

Compliance Is About More Than Paperwork, Cybersecurity is Taking Center Stage

Webinar: April 21 2016

Today's Webinar



Introductions



For CCOs: Broadening Compliance Remit



Understanding the Regulations



What Are the Tools Financial Firms Need



Q & A

About the Presenters



Jason Claycomb

Corporate Governance Officer

28 years in IT governance – Spanning
Retail & Commercial Banks, Exchanges,
Healthcare and Insurance



Justin Kapahi

Technical Director, Financial
Services Practice - External IT

14 years in Technology & Finance –
Former CTO and CEO in financial
industry

Broadening Compliance Remit

Two recent surveys of CCOs found:

- **50%** of Compliance professionals feel that their biggest challenge is the increasing responsibility for non-traditional compliance activities, such as information/cyber security or third-party vendor reviews.
- Cyber security ranks as the top priority in terms of future investments, as **32%** of compliance officers believe this will be a major focus in the near-term.

-Charles Schwab, *The Corporate Compliance Role: An Industry Survey from Compliance Solutions*, November 2015

- One particular area that is beginning to affect the compliance arena is technology, IT risk and the issues relating to cyber crime and to resilience. For firms, cyber risks are multi-faceted and must not simply be left to the IT function. Compliance functions need to be engaged in the consideration of risks to the business (and by association the potential effect on their customers)...

-Thomson Reuters, *Cost of Compliance 2015*

Evolution of Legal and Regulatory Framework

1990-2000

- ⦿ “Fiduciary duty”
- ⦿ Left to interpretation
- ⦿ 1996: Reg S-P (Privacy)

2001-present

- ⦿ 2001: SEC Electronic Media Guidance
- ⦿ 2003: SEC Compliance Program Rule
- ⦿ 2013: Reg S-ID Identify Theft
Red Flags Rules
- ⦿ 2014: SEC Alert
- ⦿ State privacy and data breach laws
- ⦿ 2015 OCIE Sweep Results
- ⦿ 2015 SEC Alert: 2nd Round of Examinations

1st Cybersecurity Examination Sweep Interesting Facts

- **51%** of advisors have written business continuity plans that address the impact of cyber-attacks or intrusions.
- **74%** of advisors and **88%** of broker dealers stated that they have experienced cyber-attacks.
- **43%** of advisors reported receiving fraudulent emails seeking to transfer client funds.
- **24%** of advisors incorporate their cyber-security requirements into their contracts with their vendors.
- Almost all advisors, **91%**, make use of encryption in some form.

September 2015 OCIE Risk Alert

- ✔ Securing client records and information
- ✔ Identifying and protecting against potential threats to client information
- ✔ Protecting against unauthorized use or access to client information
- ✔ Designing & implementing appropriate controls to protect client information
- ✔ Ensuring these controls are operating effectively and are reviewed and revised accordingly





Governance & Risk Assessment

- Firms must document policy, procedures and personnel responsible for cybersecurity
- Firms must design & implement appropriate controls
- Firms must ensure controls are operating effectively by conducting periodic risk assessments
- Senior management of firms must be involved in cybersecurity plans and policy of that firm

U.S. Securities and
Exchange Commission

[ABOUT](#)

[DIVISIONS](#)

[ENFORCEMENT](#)

[REGULATION](#)

[EDUCATION](#)

[FILINGS](#)

[PRESS RELEASE](#)

SEC Charges Investment Adviser With Failing to Adopt Proper Cybersecurity Policies and Procedures Prior To Breach

Access Rights & Controls

- Firms must have basic controls in place to prevent unauthorized access to systems or information
- Firms must restrict access to various systems and data through management of user credentials, authentication, and authorization methods, including remote access, customer logins and passwords
- Firms must have policies and procedures related to:
 - Access by unauthorized persons to firm network resources, including establishing, updating, terminating and changing such access;
 - Access to the firm's system externally, whether on firm-issued or personal devices, including encryption, monitoring and deactivation of such devices



Data Loss Prevention

- Firms must have procedures in place on how data is handled especially PII
- Firms must monitor data transferred outside the firm by employees or third parties
 - Monitor email attachments or uploads
 - Check for unauthorized data transfer
 - Multi Factor Client Verification



Vendor Management

- Firms must always examine a vendor's SSAE-16 report to make sure their control objectives align with your firms'
- Firms must understand what data is at which service provider / third party administrator (TPA) / vendor / cloud provider
- Firms need to carefully manage credentials and access to all providers and use single-sign on/federation when possible
- Firms need to work with vendors to restrict access by location or system



Training

- The #1 threat is the uninformed employee
 - User awareness is the most important security measure that your company can implement.
 - An informed user behaves more responsibly when using the corporate system
 - Doesn't open suspicious attachments
 - Never tries to install software
 - Doesn't internet "surf" on the corporate computer
 - Uses mobile devices responsibly
 - Knows who to speak to about suspicious or unknown activity

Incident Response

- Firms must have an incident response plan for data breaches and cyberterrorism
 - Checklist
 - Procedures
- Firms must assess damage and risk and respond immediately
- Firms need to have cybersecurity insurance in place

From Our Security Assessments



Top areas where financial firms are not compliant:

1. Firms typically do not have a CSO. When they do they lack the necessary IT experience.
2. Firms lack any type of security awareness training.
3. Firms lack a formal incident response plan.
4. Firms do not have robust vendor cybersecurity assessment procedures.
5. Firms lack proactive auditing of IT and cybersecurity.
6. Firms' employees are often able to move company data to personal and home devices, with no accountability or tracking measures in place.
7. Firms tend to lack robust, immediate disaster recovery in case of emergency

What are the Tools Financial Firms Need?

- Effective Information Security Policy / Handbook
 - Users must understand what resources they have and how to use them safely
 - Items that you may not be able to solve technically can be greatly improved with policy
- User Access Checklists
- System Reviews
- Risk Assessments
- Security Awareness Training
 - Similar to Inside Trading Awareness
- Perform Analysis on your Vendors
 - Do you understand an SSAE-16 Report?

What are the Tools Financial Firms Need?

- File Archive with 7 year retention
- Email, Website, and Social Media Archive
- Email Encryption and/or Secure File Sharing
 - Train your users to utilize this properly
- Expertly configured and monitored firewall and network
- Anti-Virus and Anti-Malware on servers, cloud services, desktops, and email
- Web Filtering
- Data Loss (Leakage) Protection
 - Mobile Device Management
 - Mobile Device Laptop / Encryption
 - DLP Systems
 - Remote Access Systems that can block downloading

Top 10 Questions to Ask Your SaaS Vendor

1. Where is client data stored? What type of facility?
2. Who has access to my clients' information?
3. Is this audited? How often? Can you see those audits?
4. What is your hiring process?
5. What kind of disaster recovery plan do you have in place?
6. What is your policy regarding notification if there is a breach?
7. What liability are you responsible for if there is a breach?
8. Have you had any breaches in the past? In the past 12 months?
9. Does your software have the ability to permission access to data by user?
10. Can the application permission who can download information?

Security & Compliance: Secure File Sharing

The screenshot shows the BASIS Wealth Management interface. A dialog box titled "How would you like to share?" is open, offering three sharing options:

- Share public link**: For non-critical documents. Pickup possible by any device.
- Share tracked link**: With SMS receipt notification. Pickup via any mobile phone.
- Share private link**: For secure sharing of sensitive documents. Pickup restricted by phone number.

The "Share tracked link" option is highlighted with a blue border. In the background, a file list is visible with columns for "File Size" and "Name".

This screenshot shows a file sharing interface for a PDF file named "Marketing PDF.pdf". Below the file name, there is a prompt: "Enter your unlock code:" followed by a series of input boxes for the code.

Secure File Sharing to Meet Financial Services Firms Compliance and Security Requirements

Security & Compliance: Logging & Reporting

Tracking user activity:

- Logins
- Logouts
- App Launches
- Files Opened
- Files Shared

The screenshot shows the BASIS Wealth Management interface. At the top left is the BASIS logo and 'Wealth Management'. At the top right, the user 'Robert' is logged in, with links for 'Help' and 'Log out'. Below the logo is a navigation menu for 'Robert's profile' with options: Profile, Activity, Change password, Devices and security, Web apps, OS33 Admin, > Activity, Web apps, and Theme. The main 'Activity' section has a search bar and a 'Pro-filter' button. The activity log shows a list of events for user 'Sam Attias' on Tuesday, 2015/07/21. The events include: 'Signed in' at 12:13:05 PM from New York, NY, US; 'Sign-in expired' at 7:10:22 PM from US; 'Signed out' at 11:09:11 AM from Miami, FL, US; 'Signed in' at 11:08:24 AM; 'Launched Excel 2013' at 9:10:11 AM from US; 'Launched Outlook 2013'; 'Changed internet provider (XO Communications)'; and 'Signed in' at 9:09:00 AM.

User	Activity	Time	Location
Sam Attias	Signed in	12:13:05 PM	New York, NY, US
Tuesday, 2015/07/21 7:00 PM			
Sam Attias	Sign-in expired	7:10:22 PM	US
Tuesday, 2015/07/21 11:00 AM			
Justin Kapahi	Signed out	11:09:11 AM	Miami, FL, US
	Signed in	11:08:24 AM	
Tuesday, 2015/07/21 9:00 AM			
Sam Attias	Launched Excel 2013	9:10:11 AM	US
	Launched Outlook 2013		
	Changed internet provider (XO Communications)		
	Signed in	9:09:00 AM	

Security & Compliance: End Validation

End Point Validation:



- Authorize by device
- Remotely Wipe Compromised Endpoints
- Inventory all access devices (SEC requirement)



The screenshot displays the BASIS Wealth Management interface. On the left, a navigation menu for 'Robert's profile' includes links for Profile, Activity, Change password, Devices and security (selected), Web apps, OS33 Admin, Activity, Web apps, and Theme. The main content area is titled 'Devices and security' and is divided into three sections: 'Connected devices', 'Connected apps', and 'Connected browsers'. Each section lists active devices or applications with their names, locations, and last activity times, along with 'Nearby' buttons and information icons.


Section	Item Name	Location	Last Activity	Action
Connected devices	OS33Laptop	New York, NY, US	4 minutes ago	Nearby
	iPhone 6	New York, NY, US	5 minutes ago	Nearby
	iPhone 6	New York, NY, US	18 minutes ago	Nearby
	OFFICE	New York, NY, US	42 minutes ago	Nearby
Connected apps	No app sessions.			
Connected browsers	Chrome	New York, NY, US	a few seconds ago	
	Chrome	New York, NY, US	3 minutes ago	
	IE	New York, NY, US	7 minutes ago	Nearby
	Firefox	New York, NY, US	12 minutes ago	


Facilitate company control & security



Activity 1/23/2016   Pro-filter

- Signed out
- Signed in 10:04:5
-  CSU Data Centers.pdf has been downloaded.
-  CSU Data Centers.pdf has been previewed.
- Signed in 5:10:1
- Signed out
- Signed in
- Signed out
- Signed in





 **Fri. Jan 22, 2016**
PM 05:10:12

Activity
Signed in

Location
New York, NY, US
[View location activity](#)

IP
65.126.142.6
[View IP activity](#)

[View session activity](#)



Logging & Reporting

For tracking user activity

- Logins
- Logouts
- App Launches
- Files Opened
- Files Shared

The screenshot displays the OS33 Activity page. At the top, there are filters for '09.09.2014+', 'All events', and 'All users'. A search bar and 'Export data' button are also present. The left sidebar contains navigation options: Settings (Profile, Activity, Devices & security), OS33 Admin (Company, Users, Groups, Activity, Usage, Servers, Web apps, Windows apps, SSO app admin, Theme), and a footer with 'Powered by OS33' and 'Serviced by External IT'.


The main activity list shows the following events:

Event	Date	Location
Alex's Mac logged into OS33 for Mac		
MyPC Installed 'OS33 for Mac'		
Alex's Mac logged out		
Alex's Mac launched 'Microsoft Word'		
Alex's Mac launched 'Microsoft Outlook'	10/1/2014	From New York, N
Alex logged in from Chrome	10/1/2014	From New York, NY, US.
Alex's Mac logged out	10/1/2014	From New York, NY, US.
Alex's Mac logged in via OS33 for Windows	10/1/2014	From New York, NY, US.
Link opened 'Marketing2013.ppt'	10/1/2014	Picked up by (917) 756-9575
You shared 'Marketing2013.ppt'	10/1/2014	From New York, N
Alex's Mac launched 'Microsoft Outlook'	10/1/2014	From New York, N
Connected Alex's iPhone to OS33	10/1/2014	From New York, N

Two pop-up windows provide details for specific events:

- Alex's Mac**
 - First connected: 123.123.12.1 at 13:58 on 2.12.2014
 - Last online: 127.33.98.1 at 11:58 2.12.2014 in New York
 - View device sessions
 - View all device activity
- Marketing2013.ppt**
 - Link created: From Alex's Mac (102.86.84.12) 12:58 p on 2.12.2014
 - Picked up by: (718) 112.1204 at 13:58 on 2.12.2014 (212) 113.9847 at 12:03 a 12.12.2014
 - View link in shared files
 - View all file activity

Enforcing local PC security



Your work. On-demand.

Your work email

Password

[Get help](#)

Security tips.

OS33 is designed to keep your work secure. Please take a minute to review your security settings so you stay safe online.

- ✓ Your machine is password protected
No action necessary
- ✓ Your screensaver is password protected
No action necessary
- ✓ Your screensaver activates after 5 minutes
No action necessary
- ✓ You are protected against malware and viruses
Virus protection installed

Security lock down.

OS33 is designed to keep your work secure. Please secure your computer with the settings below before installing OS33:

- ✗ Your machine is not password protected
[Set a password](#)
- ✗ Your screensaver requires a password
[Set a screensaver password](#)
- ✗ Your screensaver activates after 5 minutes
[Set screensaver lock](#)
- ✗ You are protected against malware and viruses
[Install virus protection](#)

Please complete the checklist above to continue.

Devices dashboard | Admin

OS33 Switch to classic OS33 Admin Help Log out

Settings

- Profile
- Activity
- Password
- Devices & security
- Web apps

OS33 Admin

- Company
- Users
- Groups
- Activity
- Usage
- Servers
- Web apps
- Windows apps
- SSO app admin
- Theme

> Devices

Devices

Access requests

12 requests passing security checks [Review requests](#)

5 requests failing security checks [Review requests](#)

All devices

318 Total

145 devices with security insights [Secure your network](#)

273 unknown devices

Security checks

101 of 101 users can log in without security checks. You can change these settings in the classic company admin section. [Secure your network](#)

✗ 241 Failed security checks
Computers with system access that failed at least one check [View devices](#)

✓ 54 Passed security checks
Computers with access that passed all security checks [View devices](#)

Device breakdown

Device Type	Count
Windows desktops	127
Windows laptops	70
iOS devices	50
Macs	45
Mac laptops	19
Android devices	12
Unknown devices	273

Q&A?

Thank you!

Jason Claycomb jclaycomb@os33.com

Justin Kapahi jkapahi@externalit.com