5ironCYBER

CYBERSECURITY & SARS2025

Jason Bradley
EVP, 5ironCyber

Introduction

Purpose

- **Understand why cybersecurity is critical for SARs filing.**
- **Learn practical tips for collaborating with IT teams.**

Agenda

- Cybersecurity threats and BSA compliance
- Collaborating with IT teams
- Bridging knowledge gaps
- SAR filing for cyber events
- Case studies and Q&A

The Intersection of Cybersecurity & BSA Compliance

BSA/AML Implications

Regulatory Expectations and Financial Crime Issues

- Cybersecurity threats are no longer just IT problems—they are now compliance challenges. Financial institutions are prime targets, and the impact can include fraud, identity theft, and account takeovers. From a compliance perspective, regulatory expectations demand that institutions treat these threats as potential financial crimes. Understanding this intersection is key to fulfilling you

The Intersection of Cybersecurity & BSA Compliance

Cybersecurity Threats

- **Data Breaches** - Unauthorized access to sensitive information, such as customer data or financial records, that requires reporting to regulatory bodies.
- **Ransomware** - Malware that encrypts files and demands payment for decryption, posing a significant threat to the integrity of financial systems.
- **Phishing** - Deceptive attempts to obtain sensitive information (e.g., passwords, account details) through fraudulent emails or websites.
- **Business Email Compromise (BEC)** - Cybercriminals impersonate executives or trusted partners to initiate unauthorized transfers of funds.
- **Malware Attacks** - Harmful software designed to disrupt, damage, or gain unauthorized access to computer systems, affecting transactional records.
- **Insider Threats** - Employees or contractors misusing their access to compromise systems or steal sensitive information.

The Intersection of Threats TO . . . Cybersecurity & BSA Compliance

Understanding The Threat of AI

- **Hallucination/Factual Errors** - If generative AI is used to assist in drafting narratives, summaries, or research, it may fabricate or misstate facts (“hallucinate”) — e.g. “inventing” transactions, misattributing ownership, or incorrectly summarizing external data.

- **Opacity/Lack of Explainability (“Black Box”)** - Highly complex models may not allow clear explanations of why a given alert was generated (e.g. which features drove the decision).

- **Overreliance/Automation Without Oversight** - Mistakes could lead to filing incorrect SARs, missing actual suspicious activity, or failing to review alerts appropriately. ***YOU own your SAR***

- **Data Privacy/Data Leakage** - The AI system may require ingesting external datasets (public records, third-party data, media feeds), which introduces risk of data breaches or violation of privacy laws. Also, logs or model outputs might leak sensitive customer data.

The Intersection of Threats TO . . . Cybersecurity & BSA Compliance

What AI is already being used inside your Organization?

- ChatGPT (Assistant)
- Microsoft Copilot (Assistant)
- Google Gemini (Assistant)
- Chatbots: “Erica” (Bank of America)
- SentinelOne/Crowdstrike (Endpoint Security)
- Verafin (Fraud)
- ComplyAdvantage (Fraud)
- Candescent (Fraud debt alert clearing)
- Temenos (Compliance)
- Salesforce (CRM/Data Management)

How are you governing the apps and their data?

Thoughts on AI Governance

- **Maintain a Model Inventory** - Each AI component should be in a register including version, purpose, owner, validation status, refresh frequency, risk tier.
- **Change Management "Counsel"** - Any changes (retraining, threshold tweaks, new features) must pass review by compliance, risk, and technology.
- **Cross-Functional Engagement**: Involve IT, legal/privacy, internal audit to ensure integrity, security, and compliance alignment.
- **Regulator/Examiner Readiness** - Be prepared to present model documentation, performance metrics, override logs, and validation reports upon request.
- **Continuous Monitoring and Feedback Loop** - Regularly check for drift, unusual model outputs, and feedback from investigators to refine models.
- **Training and Awareness**: Ensure compliance analysts, investigators, and management are educated on how AI works, its limitations, and how to interpret outputs.

Bridging Knowledge Gaps

Improve Your Understanding

Sample Glossaries of IT and Security Terms

- https://www.sans.org/security-resources/glossary-of-terms/
- https://www.coursera.org/resources/cybersecurity-terms

Example

- **IP Address—**A computer's inter-network address that is assigned for use by the Internet Protocol and other protocols. An IP version 4 address is written as a series of four 8-bit numbers separated by periods. IP version 6 uses hexadecimal numbers separated by colons, and offers a much larger address space due to its longer bit size.
  - IPv4 format—192.168. 1.1
  - IPv6 format—2001:0db8:85a3:0000:0000:8a2e:0370:7334

Build Relationships with Your IT Team

Foster Trust

- Engage IT/Security to make sure they are aware they need to be a part of the SAR process
- Keep Communication open between the BSA Officer and the IT/Security group
- Have a plan to request information from IT/Security if needed

Joint Initiatives

- Enable IT/Security to recommend filing a SAR (Often it’s the only way you know to file one)
- If IT/Security reports an event to FBI’s Internet Crime Complaint Center (ic3.gov), they should let you know about it.

Ensure outsourced IT/Security is included in these processes

Collaborating with IT Teams

IT provides the technical expertise required to effectively file a cyber-SAR

Strategies

- Key questions
  - 'What systems were targeted?'
  - 'What was the method of entry?’
  - Etc.
- Translating cyber-related details for SARs

Including Cyber-related Information in SAR Reporting

Elements

- Description and magnitude of the event
- Known or suspected time, location, and characteristics or signatures of the event
- Indicators of compromise (IOCs)
- Relevant IP addresses and their timestamps
- Device identifiers
- Methodologies used
- Other information the institution believes is relevant

https://omb.report/icr/201710-1506-002/doc/78187401

Gathering Information

- **The data gathered from IT/Security will help you select the Suspicious Activity Characterization**
  - ie., Cyber Event, Account Takeover, Unauthorized Electronic Intrusion, Wire Fraud, etc.
- **The information collected will provide details critical to law enforcement**
  - IP Address Information (Remember IPv4 or IPv6?)
  - Host Domain information
  - Methodology
  - Etc.

SAR Reporting of Cyber-Events

Overview of FinCEN Guidance (FIN-2016-A005)

- In determining whether a cyber-event should be reported, a financial institution should consider all available information surrounding the cyber-event, including its nature and the information and systems targeted. Similarly, to determine monetary amounts involved in the transactions or attempted transactions, a financial institution should consider in aggregate the funds and assets involved in or put at risk by the cyber-event.

https://www.occ.gov/news-issuances/alerts/2012/alert-2012-16.html

SAR Reporting of Cyber-Events

Example

Bank A is told by its customer, ABC Corp, that a recent wire payment issued from its account was fraudulent. Bank A is told that fraudsters imitated the CEO of ABC Corp.'s e-mail to instruct ABC employees to wire funds from ABC's accounts at Bank A to an account at Bank B. ABC Corp tells Bank A that these fraudulent e-mails were made to look like the CEO used the e-mail address CEO@ABCcorp.co instead of the legitimate CEO@ABCcorp.com. These fraudulent e-mails appeared to be instructing employees to issue urgent payments to one of ABC's suppliers for $300,000. Bank A recognizes this as a Business E-mail Compromise (BEC) scheme. In the SAR narrative, Bank A describes the incident and mentions the term "BEC Fraud" and FinCEN advisory FIN-2016-A003.

https://omb.report/icr/201710-1506-002/doc/78187401

SAR Reporting of Cyber-Events

Example

Bank D identifies an incident that targeted Bank D's own systems, resulting in access to Bank D's payment systems and an attempted transfer of $50,000 through Bank D's 123-wire system. Bank D's compliance team asks its IT department for additional technical information related to this incident, and whether there were any key indicators associated with the event. Bank D's IT department confirms that the incident was a cyber event against Bank D, but is unable to spend resources locating additional information due to their necessary focus on continuity of business operations. Bank D files a SAR based on the available information.

https://omb.report/icr/201710-1506-002/doc/78187401

IC3.gov

FEDERAL BUREAU OF INVESTIGATION
Internet Crime Complaint Center IC3

Created to enable the public to report information concerning suspected Internet-facilitated criminal activity and to develop effective alliances with law enforcement and industry partners.

https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

IC3.gov Recovery Asset Team

The Internet Crime Complaint Center's Recovery Asset Team (RAT) was established in February 2018 to streamline communication with financial institutions and assist FBI field offices with the freezing of funds for victims who made transfers to domestic accounts under fraudulent pretenses.

https://www.ic3.gov/AnnualReport/Reports/2023_IC3Report.pdf

IC3.gov Recovery Asset Team

Successes

Incidents: 3,008

Losses: $758.05 Million

Frozen: $538.39 Million

Success Rate: 71%

https://www.ic3.gov/AnnualReport/Reports/2023_IC3Report.pdf

Share Cyber-Related Information

- Cyber-related information, such as information about specific malware signatures, IP addresses and device identifiers, and seemingly anonymous virtual currency addresses, for example, can help identify the individuals, entities, organizations, or countries involved or responsible for the cyber-event or cyber-enabled crime linked to money laundering or terrorist activities.
  - Report to **IC3.gov**
  - Report to **FinCEN**
  - Share with other financial service organizations through organizations such as Financial Services Information Sharing and Analysis Center (FS-ISAC)
    - **fsisac.com**

5ironCYBER

QUESTIONS?

Jason Bradley
EVP, 5ironCyber

5ironCYBER

TRENDING CYBER-RELATED ATTACKS

Unauthorized Access To Customer Information

Unauthorized access refers to any attempt or successful intrusion into the institution's systems resulting in access to sensitive customer information.

Red Flags

- Multiple failed login attempts
- Unusual access times or locations
- Unauthorized access to privileged accounts

Reporting

- Include details on the nature of the unauthorized access and potential impact on customer information

Phishing Attacks Targeting Customers

Phishing involves fraudulent attempts to obtain sensitive information by posing as a trustworthy entity, typically through email or other communication channels.

Red Flags

- Unusual requests for sensitive information
- Suspicious links or attachments in emails
- Reports of phishing attempts from customers

Reporting

- Include details on the phishing attempt, such as the method used and any compromised information

Malicious Software Activities

Malicious software (malware) refers to software designed to harm or exploit computer systems. This includes viruses, ransomware, and other types of malware.

Red Flags

- Unusual network traffic patterns
- System performance degradation
- Reports of malware infections from employees or customers

Reporting

- Include details on the type of malware, affected systems, and potential impact

Insider Threats

Insider threats involve individuals within the organization who misuse their access and privileges to compromise the institution's systems or data.

Red Flags

- Unusual access patterns or activities by employees
- Multiple policy violations by an employee
- Suspicious financial transactions linked to an insider

Reporting

- Include details on the insider's role, motives, and any accomplices if identified

Digital Check Fraud

Digital check fraud involves the manipulation of digital images of checks for unauthorized financial gain. Fraudsters alter check details or create counterfeit checks using digitally altered images.

Red Flags

- Unusual patterns in check transactions, ex. sudden increases in check amounts.
- Detection of altered check images through advanced image analysis tools.
- Reports from customers regarding suspicious check activities.

Reporting

- Include details on the altered checks, affected accounts, and any additional information on the fraudulent activities.

Enhanced Social Engineering

Enhanced social engineering involves sophisticated manipulation techniques to deceive individuals into divulging sensitive information or performing actions that lead to financial losses.

Red Flags

- Unusual communication patterns, such as targeted and personalized messages.
- Requests for sensitive information, such as login credentials or account details.
- Instances of employees being manipulated into performing unauthorized transactions.

Reporting

- Provide details on the methods used, individuals targeted, and any compromised information.