

# Financial Firms Face Further Scrutiny of their Cybersecurity Practices – Is Your Firm Ready?

*External IT's Observations from the Field*

Justin Kapahi – External IT

# About the Presenters



Justin  
Kapahi

Technical Director -  
Financial Services  
Practice

15 years in Technology &  
Finance - Former CTO and CEO  
in financial industry



Sam Attias

Managing Director

16 years of industry experience  
- Wealth Management, Investment  
Banking, Fixed Income, M&A

# Who Is External IT?

FOUNDED IN NYC, 2002



Focused on delivering solutions for advisors, broker-dealers and family offices

# 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
- ⦿ SEC Alert: 2<sup>nd</sup> Round of Examinations

# 1<sup>st</sup> 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.

# From Our Security Assessments

Top 3 areas where financial firms' cybersecurity is lacking:

1. Firms tend to lack an official security information security policy and proactive auditing of IT and IT security.
2. Firm's employees are often able to move company data to personal and home devices, with no accountability or tracking measures in place.
3. Firms tend to lack any kind of disaster recovery or business continuity plans in place in case of emergency.

# What Is Your Cybersecurity Obligation?

- Second Round of Cybersecurity Examinations will involve more testing to assess implementation of firms procedures and controls.

- Examination will focus on six areas:



Governance and Risk Assessment

Access Rights and Controls

Data Loss Prevention

Vendor Management

Training

Incident Response

# What does that really mean?

- 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





# What are the Tools Financial Firms Need?

- Effective Information Security Policy, User Access Checklists, System Reviews, Risk Assessments, and Security Awareness Training
- Expertly configured and monitored firewall and network
- File Archive with 7 year retention
- Email, Website, and Social Media Archive
- Anti-Virus and Anti-Malware on servers, cloud services, desktops, and email
- Web Filtering and Data Leakage Protection
- Email Encryption and Secure File Sharing
- A Disaster Recovery system with an RTO of less than 2 days (most of your systems such as Files and Email should never be down)
- Redundant Internet and Power (if in stand alone facility)

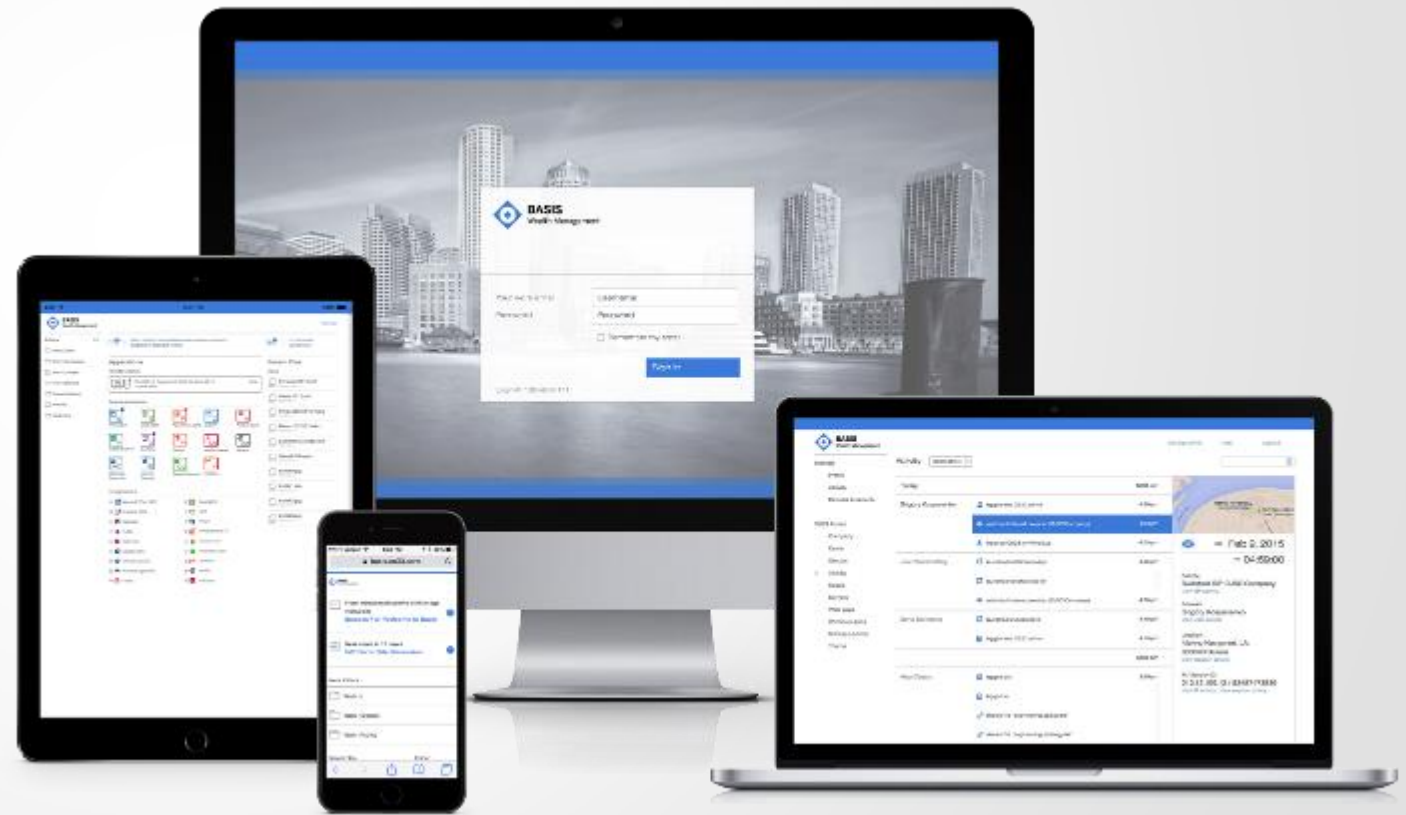
# Why Is All of This Important?



- You don't want your system to be down
  - You need to execute a timely trade
  - You need to service your clients
  - Your employees need to be able to work (finance employees typically highly paid)
- Your reputation and your business is at stake
  - You can get breached
  - You will lose clients and money
- SEC Audit Process
  - You don't want to be flagged and you don't want to be fined

# The Cloud Desktop Demo

- High security login & audit logging
- Branded & configured for Your Company
- One password to launch web + win apps securely
- Designed for every device
- Industry compliant & audit ready



# Q & A

Thank you!  
Any questions?

Justin      [jkapahi@externalit.com](mailto:jkapahi@externalit.com)

External IT Phone: 800.646.0700

