligible to receive data and/or messages. But, with *ShareFile* and others, the recipient can immediately begin to receive data and/or messages; however, the recipient has to, minimally, provide a UserID/e-mail address and/or password to track themselves within the portal as having received that data/message.

Unlike a conventional e-mail (which people can delete, or dispute whether they sent or received it), *AppRiver*[4], for example, automatically tracks & documents when all data transmissions are received, read, replied-to, and/or forwarded. The service also allows the sender (viewed from this perspective as the *owner* of the data) to recall previously-sent data once the sender determines that the information should have been used and/or moved to another storage location.

[4] *AppRiver* (www.appriver.com) is a Florida-based e-mail encryption company, a major national market leader is that space, which can be employed by organizations & individuals to electronically transmit sensitive information.

Table of Contents quick.link

Independent even of the additional layers of security/encryption provided by these vendors is the inherent goodwill expressed between business parties utilizing such resources; knowing that the other party will enact the utmost degree of protection over the sensitivity and confidentiality of its information.

II. Proprietary Information Systems:

Storage:

Financial services firms predominantly store their proprietary and customer information within various information systems. These systems are typically stored in one or more of the following locations:

- Physical server(s)
- Off-site server(s), typically through a vendor relationship
- The Cloud (internet), through a vendor relationship

Broker-dealers, for example, are required under *SEC Act 1934.240.17a-4* to retain *all* of their electronic records[5] in an easily searchable and readily available format. Currently, most Cloud vendors will not attest to *17a-4*[4]; meaning that they will not commit to making available easily searchable broker-dealer records for regulators. In other words, while an investments firm can retain records in The Cloud, such a decision most often will not comply with the *SEC's* electronic records retention requirements.

A firm can use its own physical server(s) to retain electronic records, however the firm must test to ensure that such a proprietary server(s) consistently produces up-to-date and easily searchable records, which can be made readily available (within a few days) to regulators, upon request. *FINRA Rule 8210* usually allows a broker-dealer 14 business days to produce requested records; however a financial firm most likely will want to review such records before disclosing them to the regulator.

[5] Financial statements stored electronically (which is mostly the case) within a general ledger system (i.e. *QuickBooks, Peachtree, Xero, Great Plains, SAP, Oracle*, etc.) also must be retained, pursuant to *SEA 17a-4*.

Table of Contents quick.link

The preferred method for a financial services firm to meet the *SEC's* electronic records retention requirements (*17a-4*) is to retain the records at an off-site server, contractually maintained by a vendor. Not only will the firm not have to allocate any of its own resources toward retaining the records, but, more importantly, the vendor will provide the firm with a *17a-4* electronic records retention attestation letter[6].

Systems:

In addition to general ledger accounting systems (discussed in Footnote 2) and financial reporting software, financial firms use a wide array of other systems (the following) to manage the services they provide to clients.

Shared-Networks:

Several financial firms make proprietary and customer data available to employees using shared-network folders and files. While this flexibility often increases the efficiency of work and simultaneous viewing access, such shared arrangements can compromise the sensitivity of the underlying data, if not properly safeguarded.

> For example, does your firm want to make any folder and/or file accessible to all employees? A lot of firms do that. But, does that really make sense? Who *needs* access to particular pieces of data? Such questions will be explored in *Section IV – Access Rights and Controls*.

Clearing Arrangements*:

Several broker-dealers and investment advisers have contractual arrangements with clearing firms (such as *Merrill Lynch, Pershing, National Financial Services, Sterne Agee*, to name a few), which process their proprietary and customer securities transactions. Such relationships preclude the broker-dealers and investment advisers from having to trade securities from their own inventories. A clearing arrangement allows such firms to send orders to another broker-dealer (i.e. the *Custodian* clearing firm), and the custodian then executes the trade on behalf of the financial firm.

---

[6] *FINRA* requires its broker-dealer members to keep current all of their *17a-4* electronic records retention attestation letters (both proprietary & vendor-provided) within *FINRA's Firm Gateway* system.

Table of Contents quick.link

While clearing firm relationships solve inventory and capital hindrances which broker-dealers and investment advisers may face, such relationships also open additional layers of electronic systems and data. The major clearing firms have their own systems, which the subscribed *Correspondent* broker-dealers and investment advisers have a responsibility to access and monitor, in order to effectively supervise their customers' securities activities[7]. That means that any reports or supplementary information generated by the Correspondent through the Custodian's systems (which are not regularly archived by the Custodian, pursuant to the written Clearing Arrangement) automatically become property of the financial firm, and therefore subject to the *SEC 17a-4* retention and all other books & records regulatory requirements.

Trading Systems:

As trading methods continue to evolve, financial firms are matriculating to new and advanced platforms[8]. For some firms (like in the instances of high-frequency, algorithmic traders), the trading system may present the most risk-laden confidential information source in the whole company. If a hacker could somehow obtain access to a high-frequency trading account, the resulting activity could bring down an entire firm, and its customers[4].

Regardless of the complexity of a firm's proprietary trading system(s), adequate safeguards and controls must be implemented and monitored on a continuous basis to ensure not only the effectiveness and compliance of the system(s), but also the confidentiality of the client's transactions and personal information.

Portfolio Software:

Then, financial firms possess a wide array of production and statistical software to monitor their businesses. Advisory firms typically use portfolio software packages such as *Advent* and others. Such portfolio management systems, in addition to producing a wide range of reports to assess the performance of securities and sectors, also calculate the quarterly investment advisory fees charged to the clients. Such systems pose the critical question:

[7] The investing customers are direct customers of the Correspondent broker-dealer or investment adviser, not the Custodian clearing firm. The customers sign an account agreement with the broker-dealer or investment adviser, where it must be disclosed that all (or specific) securities transactions will be executed under a fully-disclosed clearing agreement with the Custodian.

[8] Most of these firms clear (execute) their own trades, unlike those with Clearing Arrangements[*]. These broker-dealers must maintain customer reserves, which are assessed in their net capital computations.

Table of Contents quick.link

Who, and under what controls, will be permitted access to such systems? That risk will be critically analyzed in *Section IV – Access Rights and Controls*.

Most broker-dealers record commission payouts independent from their clearing arrangements, using production databases. Those reports need to be reviewed by registered securities principals to ensure that production-based expenses adequately correspond with commission revenue; the adverse result of which could be disastrous on many regulatory levels.

So, how is this data entered into such production systems? Is the data correct?

> What is the process, and what are the controls, associated with processing the securities data within the production system?
>
> These types of concerns will be further assessed in *Section III – Risk Governance*.

Resource Management Systems[7]:

Then, financial firms utilize various resource management systems (such as *Microsoft CRM*, *Oracle*, *SAP*, *SalesForce,* and others) in order to analyze their business programs and segments from a macroscopic level.

Some of these systems merely organize customers, projects, and tasks. However, such systems may often be customized to the preferences of the financial firm, and allow for more intricate analysis. For example, firms can segment a project into specific task workflows, each assignable to a particular employee, with specified dates for completion, etc. To the extent that such workflows involve customer data and business (which they almost always do), such records must also be retained, pursuant to *17a-4*. More importantly, such records must be safeguarded so that outside parties, or worse – hackers, cannot gain access to them.

Regulatory Reporting:

Financial firms have to comply with several regulations and regulatory authorities. The SEC and/or FINRA are the two primary regulators that financial firms must satisfy on an ongoing basis. Such compliance often includes reports – Written Supervisory Procedures, Supervisory Controls Testing, AML reporting, financial reporting (Annual Audited Financial Statements, FOCUS reports, etc.), and several other forms.

Two significant questions to answer here are:

1. How are the reports being generated, and who is involved in their production?
2. How are such reports provided (or submitted) to the designated regulator?

> Both questions, again, lead to access & rights. Who has *access* to the information? Who possesses the *rights* to transmit such data to the regulatory authority?

Table of Contents quick.link

III. Risk Governance – *Written Information Security Policies & Procedures* (*WISP*[2]):

After outlining the various types of data & systems your financial firm may utilize, you need to assess how such data & systems will be managed and safeguarded. The *9/15/2015 SEC OCIE Cybersecurity Examination Initiative* recommends that every financial services firm have a Chief Information Security Officer ("*CISO*"). The *Initiative* does not opine on what other role(s) the *CISO* should have at the firm (i.e. CCO, CIO, etc.), however it specifies that the *CISO*[9] should be "responsible for cybersecurity matters."

The *Initiative* also expresses that "other employees" should also be responsible for cybersecurity matters; not limiting responsibility to the *CISO*[8].

Your financial services firm should select a *CISO* that has a deft grasp on the firm's overall lines of business & processes, while also possessing an intimate familiarity with the firm's levels & types of information (especially customer-related) and its systems. The *CISO* should also be well-versed and current in the regulatory (*SEC, FINRA,* individual State) perspectives and expectations pertaining to cybersecurity compliance.

So, while your Chief Information Officer (CIO) or Chief Operating Officer (COO) may have the most in-depth knowledge of your firm's overall business, data, systems, and processes; that individual may not be the best source for the regulators' expectations for cybersecurity compliance. And, vice versa, while your CCO may have a solid grasp on the *SEC's* most up-to-date cybersecurity recommendations and best practices, that individual may not possess enough expertise regarding the interrelationship between the firm's complex systems.

> The conclusion the *CISO*[8] delegates cybersecurity responsibilities.is that your firm should select as *CISO* the employee with the best *overall*, *balanced* understanding of its business *and* the aggregate information environment under which it operates.

The *SEC Initiative* immediately identifies the *WISP*[2] (for which this instructional template represents) as the first component to *Risk Governance*, articulating that:

> The *WISP* must:

- Protect "*broker-dealer customer and/or investment adviser client … records and information, including those designed to secure customer documents and information*,"
- "*protect against anticipated threats to customer information,*"

[9] *CISO – Chief Information Security Officer*. The *SEC Cybersecurity Examination Initiative (9/15/2015)* does not dictate that the *CISO* of a broker-dealer needs to a be a *FINRA*-registered individual.

Table of Contents quick.link

- "*and protect against unauthorized access to customer accounts or information; "*

The *Initiative* further recommends that the *WISP*[2] include a description of the firm's organizational structure, particular to "*the positions and departments responsible for cybersecurity-related matters* …", which, of course, include the *CISO*[8], and any and all employees with which the *CISO* has delegated cybersecurity supervision or maintenance responsibilities.

In *Section I – Customer Data*, it was explained that the *WISP* should incorporate the dynamics of *both* a firm's *Data Protection Program* and *Information Privacy Protection Procedures*. Moreover, the *WISP must* be consistent with your firm's overall *WSPs (Written Supervisory Procedures)* as such overall procedures pertain to information security.

Adequate business insurance coverage is a key factor for both broker-dealers and investment advisory firms (*i.e.* Errors & Omissions "E&O", Directors & Officers "D&O" Liability, Financial Institution "Fidelity" Bond, Retirement Plan insurance, etc.). E&O, D&O, Fidelity, and other forms of General Liability insurance may contain cybersecurity provisions and/or associated levels of insurable coverage & deductibles pertaining to information theft and/or data breaches.

Such cybersecurity insurance provisions may contain procedures, which your firm may be able to incorporate, in some degree, within your *WISP*. So, it is advisable to review any cybersecurity provisions within your firm's business insurance policies before crafting, or enforcing the *WISP*.

As with any other layer of regulatory compliance, *documentation* is key to addressing or resolving potential customer problems; and therefore, *documentation* will also be paramount in securing an effective *WISP* for your firm's cybersecurity environment.

Not only do reasonable processes & procedures need to be implemented and supervised, but the steps associated with such processes & procedures need to be documented, in order to evidence that they occurred.

The *WISP* should also include the hierarchy through which the *CISO* delegates cybersecurity responsibilities. The hierarchy should be established in a manner which prompts the detection of risk within the firm's information data-flows, systems, and ports of entry/egress.

A *WISP* is designed to be complex, workflow-oriented, and task-specific – an illustration of a financial firm's information environment and the controls required to protect it from internal and external threats. Due to its complexity and specificity, several firms will find it beneficial to work with a cybersecurity compliance consultant to ensure that their *WISP* manuals are adequately updated on a timely basis.

Table of Contents quick.link

Like any other supervisory controls systems at your firm, the *WISP* needs to be periodically tested to ensure that it continues to safeguard the firm's proprietary and customer information. This process of evaluating the *WISP* will be further explained in *Section X – Independent Cybersecurity Assessment*.

IV. Access Rights & Controls:

A financial firm's sensitive data (such as *NPPI* and *RNPPI - Section I*) can only be protected to the extent that access to such data is restricted to those employees, third-parties, and/or vendors that require such access in order to provide customer services, or enable customer services to be provided.

Most financial firms use networks, which require universal log-in IDs and passwords to enter. But, what happens after that point? Should every employee have the same access to the full window of your firm's business and services? Most likely, not.

Microsoft, for example, and other operating systems, are equipped with various security parameters, which can limit access to specific folders and/or files; and often such restrictions can be set based upon the universal log-in. For example, if John Doe's log-in ID is Jdoe32#, once John "universally" logs-into the network, his log-in ID can automatically grant him access to various folders, files, and systems to which he needs access. The *CISO*[8] is ultimately responsible for determining who needs access to which records, systems, and functions.

Access Rights & Controls can be very clearly illustrated within the financial recordkeeping sector. Every broker-dealer, for example, is required to have a general ledger, which contains all of its financial transactions.

One of the most important regulatory questions asked by financial examiners is:
Who has *access* to that general ledger?

That depends on a number of factors:

- How large in the firm (i.e. How much business & how many transactions are consistently flowing through the general ledger)?
  - How many employees are adjusting (recording entries) within the general ledger?
  - Which employees need to review the accounts and transactions?

- How does the firm disburse its cash? Often, cash is disbursed through the general ledger. How many of the accountants need to be able to disburse cash (print checks, release wires, execute bank ACH payments, etc.)?

- Is there anyone (not a day-to-day accountant) at the firm (CFO or Controller perhaps) who may need to know the current or historical financial records

Table of Contents quick.link

(observe the financial statements) at any time? If so, perhaps this individual has "read-only" access.

So, there's a lot to contemplate within this *one* sector of your information controls environment. It's a lot of work to dissect the accounting controls environment, especially in the initial stages of a business (to which we have just tipped the iceberg, above).

So, when getting their hands on the new accounting software, a lot of firm principals tend to hypothesize:

"Well, Jenny *could* need to cut checks if I'm on vacation?"

"What happens if *FINRA* calls without notice, and needs some balance sheets & income statements? Well, I do want Frank to *be able* to close-out Retained Earnings for the end of last year, to reset it for the current year. That would look kind of bad if we hadn't done that."

- Rather than take the time to craft reasonable, yet also efficient controls, around these questions, the simple solution unfortunately chosen by a lot of firms is to just give all of their accountants full access to all of the functions pointed out, above.

And, what are the *risks* of providing such wide-range access?:

- Embezzlement
- Compromising sensitive employee-specific data, such as compensation.
- Financial misstatements recorded by an individual in an area(s) of the general ledger, which he/she doesn't even need to have access.
- Regulatory citations and/or fines in the area of Financial Accounting Controls.

A financial firm needs to assess the various access rights & controls versus the risks associated with both *providing rights* & *restricting rights* across every area of its information system.

Depending on the size of the firm, the *CISO*[8] may wish to appoint an *Information Manager* in each primary sector of the business, such as (for example):

- Finance
- Information Systems
- Compliance
- Trading
- Operations
- Asset Management

Table of Contents quick.link

When an employee, representative, or adviser has a question or concern about the handling of specific data or information workflows, the Information Manager can be utilized as a point of contact.

V. Data Loss Prevention:

Ports are the areas of entry and egress within your firm's information environment. For a financial firm, ports exist in some of the following places:

- E-Mail
- Instant messaging
- Custodial Investments platform (where the customer positions & account statements can be accessed)
- Trading platforms (whether proprietary or introduced[3])
- Order management systems
- Portfolio management platforms
- Exchange interfacing platforms[10]
- Client resource database systems[11] (which can also be used to transmit e-mails)

Protecting your firm's ports is essential to maintaining a cyber-secure information environment. *Network sweeps*[12] should be routinely conducted in order to evaluate for port vulnerabilities. And, the firm needs to implement a documentary process which specifies:

- Who *initiates* the sweeps - *CISO*, *Information Managers* reporting to the *CISO*, outside IT vendor
    - Some IT consultants can deploy programs that routinely conduct sweeps.

- Who *reviews* the sweeps? When firms leave this part to the IT vendor, the results can expose the business to varying elements of risk. What happens, for example, if the IT vendor fails to properly distinguish between *customers* and *third-parties*? If the sweep illustrates that a *customer* port is open to *third-parties*, but doesn't possess the business knowledge to differentiate between the 2 populations, the firm (by outsourcing this review phase) may be compromising information.

- Who *resolves* port vulnerabilities detected through the sweeps?

- What is the *documentation* (and method of *storage* for such documentation) that evidences the sweep results & describes the resolution of vulnerabilities?

[10] Some firms make some securities transactions through separate relationships/agreements with specific exchanges (i.e. BATS, DirectEdge, CBOE, etc.)

[11] Including *Microsoft CRM*, *Oracle*, *SAP*, *SalesForce*, and others

[12] Also discussed in *Section IX – Incident Response Procedures*.

Table of Contents quick.link

If you don't maintain a record of the sweeps conducted, the vulnerabilities detected, and changing status of such vulnerabilities; you may as well not conduct the sweeps at all.

If you cannot articulately demonstrate your proactive system for preventing data loss, and produce results attesting to its effectiveness, the *OCIE Initiative* provides the SEC and/or FINRA with guidance to suggest that your firm may not be adequately preventing data loss.

VI. Vendor Management:

Most financial firms use vendors to help facilitate their business operations. It's usually too difficult, with all of the fiduciary and regulatory responsibilities, for investments companies to meet all of their responsibilities entirely on their own. So, vendors are part of the business; however, controlling & monitoring the levels of access your firm provides to vendors is critical in order to remain cyber compliant.

Surprisingly, the levels of access provided to IT vendors are often better controlled than those shared with vendors in the other service sectors. That, however, is logical; a firm is already cautious about opening up its information environment to an outside party, which specializes in *information* and its underlying security. Therefore, the safeguards tend to be raised when forming those arrangements. But, vendors in other service sectors tend of have a way of lulling financial firms (primarily unintentionally) under potentially false notions of assumed security. For example, let's say your firm provides *Consolidated Customer Account Statements*[13] to some percentage of your investors. There are a large number of vendors providing that service for broker-dealers and investment advisers – *Allbridge* being a leader in the industry.

The least amount of risk involved in publishing *Consolidated Customer Account Statements* for your investors is when all of the sources of such investments (or custodians of the underlying securities) fall under your firm. For instance, an investor may have direct mutual funds purchased from a registered representative at your broker-dealer, equities held in an introduced *Pershing* clearing account through your broker-dealer, and alternative investments (i.e. let's just say REITs, for this purpose) held in an investment advisory account, managed by a registered investment advisor either directly affiliated or dually-registered with your broker-dealer.

---

[13] *Consolidated Customer Account Statements* consolidate the identity and market value of various investments, held at various financial institutions, onto one published report, disclosing the custodians, etc. However, *Consolidated Customer Account Statements* serve as an illustrative reporting tool for investors, and do not substitute for an actual Account Statement, published by the financial institution holding the security(ies) and distributed to the customer.

Table of Contents quick.link

The scenario is that all of these securities being reported on the *Consolidated Account Statement*[12] fall under the umbrella of your financial firm. All of the registered individuals (whether broker-dealer-licensed or registered as investment advisers) fall under the supervisory purview of your firm. You can produce records (i.e. customer statements, trade confirmations, order tickets) to document the activity or value pertaining to any of those securities or associated transactions.

The more prevalent risk occurs when the investor is working with more than one financial institution (yours and others). The investor has signed permissions between your firm and the other institutions for electronic securities data feeds to be transmitted from the outside institutions to your firm, through the *Allbridge* (for example) platform. It's not too difficult to envision the potentially cascading fiduciary, market-sensitive, and regulatory headaches associated with this type of arrangement.

Let's just go over a few of these headaches:

1. The outside financial institutions have attested (through their written agreements) that they stand behind the position totals and market values stated within their feeds; but now your firm has to make sure that those underlying balances are accurately reported on the *Consolidated Account Statements*, which your firm will provide to the customers.

    - *Consolidated Account Statements* are typically reported as of a month-end or quarter-end (similar to a traditional custodial account statement); so now your Operations team needs to reconcile the data within the *Allbridge* (example) platform (collected from the data feeds) with the amounts that the platform is queued to print onto the *Consolidated Statements*.

    - The controls developed to supervise such functions in a compliant fashion, while also safeguarding the clients' information, is called ***Vendor Management***.

2. Some of your clients may like to receive their *Consolidated Statements* by mail, but since such Statements are more a sophisticated tool, there is a strong likelihood that these customers would prefer, at least minimally[14], to access this report via an encrypted e-mail (another service that these *Consolidated Statement* vendors provide).

    - So, now you have customers opening *Consolidated Account Statements*[12] in the comfort of their own homes[9], statements that contain securities information in no way associated with your financial firm or its representatives/advisers, statements that were distributed by a vendor.

[14] Several *Consolidated Account Statement* customers are also able to access their reports through mobile devices.

Table of Contents quick.link

- The controls developed to supervise such functions in a compliant fashion, while also safeguarding the clients' information, is called ***Vendor Management***.

- While it's acceptable that *Allbridge* (for example) is sending out the encrypted e-mails under the direction of your firm, you need to be concerned with the content of the encrypted data (the *Consolidated Statement*) that is being transmitted with such e-mails.

- Now, we cross back to *17a-4*[4]. That's fine that each investor is going to click a hyperlink in an e-mail from the vendor, and then most likely have to enter a password to open his/her *Consolidated Statement*, but does your firm have a copy of that exact report being viewed? You should, because that copy is a business book/record (an electronic record), which are required to be stored, under *SEA 17a-4*.

Consolidated Customer Account Statements are a specialized tool used by some investments firms (possibly not yours), but the chances are strong that your firm has *some* vendor relationship(s) which result in *similar* issues. ***Vendor Management*** is the cybersecurity area that controls and mitigates, under the direction of the *CISO* and any subordinate Information Managers, the overall risk of sharing customer information with outside parties.

Table of Contents quick.link

VII. Employee Training

A *WISP*[2] is designed to be complex, workflow-oriented, and task-specific – an illustration of a financial firm's information environment and the controls required to protect it from internal and external threats. Therefore, all new employees should be trained upon inception with your firm, and all other employees should be updated[15] with the current *WISP*[2] annually.

> To the extent your firm has various, segmented departments, it is advisable to conduct separate, department-specific cyber trainings, minimally, every few years[16].

Broker-dealers are required to conduct an Annual Firm Element training for all associated persons. The annual cyber training on the *WISP* could be used as a Firm Element training, although it would most likely not be viewed as reasonable by the regulators to overlap these two forms of training more than every few years.

The annual training on the *WISP* is the *CISO*'s[8] opportunity to verbally communicate, with the medium for questions & answers, the dynamics of the *WISP*, and to articulate each employee's (department's) role and responsibilities within the firm's information environment. However, while this training session may only occur annually, the *CISO* should also ensure that written (and/or electronic) communications (*WISP* updates, cyber procedural changes) are consistently provided to employees throughout the year.

To the extent that vendors and/or third-parties access customer data within your firm's information environment, your employees must be properly trained to understand the range of access and limitations to information held by each vendor and/or third-party. Such employee training, if applicable, should be incorporated within your firm's annual cybersecurity training session(s).

And, of course, to the extent vendors play an active role within your firm's information environment, such vendors must also be trained on your cybersecurity controls and procedures.

---

[15] Your firm needs to *document* the content of the *WISP* Training (preferably delivered annually), including attendance and dates of training. These records will be necessary to demonstrate to the *SEC* (and/or *FINRA*) that your employees have received adequate cybersecurity training.

[16] If applicable, in the years of separate, department-specific cyber trainings, such trainings could be conducted in lieu of an overall firm-wide training session.

Table of Contents quick.link

VIII. Vendor Training:

Just as a firm's employees must be trained on the workflows of its *WISP*[2], so must vendors[17] also learn and comply with the policies & procedures of the information environment, data, and systems. Vendors need to know how to interact with and handle firm data (both customer and proprietary) that crosses their paths.

Vendor training on the *WISP* can be handled a few different ways:

- On a case-by-case basis (preferably when onboarding a new vendor)
- Periodically, every few years. If vendors share similar data interaction, the firm could train more than one vendor simultaneously.
- Vendors could be trained remotely; because they are not employees of the firm, the *CISO* may find that it is not as productive to train these vendors in-person. Questions & answers could be handled either post-session, or could be facilitated in real-time through an on-line training forum (i.e. webex, for example).

The *CISO*[8] should also maintain active records of all vendors who access any type of the firm's business information (customer-related or otherwise). When a vendor change, addition, or termination occurs, such records should be amended accordingly.

[17] Not all vendors receive access to a firm's business and/or customer data. If that is the case, these vendors do not need to be trained on the firm's *WISP*, unless of course the vendor mandates such training.

Table of Contents quick.link

IX. Incident Response Procedures:

Network sweeps[11] (introduced in *Section V – Data Loss Prevention*) will identify *incidents*[18] - events in which the firm's information controls environment has been compromised in some way. The incidents vary, and can be measured across the following characteristics:

- Severity:
    - How *severe* is the incident?
        - Was data stolen by a hacker?
        - Or, did you detect that one employee used another employee's LogIn or Password to do a job, for which the first employee was responsible anyway?

Obviously, these two examples, above, range from Most Severe to Least Severe.

Your firm (and *CISO*[8]) can choose to measure severity using a variety of metrics. Perhaps your range of measurement is as simple as 1 (least severe) to 10 (most severe). Or, maybe your organization is too complex to use a simple 1-to-10 scale[19].

Or, perhaps you need to score the severity level on a percentage basis, either assessed versus the Overall Information Environment (of which 100% would represent the total inability to use the firm's Information Systems, which has been disabled due to the incident) or versus a Departmental Information Environment (of which 100% would represent an entire department's system becoming disabled).

Regardless of how your *CISO* and firm decide to measure *incident severity*, it is advisable that your metrics are simple, easy to understand, and easy to assign, whether by an individual(s) or system-generated.

[18] In this world of constant electronic communications, all financial firms experience cybersecurity *incidents*. It's just a matter of whether, and to what extent, such incidents are being identified. The incidents vary in levels of severity, sensitivity, and overall risk; but cybersecurity incidents are occurring in the financial industry and others all the time.

[19] *1-to-10 Scale* or *10-point scale*

Table of Contents quick.link

- Sensitivity:

  - How sensitive was the information compromised? This may not be applicable, if no data was compromised; however in the event(s) that data was accessed or stolen, your firm needs to be able to measure the sensitivity of the contents of the information.
  - In *Section I – Customer Data*, we presented the following data categories:

PII	Personally Identifiable Information
NPPI	Non-Public Personal Information
RNPPI	Restricted Non-Public Personal Information

The table above merely distinguishes between the types of Data (important), but your firm also needs to add the *Level of Sensitivity* to those categories in order to properly evaluate the scope of an incident(s).

To measure the sensitivity of an incident, the firm should probably stick to either a 10-point scale[18] (as described in the Severity subsection) or a simple color-coding schematic[20].

So, examples of sensitivity categorization could be:

9-RNPPI
Yellow NPPI
Green PII – perhaps this customer is an executive at a publicly-traded company (information that is widely & readily available on a public basis)

- Overall Risk:

Your firm should combine the *sensitivity* of the data compromised with the *severity* of the information breach to derive the *Overall Risk* posed by a cybersecurity incident(s). The *Overall Risk* (usually represented by a Score) not only informs your firm of the historical risk incurred by the incident being analyzed, but also *forecasts* the risk that a similar incident poses to your firm's or department's information environment in the near future.

[20] It is advisable that color-coding schematics also remain simple. Perhaps a 3-color schematic (Red-most sensitive, Yellow-sensitive, Green-not sensitive) or a 4-color framework (Red-most sensitive, Orange-moderately sensitive, Yellow-sensitive, Green-not sensitive) would be best communicated to your employees.

Table of Contents quick.link

- Response to Incidents:

  The *severity*, *sensitivity*, and *overall risk* calculated by historical incidents can provide your firm with vital data necessary to *respond* to future system and information breaches. However, your firm can have the most in-depth analytical results on past cyber incidents, but without a comprehensive, structured plan to effectively *respond* to such incidents, your information environment remains at great vulnerability.

  The questions (all to be answered by your *WISP*[2]) are pointed and direct, and intentionally so:

  1. Who responds?
  2. What is the system of incident response?
  3. Does the response differ by *severity*, *sensitivity*, and *overall risk*? Regulators would expect this.
  4. How do responses get *documented*?
  5. If there is an employee, vendor, or third-party in some way *involved* in the incident, or did that individual, either intentionally or unintentionally, in some way(s) *contribute* to the incident occurring?
     - If so, does that employee, vendor, or third-party get *notified* of the incident, and, if no fault, does that individual *receive guidance* on how to avoid a future, similar incident?
  6. What is the firm's policy for notifying a customer(s) of a cybersecurity breach that materially compromised *NPPI* or *RNPPI*?
  7. Depending on the customer information compromised, what steps and procedures are taken by the firm to *resolve* the incident(s)?
     - Who, from the firm's side, is involved in these resolutions?
     - What resolution actions are taken?
     - How do customers react to such resolution steps? Are they satisfied/dissatisfied?

The key aspect to Incident Response is the *timing*. How quickly is your firm and its employees able to respond to cybersecurity incidents? A comprehensive and well communicated *Incident Response Plan* in your *WISP* should result in efficient deployment of solutions. If your Incident Responses are slow, customers will lose faith and trust, and regulators will be concerned.

Table of Contents quick.link

Costs of Breaches:

What are the potential *costs* associated with cybersecurity breaches?

States and insurance providers collectively estimate the cost of each compromised personal record at $100 - $300.

So, you do the math:

Say a breach (detected or undetected) of your firm's information environment leads to 100 personal records being compromised:

Personal Records Compromised	**Fine/Cost** per Breach	Total Fines/Costs
100	$ 200	$ 20,000

Well, that's not so bad, right? Well, but then, you agree to provide 3 years of subsequent *credit monitoring* for each customer; because you want to retain these 100 clients, right? The major credit bureaus and monitoring services are reaching fairly estimable economies of scale; so, we will use the number $240 per account compromised as the annual cost of providing credit monitoring services to one customer.

Yrs of Credit Monitoring Service Provided	Personal Records Compromised	Annual Cost of Credit Monitoring	Total Credit Monitoring Costs
3	100	$ 240	$ 72,000

Okay, so know you're pushing $100,000 in cybersecurity incident (or breach) costs; and we haven't even contemplated any legal and/or public accounting implications –

Fines/Costs Incidents/Breaches	**Fine/Cost** per Breach	Total Fines/Costs
$ 20,000	$ 72,000	$ 92,000

Let's also surmise that your firm may have not been encrypting, or properly encrypting, its e-mails to and from customers up to the point when the incidents were detected. The regulators/states could just give your firm a sharp citation in their cybersecurity examination report, or they could opt to levy a fine, significant or modest.

Table of Contents quick.link

X. Independent Cybersecurity Assessment:

In *Section III – Risk Governance/WISP*, it was noted that the *WISP*[2] needs to be periodically tested to ensure that it continues to safeguard the firm's proprietary and customer information. While that is true and important, there is no substitute for an *Independent Cybersecurity Assessment* of your firm's *WISP*, actual information environment in real-time, and current data flows.

The *9/15/2015 SEC OCIE Cybersecurity Initiative*[1] point on *Governance and Risk Assessment* highlights the need for independent evaluation of an investments company's information systems by stating:

> "Examiners may assess whether registrants have cybersecurity governance and risk assessment processes relative to the key areas of focus discussed below[21]. Examiners also may assess whether firms are periodically evaluating cybersecurity risks and whether their controls and risk assessment processes are tailored to their business. …"

So, if *SEC* (and/or *FINRA*) examiners are going to evaluate your firm's information systems environment, its controls, and safeguards, why would you *not* want a regulatory consultant to evaluate your cybersecurity status beforehand?!

How often should your firm receive an independent cybersecurity assessment? As is often in the regulatory viewpoint, you need to determine what frequency is *reasonable*.

Does your adviser have $1 billion in AUM?
You should probably arrange for an independent assessment annually.

Does your broker-dealer specialize in high-frequency trading?
Once again, you should probably be on an annual assessment cycle.

We typically observe that most broker-dealers and investment advisers should receive an independent cybersecurity assessment every *few* years. A key indicator on this frequency could correlate with your firm's regulatory examination cycle. The regulatory authorities are requesting Executive Management Summary reports, which document the findings and/or recommendations drawn from cybersecurity assessments. And, an independent assessment (like a financial audit) engenders a degree of risk governance and internal control analysis that cannot be matched from a proprietary basis.

---

[21] *Access Rights and Controls, Data Loss Prevention, Vendor Management, Training, Incident Response*

Table of Contents quick.link

A lot of financial firms are engaging consultants in beneficial *Cybersecurity Pre-Assessments* to assist in the review and/or development of the *WISP* (as articulated in this instructional document). A ***Pre-Assessment***, a service fully offered by **Intersource** is an in-depth, concentrated review of your firm's Systems Controls Environment & Interface(s).

Intersource Consulting Group LLC believes in open, active, and constructive communication with your firm's *CISO*, *CISO designees*, and any *outside IT vendors* to conduct our **comprehensive *Pre-Assessments***, which address & ***independently report upon*** the following *SEC OCIE Cybersecurity Initiative*[1] components:

- Governance and Risk Assessment
- Access Rights and Controls
- Data Loss Prevention controls
- Vendor Management controls
- Training program(s)
- Incident Response execution planning

However, we would be amiss to not disclose that a ***Full Independent Cybersecurity Assessment*** needs to ***test & evaluate*** the aforementioned key points of the *OCIE Initiative*[1] (to also include an evaluation of a firm's Penetration Testing controls).

Intersource Consulting Group LLC has business contacts (high-level technology & information security companies, prevalent in the financial services sector) whom conduct ***Full Independent Cybersecurity Assessments*** of firms like yours – broker-dealers, investment advisers, and dual broker-dealer/investment advisory firms. Such *Independent Cybersecurity Assessment* are comprehensive, and in addition to addressing the aforementioned *OCIE Initiative*[1] points, can also provide an assortment or full set of the following services:

- Internal Controls & Inherent Risks Review
- Vulnerabilities Scanning of Information Environment
- Incident Response Evaluation
- Executive Management Summary (to meet regulatory requests), which outlines findings and recommendations

Nowadays, cybersecurity assessments can often be conducted remotely, with as little intervention and business disruption as possible. Please be sure that your selected *Independent Assessment* vendor utilizes secure data transmission means to protect your business & customer information at all times.

Please feel free to reach out to us with any cybersecurity questions.

Thank you!

Ernie Kappotis
Ernie D. Kappotis
CFO – **Intersource Consulting Group LLC**
978-335-7015
ekappotis@intersourcecg.com

Table of Contents quick.link

XI. *Glossary of Terms*:

1. *SEC OCIE Cybersecurity Examination Initiative* from September 15, 2015 or 9/15/2015, or *OCIE Initiative* or *Cyber Initiative* or *Initiative* – all refer to the:
   SEC OCIE Cybersecurity Examination Initiative from September 15, 2015

2. *WISP* – Written Information Security Policies & Procedures

3. *PII* – Personally Identifiable Information

4. *NPPI* – Non-Public Personal Information

5. *RNPPI* – Restricted Non-Public Personal Information

6. *CISO* – Chief Information Security Officer

7. *Information Managers* – department-specific employees charged with executing the *WISP*, under the direction of the *CISO*

8. *Consolidated Customer Account Statements* or *Customer Account Statements* – statements that consolidate the identity and market value of various investments, held at various financial institutions, onto one published report, disclosing the custodians, etc. However, *Consolidated Customer Account Statements* serve as an illustrative reporting tool for investors, and do not substitute for an actual Customer Account Statement, published by the financial institution holding the security(ies) and distributed to the customer.

9. *Port* – any location, mechanism or means of entry or egress (exit) through with data can flow either into or from your firm's information environment

10. *Cybersecurity Incident(s)* – an occurrence(s) in which the financial firm's information controls environment is penetrated, or in which information is compromised (due to either intentional or unintentional efforts) due to a failure to follow established controls

Table of Contents quick.link