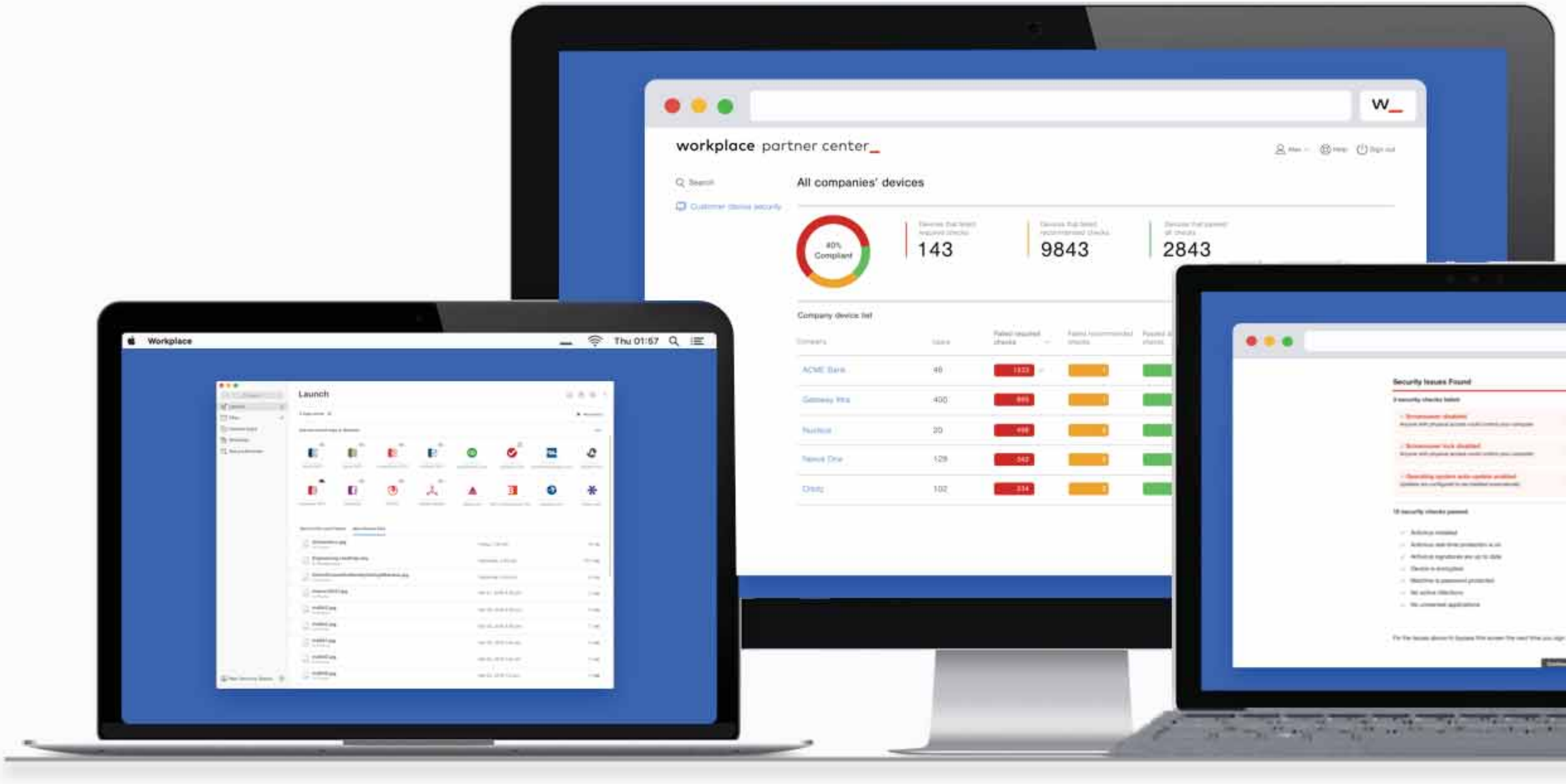
workplace_
by OS33

FINANCIAL SERVICES INSTITUTE
VOICE OF INDEPENDENT FINANCIAL SERVICES FIRMS AND INDEPENDENT FINANCIAL ADVISORS

FINRA 2018
Cybersecurity Best Practice



July 24, 2019

This document contains confidential information that is proprietary to Workplace by OS33.

Presented By

FINANCIAL ADVISOR
FA
KNOWLEDGE FOR THE SOPHISTICATED ADVISOR
July 2019 • www.fa-mag.com
Deglobalization Could Hit Equity Multiples
Globalization Has Coincided With Years Of High Stock Prices
Dealing With Clients' Cognitive Decline
Help Clients With A Team Approach
Cultivating Foreign Clients
How To Work With Them On Planning Challenges
2019 RIA SURVEY & RANKING
SWIMMING WITH THE SHARKS
After coming through a choppy 2018 with flying colors, the RIA industry is becoming a fast-consolidating food chain.

fa-mag.com

Speaker

Sam Attias

VP, Partnership Development

Workplace by OS33 is the leading SaaS platform enabling turnkey Compliance & Cybersecurity for Broker-Dealers, RIAs, and Insurance Companies that leverage independent representatives and advisors.

WHAT KEEPS YOU UP AT NIGHT

SUMMIT FINANCIAL	Lincoln Financial Group®	VOYA® FINANCIAL	LPL Financial + 11 other firms
Ground-breaking shift in BD responsibility of advisors' technology usage.	Failure to safeguard confidential customer data from foreign hackers.	Fined **$1M** for cybersecurity failures leading to the compromise of customer data.	12 BD firms fined a total of $**14.4M** for failure to store customer data in WORM compliant format.

FINRA 2019 Cybersecurity Report

5 sections to this report:

1. Branch Controls
2. Phishing
3. Insider Threats
4. Penetration Testing
5. Mobile Devices

STRENGTHEN YOUR BRANCH OFFICES

Most broker-dealers have developed Written Supervisory Procedures (WSPs) to define firm level cybersecurity controls, but how can branch offices and advisors be prepared too?

- Create a comprehensive set of minimum standards for the branch level
- Implement a review program - includes inspections and remote surveillance
- Asset Inventory:
  - List of required /recommended hardware & software vendors
- Technical Controls – passwords, encryption, wireless, AV/AM, MFA, IAM

UNMASK THE ATTACKS

Phishing attacks are one of the most common cybersecurity threats known to firms and attackers' disguises are becoming increasingly difficult to distinguish from legitimate communications. How do you keep employees informed?

- Develop policies and procedures to identify, delete, and notify designated staff of phishing incidents, ensure remediation after an attack
- Establish consequences and conduct remedial training for employees
- Log all phishing incidents and firm responses, and report incidents
- Data access conditional upon phish testing remediation?

PROTECT YOUR FIRM FROM INSIDE OUT

Insiders are those who have or have had access to the firm’s systems and data. This includes employees, consultants, **third-party vendors**, and more. Do you know what to look out for and how to stop it?

- Designate a senior executive or manager to be responsible for the firm’s insider threat controls
- Policies to automatically revoke network and system access
- Identity Access Mgmt. and comprehensive password policies (MFA)
- SIEM, UEBA & DLP Tools – Proactive!

SOLIDIFY YOUR WALLS

Penetration testing identifies holes in a firm’s internal and external security systems, enabling them to remedy vulnerabilities. Does your firm’s systems have holes that need to be filled?

- Conduct thorough due diligence of reputable third-party testers
- Look for a vendor with the appropriate certifications, including Certified Ethical Hacker (CEH), (OSCP) or GIAC Penetration Tester (GPEN)
- Establish parameters that specify appropriate timing of testing and the applications, systems, networks, IP addresses etc. that should be tested
- Automated tools available

GAIN GREATER CONTROL OVER MOBILE DEVICE USE

As the use of smartphones, tablets & laptops have grown, so have their cybersecurity risks. Set parameters to maintain greater control & combat risks.

- Establish policies for staff and advisors to protect sensitive firm data
- Standards for the use of personal devices for firm business (its all business!)
- Conduct training for all staff and advisors
- Ensure devices aren’t Jailbroken
- Enable remote wipe capabilities for firm data
- Manage access by location

OTHER REGULATORS

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Thank you.

Sam Attias

VP, Partnership Development

sattias@os33.com

workplace_