Enterprise Risk Alert

A bi-weekly publication from the Accordo Team

October 13, 2017

2017 Regulatory and Examination Priorities Letter

FINRA (Aug. 13, 2016)

Events like the Equifax breach highlight the continued importance of cyber controls. FINRA's priority letter addressed the growing concerns related to cybersecurity threats, the ever-changing technology landscape, and the need for a flexible approach to cybersecurity regulation. FINRA plans to assess firms' programs, focusing on data loss prevention, data protection and monitoring, vendor risk management and insider threats. FINRA also highlighted two main areas of concern, cybersecurity controls at branch offices and regulatory requirements under Securities Exchange Act Rule 17a-4(f), namely maintaining specific records in WORM format, or "Write Once, Read Many". Link

The $81 million virtual Bangladesh Bank heist is linked to the Sony hack

Business Insider (May 13, 2016)

The malware used in the cyber heist on Bangladesh Central Bank is reported, by BAE Systems, to be connected to the 2014 cyber attacks on Sony. The same malicious software was also identified in a recent cyber attack on a Vietnamese bank. The details of the attacks reveal similarities in code to other cyber attacks dating back to 2009, including encryption keys and program objects. Link

FINRA Fines 12 Firms a Total of $14.4 Million for Failing to Protect Records From Alteration

FINRA (Dec. 21, 2016)

FINRA issued fines to 12 firms totaling $14.4 million for failure to preserve, properly maintain and safeguard broker-dealer records. Specifically, FINRA found that the firms failed to use WORM devices to protect against manipulation or destruction of sensitive records, or define appropriate procedural and supervisory processes. FINRA also found that at least three firms failed to adhere to and fulfill record retention rule requirements. Link

Hackers Breach 400,000 UniCredit Bank Accounts for Data

Bloomberg (Jul. 26, 2017)

UniCredit SpA, Italy's largest bank, with over 8,500 branches and spanning 50 markets, was victim to a cyber-attack; the breach occurred in September, 2016, and was discovered by the bank's IT department in July of 2017. The hackers had gained unauthorized access to 400,000 client accounts through one of the bank's third parties. In response, the bank invested in its IT systems, conducted an audit and reported the incident to the Milan prosecutor. Experts expect a more aggressive wave of cyber-attacks to follow. Link

Key Considerations:

- **Establish a Top-down Approach**
  - ✓ 90% of the firms reviewed by FINRA in 2014 used NIST, ISO or ISACA standards or frameworks. Link
  - ✓ Major regulatory and operational risks for financial services firms include failure to build a successful enterprise cyber-defense program, inadequate measures to protect customer PII or establish adequate controls and failure to perform regular risk assessments to assess threats, vulnerabilities and controls.
- **Know Your Threats & Vulnerabilities**
  - ✓ Some of the most common cyber incidents at banks and broker-dealers are distributed denial-of-service attacks (DDoS), phishing, ransomware, insider threats and wire-transfer fraud.
  - ✓ Top sources for intelligence-sharing among broker-dealers include Financial Services Information Sharing and Analysis Center and United States Computer Emergency Readiness Team.
- **Conduct Cyber Risk Assessments**
  - ✓ Financial institutions should leverage industry standards and frameworks such as COBiT 5 or COSO ERM frameworks, FFIEC Cybersecurity Tool, CPMI-IOSCO risk assessment guidelines and CVSS (Common Vulnerability Scoring System), to identify, measure and monitor system vulnerabilities.
- **Take Preventative Action**
  - ✓ A recent survey of executives at financial firms found that nearly 75% of respondents used, at a minimum, 25 different technologies for cybersecurity. Link
  - ✓ Integrate cybersecurity, anti-fraud, and anti-money laundering efforts for effective supervision and controls.

ACCORDO