# 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



#### 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: 2<sup>nd</sup> 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



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

### **Solution** 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.

emergency

- 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

#### 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?

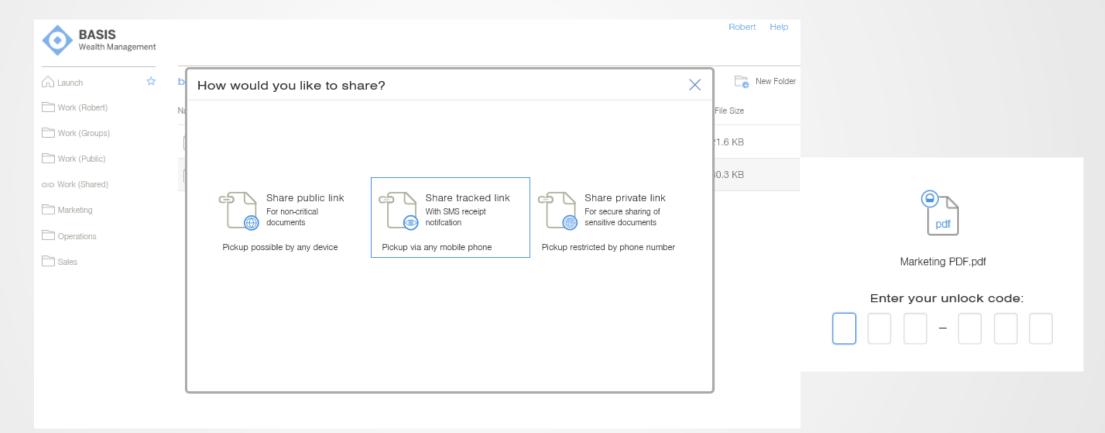
#### What are the Tools Financial Firms Need?

- 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

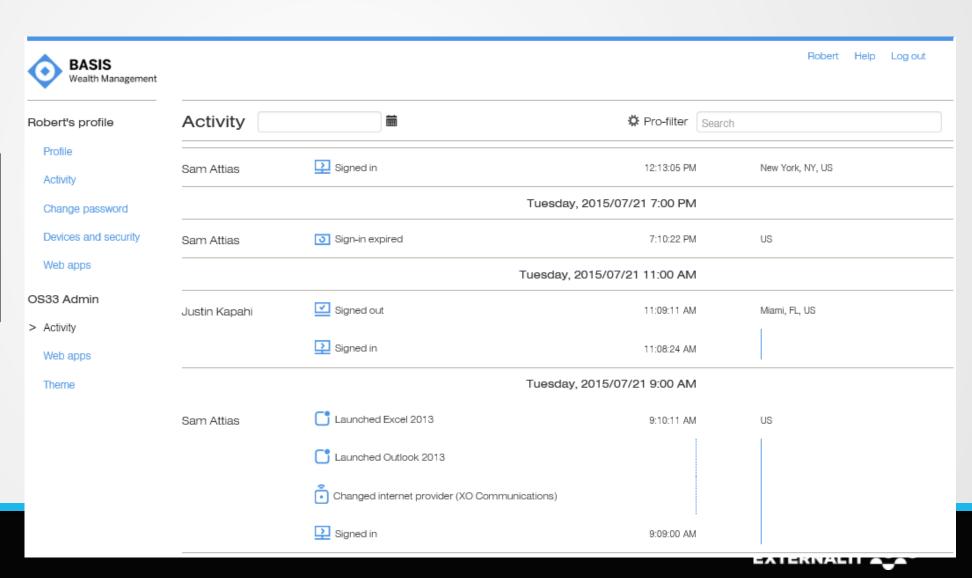


Secure File Sharing to Meet Financial Services Firms Compliance and Security Requirements

#### Security & Compliance: Logging & Reporting

#### Tracking user activity:

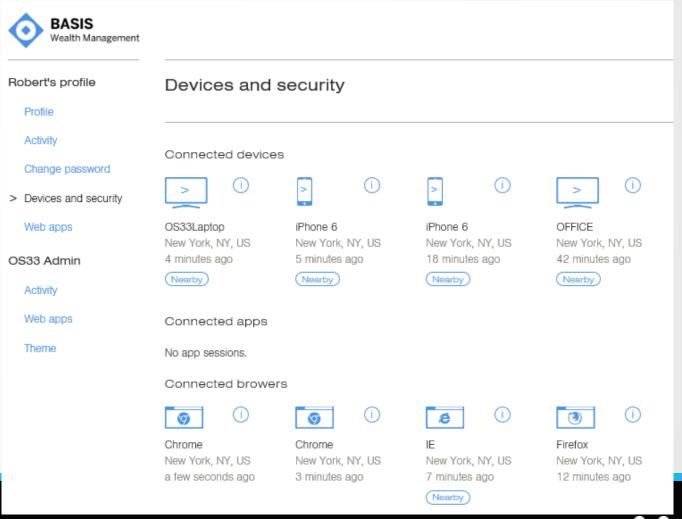
- Logins
- Logouts
- App Launches
- Files Opened
- Files Shared



#### Security & Compliance: End Validation

#### **End Point Validation:**

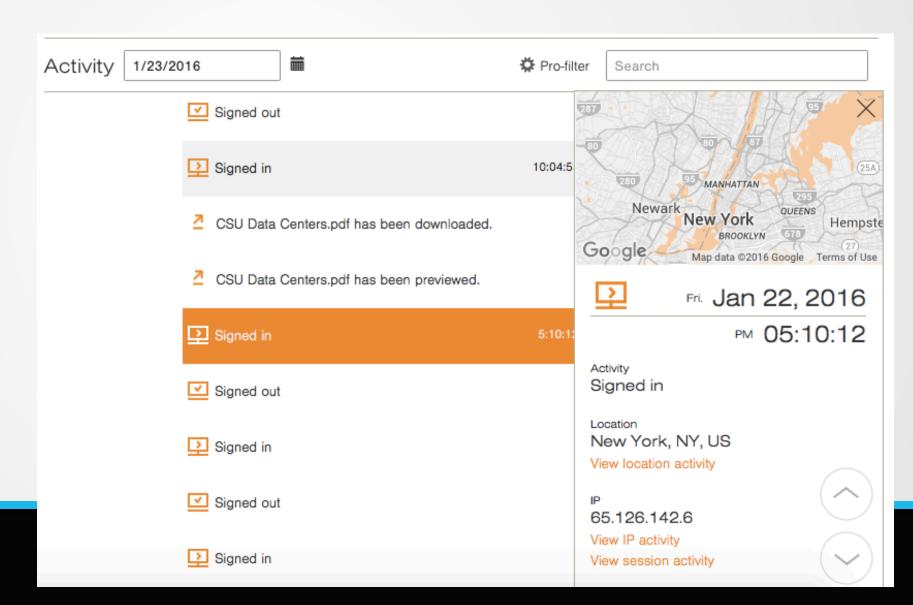
- Authorize by device
- Remotely Wipe Compromised Endpoints
- Inventory all access devices (SEC requirement)





## Facilitate company control & security

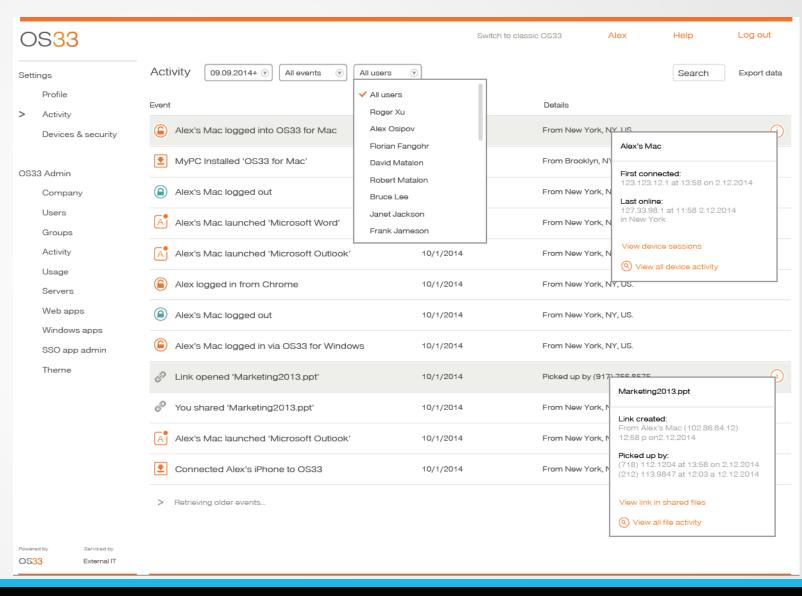




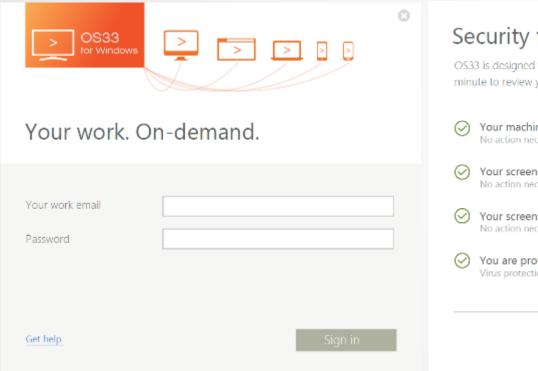
#### Logging & Reporting

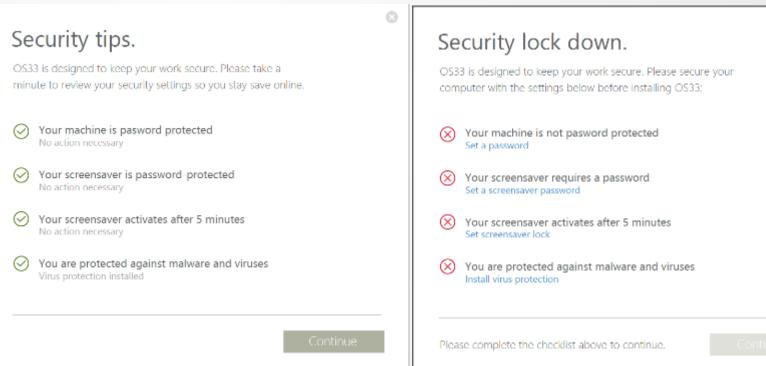
#### For tracking user activity

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

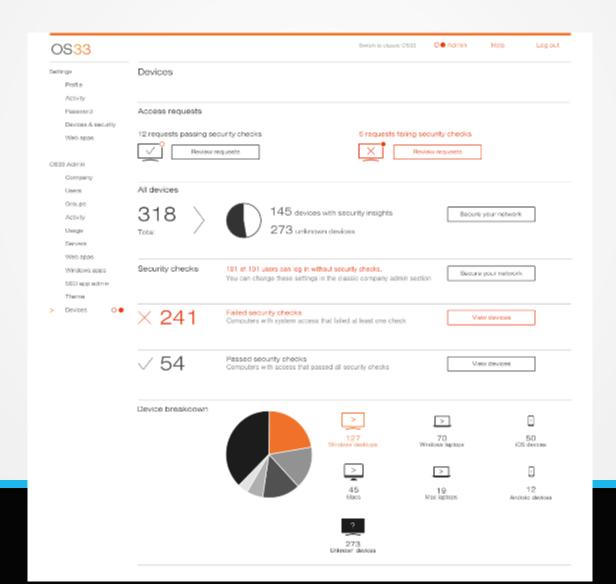


### Enforcing local PC security





# Devices dashboard | Admin





Jason Claycomb jclaycomb@os33.com Justin Kapahi jkapahi@externalit.com

