# Analysis of FINRA 2017 Exam Findings and 2018 Exam Priorities

Our observations about FINRA's 2017 Exam Findings, 2018 Priorities, and their potential relevance for Broker-Dealers.

white paper

workplace by OS33

## Introduction

Like many firms, part of our annual cycle at OS33 involves assessing the successes of the past year and planning for the next with an emphasis on a few key areas. In 2018, we will be laser-focused on helping our wealth management clients — Registered Investment Advisers, Broker-dealers and others — meet their information security and compliance objectives by offering industry-leading software and services.

An important driver for assessing our goals and anticipating those of our clients are the FINRA Examination Findings and Exam Priorities published each year, which provide tangible insights into issues that are top of mind for regulators, and signal their intentions for the year ahead. The reports assist us in aligning our understanding of critical risks for our clients and, confirming that Workplace by OS33's product roadmaps meet regulatory expectations.

There was no shortage of headline-grabbing cyber-related events in 2017: leaks from Equifax, Verizon and Deloitte as well as the WannaCry ransomware attack. It is clear from reading these FINRA missives that cybersecurity and technology risks continue to consume the financial services community. Cybersecurity is essentially a standing item on FINRA's annual examination roadmap, and its inclusion again in 2018 further solidifies this conclusion.

What follows are our observations about FINRA's 2017 Exam Findings, 2018 Priorities, and their potential relevance for Broker-dealers with a few touchpoints on Workplace by OS33's capabilities throughout.

## 2017 Report on FINRA Examination Findings

The 2017 FINRA Examination Findings provide a thematic view of risk issues that challenged firms based on their frequency and potential impact on investors and markets. At a high level, FINRA noted that firms are dedicating increasing resources —financial capital and personnel—toward mitigating cyber risk.

Specifically, FINRA observed deeper engagement from senior management in risk assessment processes as well as the procurement of technology solutions for dataloss prevention, suspicious network activity and event management. The regulator noted that firms have been devoting more time and effort to compliance activities — policies, procedures, training and testing — to ensure that employees are educated about cybersecurity and can adequately identify potential threats. Given escalating phishing and spear-phishing risks triggered through channels like email and instant messaging, it is essential for employees to be aware of these threats.

FINRA discussed specific areas where firms can improve their cyberrisk practices, many of which can be supplemented and addressed with enhanced technology controls.

### Access Management

Firms must have full transparency into how and when employees access IT systems, and maintain robust protocols to terminate access for departing employees in a timely manner.

Many Broker-dealers provide a myriad of applications to their employees and their representatives. However, they often do not have the systems to understand user activity in these applications, or they have too many siloed systems to effectively correlate them.

New technologies are available to Broker-dealers that aggregate the entire portfolio of applications they publish. These tools allow firms to keep a unified activity log that correlates not only the activity of a user but also to the device used to access each application. Unusual behavior patterns should trigger immediate alerts to the security and compliance team.

2018 will also usher in a new category of software known as "Secure Isolated Browsers". This software utilizes purpose-built browsers to publish applications that can isolate the applications from their rest of the user's systems. Browser sessions are safe from malware attacks on local machines, and local machines are protected from malicious code attacks injected into the application. The browser is itself virtual and non-persistent — content such as cached passwords get destroyed after each browser session. This feature is particularly important with respect to the latest Meltdown and Spectre vulnerabilities. Secure browsers can audit when a user copies and pastes information in or out of the browser, and can also log print requests.

At OS33, we have enhanced our Workplace platform to log application activity, device activity, as well as file activity. Broker-dealers who utilize Workplace can drill down to exactly when a file was modified, moved, deleted, downloaded or shared. We've incorporated session recording into our Secure Isolated Browsers to protect our Broker-dealer clients. We have plans to take this technology a step further and record user activity when they visit ultra-sensitive areas of web applications. These recordings will be available in the activity log, so security and compliance administrators have a complete audit trail of all sensitive activity in a user's session.

## Data Loss Prevention

FINRA noted that while large and medium-sized firms employ technical controls to prevent data leakage and file transfer risks, additional efforts are required. Although not explicitly discussed, smaller firms may be lagging behind their larger competitors in this area, and should dedicate resources toward implementing and improving data loss prevention solutions.

This is another great example of how the Secure Isolated Browser will help Brokerdealers. By publishing firm applications via these tools to employees and representatives, firms can effectively block and log all activity pertaining to data removal from the system. We find this flexibility to offer a great compromise for end users. End users require the ability to manipulate data on their local computers to provide their clients with the best data sets. Firms should be able to offer this by first making sure the endpoint is safe and then systemically deciding if an endpoint can download, copy, or print the data set. All this activity should be logged. Suspicious activity such as the removal of large data sets should alert compliance teams immediately. Workplace has had some of these features for many years now and we are fully invested in expanding these capabilities in 2018 and beyond.

## Branch Offices

FINRA discussed a range of information security issues as they pertain to the operation of branch offices — from password management and application security patching to data encryption and control of removable devices like USB sticks. The implications of the branch office recommendations are significant as they could impact a diverse range of firm policies and processes, including management of IT assets, acceptable use of electronic communication systems, and maintenance of hardware inventories.

This finding comes as no surprise. While firms spend huge portions of their budgets on securing internal systems and employees residing at headquarters, branch offices have not received the same levels of attention. This is especially true of the branch offices run by independent representatives.

Beginning this year, Workplace will be able to drive policy-based access based on the findings of an endpoint scan. While it is useful to audit and alert on the security compliance of devices, we have found that altering access and possibly denying access to applications based on the results of an endpoint scan results in enhanced security. Users should be forced to protect their devices to continue to manipulate sensitive client information.

As part of this enhanced device security, firms will be able to scan their representatives' workstations and devices to build an accurate asset inventory. The application will build compliance reports and alert the appropriate teams when devices go out of compliance. This scanning technology will be a tremendous step in extending enterprise-class security to the small and medium-sized business run by independent representatives.

In addition to the three areas above, FINRA also observed that firms should continue to refine cybersecurity practices around risk assessments, vendor management and segregation of duties.

## 2018 Examination Priorities

On January 8, 2018, FINRA released its Regulatory Examination and Priorities Letter outlining its focus areas for the coming year. As discussed above, cybersecurity has effectively become a standing agenda item in the letter and is an obvious preoccupation for FINRA. We are highlighting three technology priorities from the letter is this update — business continuity planning, technology governance, and cybersecurity.

Regulated entities of all shapes and sizes must develop Business Continuity Planning ("BCP") policies and procedures. FINRA flagged BCP as a key focus for 2018, noting recent events like Hurricanes Harvey and Maria as reinforcing the need for firms to be able to manage operations during disruptive periods. In the first few weeks of January alone, we've already had to navigate a significant winter storm event — the frighteningly named "bomb cyclone" — which likely required firms to deploy resiliency frameworks.

In 2018, FINRA will be reviewing the entire lifecycle of firms' BCP activity. Firms may be examined on planning-related activities such as how they classify data and systems to ensure that business critical information is accessible during a BCP event. FINRA may also focus on processes for transitioning to backup systems during BCP events, or how firms coordinate with third parties to ensure that business activities can continue during disruptions. BCP may already be a critical concern for those firms subject to the FFIEC's Appendix J regime, and FINRA's focus on the issue demonstrates the importance of BCP across financial services.

While many firms have some form of BCP or Disaster Recovery in place by implementing replication technologies and secondary data centers, there are a fair number of firms still relying on local backups or removable USB devices as their "BCP plan." Given the costs of these replication technologies has shrunk, one would expect to see FINRA and the SEC crack-down on firms with inadequate technologies.

Workplace provides its clients with a mission-critical dual site backup configuration. Workplace frequently tests these capabilities with automated systems and provides documentation to its clients for compliance purposes.

FINRA emphasized technology governance as another key risk for 2018, explaining that firms should be mindful of how they manage system enhancements and modifications to prevent downstream disruptions. Firms also need to be aware of IT changes to ensure that they do not inadvertently surface

system vulnerabilities, or permit broad access to sensitive information. Firms must maintain protocols to oversee the maintenance of, and changes to, their IT systems to meet FINRA's expectations.

To support technology governance, many firms have turned to outsourced providers who can utilize apply professional change management procedures as well documented snapshot and testing procedures.

Firms can implement software to produce reports that provide data for risk assessment and system audits. Workplace provides alerts so that company managers can proactively investigate suspicious activity while it is happening, rather than analyze event logs after an event occurs. Workplace provides firm executives with easy-to-understand insight into user accounts, entitlements, file activity, and security events. Executives can easily audit user accounts to monitor application activity and security modifications.

The Priorities Letter includes a brief summary of cybersecurity, which refers to the 2017 Examinations Finding Report discussed above as a guidepost for further detail. It also includes a succinct statement that firms will be examined on the effectiveness of their cybersecurity programs, with a focus on how sensitive information is protected against internal and external threats. FINRA also reminds firms that they must have cyber-related policies and procedures in place and mechanisms for determining when SARs should be filed following a cyber event.

## Conclusion

Based on the 2017 Findings and 2018 Priorities, it is clear that FINRA is maintaining a persistent focus on cybersecurity, technology, and redundancy risks facing the financial services industry. We're confident that Workplace's product and long-term strategies are well aligned to help firms address FINRA's critical concerns.


EMAIL US
sales@os33.com

CALL US
800 646 0700

VISIT US
www.os33.com