2018 FINRA Cybersecurity Conference
February 22 | New York, NY

Cyber Incident Response Plans and Resources
Thursday, February 22
2:30 p.m. – 3:30 p.m.

Every organization should develop a written plan that identifies cyber-attack scenarios and sets out appropriate responses. While plans must be customized for each organization's particular circumstances, the plan should address basic components. Join panelists as they discuss these components and provide examples of steps their firms have implemented. Panelists also provide resources and helpful tools for firms to address critical cyber threats as well as provide examples of what not to do.

Moderator: Rafael Skovron
Examination Manager, Sales Practice
FINRA San Francisco District Office

Panelists: Andrew Hartridge
Chief Information Security Officer
M&T Securities, Inc.

Paul Horn
Chief Information Security Officer
HD Vest Financial Services

Gregory Scroggs
Senior Vice President and Chief Information Security Officer
Primerica

Cyber Incident Response Plans and Resources Panelist Bios:

Moderator:

Rafael Skovron began his career by consulting for international public accounting firm Grant Thornton. Mr. Skovron's work included a large IT controls project at Fannie Mae in D.C and testing IT controls for financial audits of public companies. Mr. Skovron then joined the Office Depot Internal Audit team and performed operational, financial, and technology audits at the global headquarters in Boca Raton and in Mexico. At FINRA, Mr. Skovron has worked at both the Boca Raton and San Francisco offices leading cybersecurity and technology governance routine examinations. His cause examinations have covered breaches of broker-dealer websites, phishing, business email compromise scams, mobile security risks, cloud security and branch office risks. He is also a member of an internal consulting team that develops guidance on technology governance and cybersecurity. Mr. Skovron is also a member of the Bay Area Chapter of InfraGuard, a non-profit organization serving as a public-private partnership between U.S. businesses and the Federal Bureau of Investigation to address cybersecurity risks.

Panelists:

Andrew Hartridge serves as M&T Bank's Chief Information Security Officer, forming and executing the overall strategy for information security. Mr. Hartridge is an accomplished Information Technology executive with in-depth knowledge of Telecommunications, Information Security, Privacy, Operating Platforms and Emerging technologies. He has broad experience in the public and private sectors within financial services, health-care, and manufacturing industries. He leads Cybersecurity activities for the Company, inclusive of networking and telecommunications, identity and access management, regulatory compliance and related policy and project support, to protect the Bank's and customers' data, monetary assets, information and reputation. Prior to this position, Mr. Hartridge held progressively senior executive leadership roles at the US Internal Revenue Service where he was responsible for covering all aspects of the agency's cybersecurity program. Mr. Hartridge is a Certified Information Systems Security Professional (CISSP) and an Information Systems Security Architecture Professional (ISSAP).

Paul Horn currently serves as Chief Information Security Officer (CISO) at HD Vest Financial Services and has more than 20 years of various security experiences. Those experiences include time spent as a Special Agent with the Air Force Office of Special Investigations, leading a global information security program for DynCorp International's logistics and air operations for various government contracts, and leading the Drug Enforcement Administration's Aviation Division vulnerability management program. Mr. Horn also takes part in the Strategic Threat Assessment & Response (STAR) work group lead by the IRS to help protect taxpayers and the integrity of the tax ecosystem. In addition, Mr. Horn has been a finalist in 2013, 2014, 2015 and 2016 for Certified CISO of the Year through EC-Council and now serves on the awards committee. Mr. Horn also serves on a variety of Cyber Security Advisor Boards and has a deep dedication to the information security community by mentoring other security professionals. Mr. Horn holds a Master of Science in Management with a concentration in Information Systems Security and a Bachelor of Science in Business Administration in Information Technology from Colorado Technical University. Mr. Horn also holds the following information security certifications, Certified Chief Information Security Officer (C|CISO), Certified Information Systems Security Professional (CISSP), Certified Information Security Manger (CISM), Certified in Risk and Information Systems Control (CRISC), and GAIC Certified Incident Handler (GCIH).

Greg Scroggs attended Georgia Tech as a cooperative student with The Southern Company in Atlanta, where he served in a variety of roles: computer operations, application programming, system programming, and telecommunications functions. His next role involved both technical and management positions at the Primerica division of Travelers and Citigroup, where he held various technical operations, security, and telecommunications management positions. For the past 10 years, Mr. Scroggs has managed security engineering and operations, technology risk management, and data telecommunications for Primerica, which is now a public company. His current role at Primerica is Senior Vice President and Chief Information Security Officer (CISO).

Cyber Incident Response Plans and Resources

Panelists

- **Moderator**
  - Rafael Skovron, Examination Manager, Sales Practice, FINRA San Francisco District Office
- **Panelists**
  - Andrew Hartridge, Chief Information Security Officer, M&T Securities, Inc.
  - Paul Horn, Chief Information Security Officer, HD Vest Financial Services
  - Gregory Scroggs, Senior Vice President and Chief Information Security Officer, Primerica

To Access Polling

- Under the “Schedule” icon on the home screen,
- Select the day,
- Choose the Cyber Incident Response Plans and Resources session,
- Click on the polling icon: 📋

Polling Question 1

1. Are you from a small firm? (Under 100 RRs)
   a. Yes
   b. No

Why invest resources in incident response?

- Reduce recovery time
- Increase stakeholder confidence
- Limit reputational damage to the firm and to the industry
- Compliance with FINRA supervision rules

Polling Question 2

2. What would you do if your printers started printing out tax returns randomly?
    a. Turn the machine off
    b. Add paper and collect the tax returns
    c. Call the police
    d. Contact your Chief Information Security Officer

What is an incident?

- Potential Events
- Declared vs Confirmed
- Indicators
- Incidents vs Attacks
  - Severity levels

Key elements of an incident response plan

- Containment
- Mitigation
- Recovery
- Investigation
- Notification
- Restitution

Who are the major players in the plan?

- Commander
- Executives
- PR / Communications
- Legal
- Compliance
- What do you outsource?

Common issues when implementing a plan

- Too much data, not enough understanding of people, process, and tech
- New vendors quickly on-boarded
- Fatigue
- Incident response doesn’t scale
- No logs
  - Some logs are worth more than others

Practicing the incident response plan

- Practice beyond table tops or not?
  - Open vs closed pen tests
- Pre-scripted playbooks for more frequent attacks
- Develop scenarios for specific outcomes or not?
  - Who makes decisions, when, how will it be made.

Polling Question 3

3. **Do you rely on insurance as your incident response plan?**
    a. Yes
    b. No

Can small firms run effective incident response?

- Breach coach
- Vendors
  - Correlating events across customers
- Small Firm Checklist

How does insurance factor into incident response?

- Role of cyber insurance underwriters
- Policy review

Does incident response change in the cloud?

- Networks and data are in the cloud
- Forensic detail
- Contractual responsibilities
- Vendor involvement

Security Incident Response Plan
(S-IRP)

Revision History

Revision Number	Issue Date	Issued By	Explanation

1 Table of Contents

2 Responders

The following individuals have been identified within the Security Incident Response Plan with duties and responsibilities described in later sections of this document.

	Security Incident Response Team Core Members		
Name	**Function**	**Section**	**Telephone**
	Incident Commander	8.1	
	Incident Commander	8.1	
	Incident Administrator	8.2	
	Incident Administrator	8.2	
	Incident Administrator	8.2	
	Anti-money Laundering Responder	8.3	
	Anti-money Laundering Responder	8.3	
	Supporting Responders		
Name	**Function**	**Section**	**Telephone**
	Incident Coordinator	8.4.1	
	Incident Coordinator	8.4.1	
	Sr. Reviewing Executive	8.4.2	
	Sr. Reviewing Executive	8.4.2	
	IT Responder	8.4.3	
	IT Responder	8.4.3	
	IT Responder	8.4.3	
	SOC Responder	8.4.4	
	QSA Responder	8.4.5	
	QSA Responder	8.4.5	
	Forensic Responder	8.4.6	
	Forensic Responder	8.4.6	
	Forensic Responder	8.4.6	
	Forensic Responder	8.4.6	
	Forensic Responder	8.4.6	
	DR Responder	8.4.7	
	DR Responder	8.4.7	
	Communications Responder	8.4.8	
	Communications Responder	8.4.8	
	Risk and Compliance Responder	8.4.9	
	Risk and Compliance Responder	8.4.9	
	Finance Responder	8.4.10	
	Finance Responder	8.4.10	
	Legal Responder	8.4.11	
	Legal Responder	8.4.11	
	Legal Responder	8.4.11	
	Legal Responder	8.4.11	
	Operations Responder	8.4.12	
	Operations Responder	8.4.12	
	Sales Responder	8.4.13	
	Sales Responder	8.4.13	
	HR Responder	8.4.14	
	HR Responder	8.4.14	
	Law Enforcement Responder (FBI)	14.2	
	Law Enforcement Responder (FBI)	14.2	

	Law Enforcement Responder (USSS)	14.2	

3 Overview

The purpose of this Security Incident Response Plan ("S-IRP" or "Plan") is to provide a governing framework for Acme Corporation and its subsidiaries ("Acme" or the "Company") around Incident Response (IR) efforts for suspected and confirmed Security Incidents. The goal of the Plan is to outline Acme's approach for handling Incident Response efforts, defining Security Incident(s), identifying the organizational structure and defining roles, responsibilities, and levels of authority, identifying the severity rating of Security Incidents, and establishing methods of reporting and escalation of Security Incidents.

The S-IRP also establishes the Security Incident Response Team (SIRT). The SIRT will follow the guidance in this document. The S-IRP will be reviewed annually and updated as needed to reflect changes in technology and/or at the request of the Chief Information Security Officer (CISO). Changes to the policy will be coordinated through the Information Security Steering Committee (ISSC) for approval. In the event that items in the S-IRP are unclear, the CISO and/or Deputy Information Security Officer (Deputy ISO) will provide interpretive guidance.

3.1 Effective Date

The S-IRP will be effective January 1, 2017 but will be limited to Security Incidents rated as a Level 5 or 6 along with a Functional or Recoverability Impact of Significant or Catastrophic; or Informational Impact of Privacy Breach or Integrity Loss. These incidents will be identified as "**Declared Incidents**" and discussed further in section 5.3.

3.2 Forward

The Company must be able to respond to physical and electronic Security Incidents in a manner that protects the Company's Confidential Information (defined below) and resources (both physical and electronic) that might be affected by the Security Incident.

The Company in varying degrees, relies upon Confidential Information ("Confidential Information"), which includes Confidential or Proprietary business information of the Company, cardholder and sensitive authentication data within the Payment Card Industry Data Security Standard (PCI DSS), nonpublic personal information (NPPI) of Company customers and personally identifiable information (PII) of employees, registered representatives, Investment Advisors Representatives and customers, such customers and employees being referred to herein collectively as "Company Constituencies," and registered representatives and investment advisors being referred to herein collectively as "Advisors". See the Information Security Policy for definitions of Confidential Information, NPPI, and PII and for the detailed Information Classification Matrix.

3.3 Reporting

The SIRT, in consultation with the Legal Responders (identified in Section 8 of the S-IRP), are responsible for determining the extent of Federal, State, and Self-Regulatory Organization (SRO) notification to be made in connection with a Security Incident. The actual notification will be performed by the Legal Responders.

Security Incident's may result in a business disruption resulting in the activation of the Business Continuity Plan (BCP) and/or the Emergency Plan. See the BCP and Emergency Plan's for more details.

3.4 Scope

This S-IRP applies to all physical and electronic Security Incidents involving Company resources, including, but not limited to employees, hard copy documents, electronic documents, and any computing devices, midrange, and network environments owned or used by Acme, Advisors, third-party service providers and vendors that access, process, store, or transfer Acme Information.

For Security Incidents involving Advisors and any Advisor-owned or leased IT equipment, a Security Incident Intake Form must be completed by contacting the Help Desk or submitting an email to acmesecurity@acme.com Monday through Friday between the hours of 8:00am and 5:00pm Central Standard Time. All applicable portions of the Security Incident Intake Form and portions of this document may apply and where applicable must be followed.

4 Definitions

For the purpose of this document, a Security Incident is defined as an “Event” that has actual or potential adverse effects on an individual, computer or network resource resulting in misuse and/or abuse, compromise of information, loss and/or damage of company property and/or information. Any Event that originates from, is directed towards, or transits Company controlled computing equipment and/or network resources, to include Software as a Service (SaaS), Platform as a Service (PaaS), or Infrastructure as a Service (IaaS) in support of Acme business operations, will fall under the purview of the SIRT.

Computing device containing Company information operated and/or owned by Advisors will fall under the purview of the SIRT for reporting purposes; detection, containment, eradication, and recovery efforts will be the responsibility of the System Owner and/or Advisor. It is foreseeable that many Events will be classified and handled by semi-automated or automated means and will not require further analysis and/or escalation. The potential list of Security Incidents is contained in Section 6 of this document.

4.1 Event

For the purpose of this document, an “Event” is defined as any observable occurrence either physical or within a system or network.

4.2 Precursor

For the purpose of this document, a “Precursor” is a sign that a Security Incident may occur in the future.

4.3 Indicator

For the purpose of this document, an “Indicator” is a sign that a Security Incident may have occurred or may be occurring now.

4.4 Incident Response

For the purpose of this document, “Incident Response” means the process of detecting and analyzing a “Security Incidents” and mitigating its effect on an organization.

4.5 Investigation

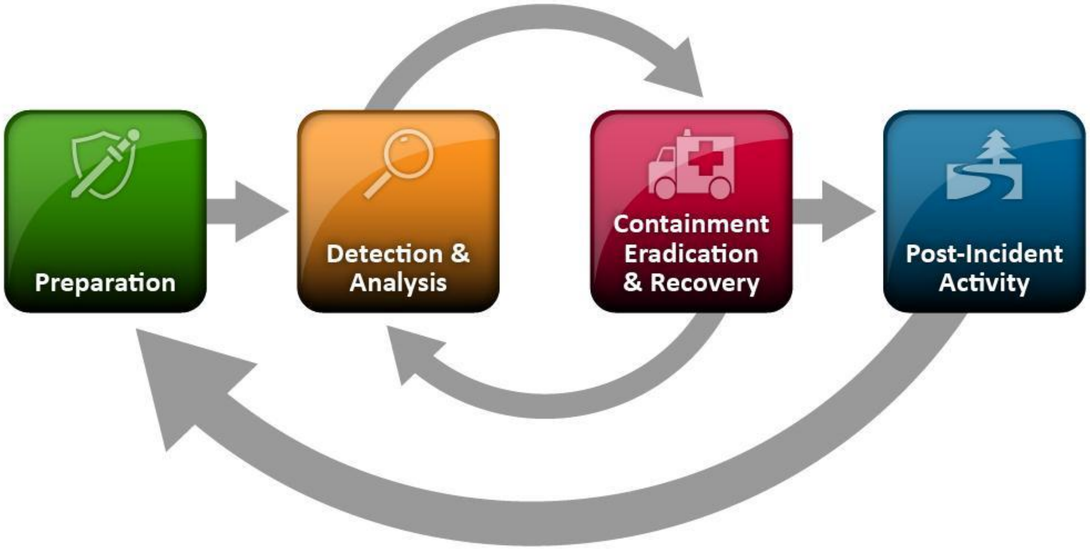
For the purpose of this document, an “Investigation” is the process for ascertaining facts and detailed examination of information.

4.6 System Owner

For the purpose of this document, a “System Owner” is the person responsible or designated for procurement, development, integration, modification, or operation and maintenance of the information system.

5 SIRT Framework

The S-IRP Life Cycle methodology establishes response capability, but also aids in preventing Security Incidents. The SIRT is typically not responsible for Security Incident prevention, it is fundamental to the success of the Security Incident Response Program. The sections below provide a basic framework that must be followed to handle and prevent Security Incidents.



5.1 Preparation

A Company goal is to try to keep the number of Security Incidents low to protect the business and its processes. If the number of Security Incidents is high in volume it may overwhelm the SIRT and their capabilities.

The SIRT must be knowledgeable with industry acceptable Incident Handling techniques. The lists of training requirements are listed in Section 11 of this document.

5.2 Detection & Analysis

Security Incidents occur in a multitude of ways, and it is not feasible to develop a step-by-step instruction for each type of Security Incident. SIRTs need to be flexible in its approach to handling and responding to any type of Security Incident. The list of Attack Vectors can be found in Section 6.4 of this document.

5.2.1 Detection

The most challenging part of the Incident Response process is the ability to accurately detect and assess suspected or possible Security Incidents and then make a determination if a Security Incident occurred. The challenge resides within the following three factors:

1. A Security Incident may be detected though a variety of means, e.g., automated network based detection tools, host based Intrusion Detection Systems (IDS), antivirus platforms, and log analyzers or by manual means such as an individual reporting an Event or problem. When applicable computing resources (applications, systems, etc.) must be configured to send Event Logs to a centralized Security Incident and Event Management (SIEM) platform for analysis to provide a central method for detection and/or initiating directives.
2. The volume of Events and/or potential signs of a Security Incident in most organizations are generally high. It is not uncommon for an organization to encounter thousands if not millions of intrusion detection Events per day.
3. Because the severity of Security Incidents is variable, individuals who have specialized technical knowledge and extensive experience need to evaluate Security Incident related data.

5.2.2 Reporting New Security Incidents

Anyone who suspects the occurrence of a Security Incident or is affected by a Security Incident must report such information via telephone to the Help Desk within 2 hours of discovery and/or learning of the information or as soon as reasonably practicable. The Help Desk's phone number is (555) 555-5555. Security Incidents may also be reported through the acmesecurity@acme.com mailbox Monday through Friday between the hours of 8:00am and 5:00pm Central Standard Time. The individual who reports the Security Incident will be known as the "Detector" and s/he will provide relevant information to the Help Desk representative that will be included in the Security Incident Intake Form. In the event the Help Desk is unavailable, notifications must be made to the CISO and/or Deputy ISO identified in Section 2 and 8.1.1

The Help Desk is initially responsible for ensuring the minimal information is contained within the Security Incident Intake Forms and providing the data to the CISO and/or Deputy ISO. The Help Desk must notify the CISO and/or Deputy ISO upon completing the Security Incident Intake Form or as soon as reasonably practicable. In some cases Information Security personnel and the Incident Administrator may self-initiate a Security Incident Intake Form.

5.2.3 Security Incident Intake Form

The Security Incident Intake Form at a minimum needs to contain the following data points prior to submitting to the CISO and/or Deputy ISO:

- Date and Time notified
- Date and Time opened
- Date and Time of when the Event took place
- Title of the Incident
- Summary on the Event and how it was detected
- Detectors name, email, and phone number (Detectors may choose to remain Anonymous if so desired)
- Acme Point of Contact (POC) for the Event
- Category of the Incident
- Scope (Functional Impact, Informational Impact, and Recoverability Impact) of the Incident
- Severity of the Incident
- Method of detection

5.2.4 Analysis

The SIRT will endeavor to efficiently analyze and validate each Security Incident and follow a pre-defined evaluation and resolution process. The SIRT will document the steps it takes during the evaluation stages. When the SIRT believes that a Security Incident has occurred, they will evaluate the scope of the Security Incident by making the following determinations, if possible: (i) the cause of the event; (ii) how it occurred by performing containment; (iii) what was affected. The SIRT will update the status of Security Incidents by performing a deeper analysis of Security Incidents, perform root cause analysis and identify corrective actions as needed.

The status for Security Incidents shall contain the following data points (as applicable):

- A summary of the Security Incident;
- Indicators related to the Security Incident;
- Actions taken by all Incident Handlers on the Security Incident;
- Impact assessments related to the Security Incident (Functional, Informational, and Recoverability);
- Contact information for other involved parties (non SIRT members);
- A list of evidence gathered during the Security Incident;
- Comments from Incident Handlers;
- Next steps to be taken, to include root cause analysis and corrective actions as needed.

IDS systems may produce false positive instances resembling Security Incidents which will require further analysis. Not all Security Incidents have Precursors and Indicators are common. Even when an Indicator is accurate, it does not automatically mean a Security Incident has occurred. For example, a server can crash due to a memory leak, and this would not be classified as a Security Incident. The Incident Commander will use his or her judgment to determine whether an Event is actually a Security Incident.

5.2.5 Security Incident Ratings

The Incident Commander will rate all new Security Incident s/he oversees and document the appropriate response(s) taken by the SIRT based on several factors such as impacts, attack vectors and privacy. If a Security Incident meets multiple severity ratings the highest level must be chosen. The Incident Commander may reduce the Security Incident classification or prioritize open Security Incident evaluations based on the information available to him or her or when readily available alternatives.

Security Incidents receiving a "Level 6" severity rating will receive the highest priority of SIRT resources. In the case of multiple Security Incidents, the higher severity rating will receive higher prioritization.

5.3 Security Incident Escalation

Security Incidents that are assigned a severity rating meeting the threshold in section 3.1 shall be known as "Declared Incidents". The SIRT members shall confirm the rating and, once this occurs, these incidents will be referred to as "Confirmed Incidents."   Incident ratings may change during the evaluation stages of a Security Incident, especially as the SIRT obtains and reviews additional information. The Incident Commander will coordinate with the SIRT to determine if a Security Incident needs to be escalated or de-escalated. The same criteria used to initially rate a new Security Incident will be used to escalate or de-escalate a severity rating. Confirmed Incidents need to be evaluated for insurance carrier notification by the Legal Responders. If such requirement exists the Legal Responder will notify the Insurance Carriers and perform any required follow up actions they request.

5.3.1 Escalation

The Incident Commander will approve the initial or escalation of any Security Incident that is identified as a "Declared Incident" with a severity "Level 6" and activate the Core SIRT members as appropriate. The Senior Reviewing Executive will inform Senior Management about the Security Incident and the reason for the escalation as soon as reasonably practicable.

The Incident Commander will approve the initial or escalation of any Security Incident that is identified as a "Declared Incident" with a severity "Level 5", and activate the Core SIRT members as appropriate. The Incident Commander will be responsible for informing Senior Management about the Security Incident and the reason for the escalation at the discretion of the SIRT.

5.3.2 De-escalation

The Incident Commander will obtain approval from the SIRT before lowering a "Confirmed Incident" with a "Level 6" rating. The Incident Commander must document the reason(s) for the de-escalation.

5.4 Containment, Eradication & Recovery

All Security Incidents will be handled in phases, including: containment, eradication and recovery.

5.4.1 Containment

The SIRT is responsible for developing containment and remediation strategies. Containment strategies will vary and will be largely dependent on the circumstances and type of Security Incident. Most Security Incidents will require some form of containment (short or long-term) to limit the damage to the company. Decision-making will be more streamlined if there are predetermined containment and remediation strategies to follow in the event of routine or standard types of Security Incidents

Collecting evidence is an important part of evaluating and resolving a Security Incident. The goal of collecting evidence is to resolve the Security Incident, and it may be needed for legal proceedings. Gathering evidence may not be required for every Security Incident. The Incident Commander will consult with the SIRT and direct the collection of evidence as needed. The Incident Commander may also discuss the evidence collection efforts with

Legal Counsel, as needed. Evidence that is collected during the investigation of a Security Incident must be accounted for and secured at all times and collected according to applicable laws and regulations so that any evidence can be admissible in court if needed.

The SIRT must physically secure and store evidence and/or material collected and/or prepared during the course of a Security Incident. Evidence must be retained for at least 120 days from the date the Security Incident is presented to the ISSC, or as long as reasonably necessary for legal purposes.

The Incident Commander has the discretion to direct the discovery of the identification of attacking hosts.

5.4.2 Eradication

Once a Security Incident has been contained, eradication may be necessary to remove and/or eliminate components and/or artifacts associated with the Security Incident. For example, malware needs to be deleted, certain user accounts may need to be disabled, and vulnerabilities that were exploited and/or involved must be identified and fixed to the extent possible.

Systems owned and operated by Advisor's that may be involved in Security Incident's may require the Advisor to coordinate with individuals who have specialized computer security skills and forensic skills and are able to perform or assist with any detection, containment, eradication and/or recovery efforts. Advisors will need to coordinate with Acme Security to determine the appropriate computer security and/or forensic skills needed prior to engaging anyone for assistance as this may result in duplicate expenses for the Advisor.

In some situations access to Acme computing resources may be temporarily suspended until a qualified security professional is able to determine all containment, eradication and recovery steps are performed and such information is communicated to the Incident Commander and/or Incident Administrator.

5.4.3 Recovery

In general, recovery efforts are performed by the Incident Coordinator. Recovery efforts involve restoring systems to normal operation, confirming systems are functioning normally, and when applicable remediating vulnerabilities to prevent similar attacks from occurring. Recovery efforts may run parallel to and/or overlap with eradication efforts.

Typical recovery actions are listed below:

- Restoring from clean backups
- Rebuilding systems from scratch
- Replacing compromised files with clean versions
- Installing patches
- Changing passwords
- Tighten network perimeter security (e.g., firewall rules, access control lists)
- Higher levels of logging for affected resources

If a Security Incident has a severity rating of "Level 6" and/or the associated computing resources (e.g., a laptop or desktop) have been involved in two or more "Level 5" severity rated Security Incidents the computing resources must be reimaged and/or restored to a last known non-compromised state prior to being placed into service. Files that were previously on the computer resource need to be scanned prior to being placed on reimaged and/or restored computing resources. Note: The restoration of files may contain malicious code that may remain dormant until the files are opened. The Incident Commander will determine whether to restore files and report his or her decision to the SIRT. If the determination is made to restore files, only common files must be restored and under no circumstances may any user profiles be transferred to a clean system and/or image.

5.5 Post-Incident Activity

Post-Incident activities are a critical part of the Security Incident response process because they provide the Company with the opportunity to learn from Incident response activities and improve the evaluation and remediation processes as needed.

The Incident Commander will schedule a “lessons learned” meeting no later than 3 weeks after a Level 5 or 6 Security Incident is fully closed out. All members of the SIRT are required to attend the lessons learned meeting. The Incident Administrator will be responsible for documenting the meeting.

The following topics need to be discussed at the lessons learned meeting and summarized and documented by the Incident Administrator:

- Exactly what happened, and at what times?
- How well did staff and management perform in dealing with the Security Incident?
- Were the documented procedures followed, were they adequate, and do they need to be improved?
- What information was needed sooner?
- Were any steps or actions taken that might have hindered recovery?
- What would the staff and management do differently the next time a similar Security Incident occurs?
- How could information sharing with other organizations have been improved if this was done?
- What corrective actions can prevent similar Security Incidents in the future?
- What precursors or indicators need to be watched for in the future to detect similar Security Incidents?
- What additional tools or resources are needed to detect, analyze, and mitigate future Security Incidents?

During this meeting, the SIRT must identify the root cause(s) of the event to the best of their ability, remedial measures taken, the team’s performance and whether any internal controls, policies and/or procedures need to be modified in an attempt to prevent similar Security Incidents from recurring. The Risk Responder will submit an Issue and Corrective Action Report (ICAR) as needed that will be tracked by the Risk Management manager who is identified in the Firm’s Supervisory Control Program.

6 Security Incident Details

The Security Incident details listed below are required for all Security Incidents and will aid during IR efforts.

6.1 Categories

All Security Incidents will be categorized, based upon the details of the Security Incident.

Security Incidents at a minimum needs to contain one of the following data points:

Category	Summary and Notes
General	Any Security Incident Category not specifically identified below.
Unauthorized Access	An individual gains physical or logical access without permission to network, system, application, data, building/office, or other resource.
Loss of Data, Equipment, and/or Documents	The loss or theft of data, documents, a computing device or media.
Attrition	An attack that employs brute force methods to impair the normal functionality of networks, systems or applications (e.g., Denial of Service, Rainbow Tables).
Malicious Code (Malware)	Successful installation of malicious software (e.g., virus, worm, Trojan horse, or other code based malicious entity) that infects an operating system or application. Malicious code that has successfully been quarantined by antivirus software does not need to be reported.
Improper Usage	A person that violates the acceptable computing use policies.
Scans, Probes, and/or Attempted Access	Any activity that seeks to access or identify a computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service.
Investigation	Unconfirmed incidents that are potentially malicious or anomalous activity warranting further review.
Exercise and/or Network Defense Testing	To be used during testing or exercises and approved testing of internal and external network defenses or responses.
Social Engineering	Attempted acquisition of information such as usernames, passwords, and credit card details by disguising the request as a purportedly trustworthy entity in person or by an electronic communication (such as email, voice mail, etc.).
Failed Authentication (Advisor/Client only)	Attempted acquisition of information such as usernames, passwords, and credit card details by disguising the request as a purportedly trustworthy entity in person or by an electronic communication (such as email, voicemail, etc.).
System Malfunctions	Computing resources associated with improper maintenance and/or operation that are operating outside its intended purpose.
Physical Harm	Physical or psychological harm to an individual or group.

6.2 Scope

For the purpose of this S-IRP, each Security Incident will be evaluated to determine the potential Scope of the Security Incident. The Scope will aid in the identification of the Severity Level, and will aid during times of concurrent Security Incidents and to prioritize response efforts. The Scope consists of evaluating the functional, informational, and recoverability impacts. When a Security Incident is initially reported, the Scope may need to be estimated. If the Scope is unknown at the time of initial discovery, the team needs to make a conservative estimate based upon the information available; the Scope must then be modified as necessary during the lifecycle of the Security Incident if additional information is obtained and it changes the Scope.

The Scope for Security Incidents at a minimum needs to contain one of the following data points for each Impact:

Impact (with Category, Notes and Summary)	
Functional Impact	
Insignificant	Organization's ability to provide services is not effected.
Minor	Organization is able to provide services to all users but has lost efficiency
Marginal	Organization is able to provide critical services to all users but has lost efficiency
Major	Organization has lost the ability to provide services to a subset of users
Significant	Organization is no longer able to provide some services to any users
Catastrophic	Organization is no longer able to provide critical services to any users
Informational Impact	
None	No information was exfiltrated, changed, deleted, or otherwise compromised
Privacy Loss	*NPPI, PII, and/or payment card data was accessed or exfiltrated
Privacy Loss (Outside Acme)	*NPPI, PII, and/or payment card data was accessed or exfiltrated outside of Acme
Proprietary Loss	Company proprietary information was accessed or exfiltrated
Integrity Loss	*NPPI, PII, payment card data and/or proprietary information was changed or deleted
Recoverability Impact	
Insignificant	Time to recovery is possible and has been put to use; less than 1 hour
Minor	Time to recovery is predictable with existing resources; less than 2 hours
Marginal	Time to recovery is predictable with additional resources; less than 4 hours
Major	Time to recovery is unpredictable; no additional resources and outside help needed; less than 8 hours
Significant	Time to recovery is unpredictable; additional resources and outside help needed; more than 8 hours
Catastrophic	Recovery is not possible; permanent loss of service or facility (e.g., NPPI was exfiltrated and posted publicly)
Financial Impact	
Very Low	Less than $100,000
Low	$100,001 - $200,000
Moderate	$200,001 - $300,000
Medium	$300,001 - $500,000
High	$500,001 - $1,000,000
Very High	Greater than $1,000,001

*See the Acme Information Security Policy for the Information Classification Matrix that provides detailed examples of NPPI and PII data points.

6.3 Severity Levels (Rating)

All Security Incidents will be classified (rated), based upon the details of the Security Incident.

The Severity Level (Rating) for Security Incidents at a minimum needs to contain one of the following data points:

Rating (with Notes and Summary)	
Level 6 (Very High)	🟥
Any Event and/or Security Incident that potentially has a significant impact on one or more of the following: • The ability to provide products and/or services to a significant number of customers; • The ability to control, record, measure, track, and/or account for a significant amount of inventory, revenue or cash; • The unacceptable risk of significant punitive regulatory actions, contractual penalties, fraudulent criminal activity, and/or civil litigation; or • Significant notoriety that has potential to affect the Company's valuation adversely, damage the brand, and/or cause widespread concern amongst customers and/or investors.	
Level 5 (High)	🟥
Any Event and/or Security Incident not rated as "Level 6" and meets on or more of the following: • Subject to mandatory reporting and/or notification; • Requires due diligence to access, identify, and/or correct a deficiency within the organization's data processing, data usage, and/or information security infrastructure; • Presents the potential, but not the likelihood of some sort of litigation, and/or media attention; or • Impacts key business functions, systems and/or "Confidential information."	
Level 4 (Medium)	🟧
Any Event and/or Security Incident not rated as "Level 6 or 5" that results in a False Positive and/or a duplicate effort.	
Level 3 (Moderate)	🟨
Any Event and/or Security Incident not rated as "Level 6, 5, or 4" that warrants further analysis and/or investigation.	
Level 2 (Low)	🟩
Any Event that is NOT categorized as a Security Incident but has precursors of a Security Incident (i.e., someone reports a potential Security Incident that is determined to not be a Security Incident); these items need be logged.	
Level 1 (Very Low)	🟦
Any Event that is NOT categorized as a Security Incident and does NOT have any precursors of a Security Incident (i.e., someone reports a potential Security Incident that is determined to not be a Security Incident); these items may be logged at the discretion of the Incident Commander.	

6.4 Attack Vector

For the purpose of this S-IRP, the attack vector will aid during times of concurrent Incidents and to prioritize response efforts based on currently available information, the network architecture and level of sophistication

The Attack Vector for Security Incidents at a minimum needs to contain one of the following data points:

Vector	Summary and Notes
Attrition	An attack that employs brute force methods
Web	Websites or web-based applications
Email	Email message or attachment
External/Removable Media	Flash drives, Compact Discs (CDs), or other peripheral devices
Impersonation/Spoofing	Replacement of legitimate content/services
Improper Usage	Violation of acceptable use or other policies
Loss or Theft of Equipment	Electronic or physical loss of a computing device, media, or document
Unknown	Cause of attack is unidentified
Other	An attack does not fit into any other vector

6.5 Privacy Likelihood/Considerations (i.e. Informational Impact)

For the purpose of this S-IRP, each Security Incident will be evaluated for an Informational Impact to determine the likelihood of potential Privacy considerations. This will aid in the identification of which Security Incidents require the attention of the Legal Counsel to help evaluate any potential Privacy Notification requirements.

7 The SIRT

Senior Management established the SIRT to ensure centralized coordination of Incident Responses. The SIRT is comprised of technical and non-technical Company employees and contractors who are charged with prevention, identification, analysis, containment, eradication, recovery, and lessons learned of Security Incidents.

7.1 SIRT Charge

The SIRT is responsible for establishing, overseeing, and carrying out the plans of action for any Security Incident that potentially threatens the confidentiality, integrity, or availability of Company resources (both physical and electronic) and those owned and/or operated by Advisors to a certain degree. The SIRT will attempt to restore/recover information and/or systems to an operational state as quickly as possible while preserving forensic data. The SIRT will provide direction and support to the Company and its Advisors when responding to any Incident under its purview.

7.2 SIRT Objectives

The SIRT's main objectives are to protect and preserve information and computing resources to ensure the availability, integrity and, as required confidentiality, of Company information and computing resources.

There are five primary objectives of the SIRT:

1. Control and manage Security Incidents.
2. Timely investigate and assess the severity of Security Incidents.
3. Timely recover or bypass Security Incidents to re-establish normal operational conditions.
4. Timely notification of "Confirmed Incidents" with a "Level 6" rating to Senior Management, the Risk Oversight Committee (ROC) and/or ISSC.
5. Prevent or establish methods to better protect the Company and its Advisors from experiencing similar Security Incidents from occurring in the future to the extent possible.

8 SIRT Members

The SIRT members (also known as “Responders”) are an operational and diverse team that has specialized skills to investigate Security Incidents and recommending measures to correct or bypass problems or conditions relating to Security Incidents. The nature of Security Incidents will determine which parties are needed to assist with response efforts and implement preventative or corrective actions.

Permanent (Core) Members	**Supporting / SME** members (at the discretion of the SIRT) may include:
• Incident Commander • Incident Administrator • Anti-money Laundering (AML) Responder	• Internal Supporting Responders o Senior Reviewing Executive o Incident Coordinator o IT o Disaster Recovery (DR) o Communications o Risk and Compliance o Finance o Legal o Operations o Sales o Human Resources • External Supporting Responders o Qualified Security Assessor (QSA) o Forensic Computing Services Firm o Security Operations Center (SOC)

The core SIRT will be assisted by supporting responders who are Subject Matter Experts (SME) within their field. **These SMEs will only be informed about an incident at the discretion of the SIRT and thus informed of their responsibilities below**. SIRT members must conduct themselves following accordance with the following general objectives:

- Conduct objective, thorough, and timely investigations.
- Evaluate Security Incidents with a focus on individuals’ privacy rights.
- Collect, preserve, and protect data, documentation and materials related to the investigation.
- Maintain confidentiality around the investigation and/or Security Incident as required.
- Maintain thorough documentation of the entire investigation process.
- Safeguard data, documentation and materials related to the investigation materials and documentation.
- Maintain the chain of custody of investigation materials and documentation.
- Evaluate the underlying facts discovered by the evidence obtained in connection with an investigation of a Security Incident and present objective conclusions in Final Reports. Conclusions must be fully supported by facts discovered during an investigation of a Security Incident.
- Conduct a post-incident review of the investigation, and document policy or procedural issues that enhanced or hindered the Security Incident detection, monitoring, investigation, and subsequent development and implementation of corrective or problem bypass measures.
- Evaluate the business impact of any recommendations that are made to Senior Management.

8.1 Incident Commander

The CISO will serve as the Primary Incident Commander. The Deputy ISO will serve as the Secondary Incident Commander.

8.1.1 Responsibilities

- Activate the SIRT and as needed Supporting Responders
- Conduct SIRT meetings
- Coordinate SIRT investigations
- Classify Security Incidents according to Section 6 of this document
- Determine investigation objectives
- Coordinate SIRT training and exercises
- Finalize post-investigation documents
- Prepare reports, as needed
- Update the Senior Reviewing Executive regarding the status of an investigation as needed
- Recommend to the CEO whether information needs to be issued the general public, when requested
- Coordinate with law enforcement at the direction of the SIRT
- Deactivate the SIRT

8.2 Incident Administrator

The Incident Administrator will assist in a number of administrative functions and assist the Incident Commander and the Incident Coordinator as needed.

8.2.1 Responsibilities

- Take notes during meetings and document their actions to include the general actions of the SIRT
- Task management and tracking labor hours of SIRT members.
- Act as the repository for all Security Incident-related evidence upon deactivation of response efforts when directed by the Incident Commander with coordination by Legal Responders.
- Monitor the acmesecurity@acme.com mailbox Monday through Friday between 08:00am and 05:00pm and self-initiate Security Incident Intake Form as needed.
- Assist in finalize notification documents and mail such documents

8.3 Anti-Money Laundering Responder

The Anti-money Laundering (AML) responder will perform AML procedures as well as account reviews and block accounts as needed.

The AML Compliance Manager will serve as the Primary Anti-money Laundering Responder. The Regulatory Compliance Manager will serve as the Secondary Anti-money Laundering Responder. Both managers are members of the AML Committee in addition to the Chief Compliance Officer.

8.3.1 Responsibilities

- Coordinate with the Chief Compliance Officer and/or the AML Committee to determine whether any punitive or legal actions are recommended for any Advisor.
- Perform account reviews and block accounts as needed. Additional notification to internal staff may be performed in lieu of blocking accounts. This will be performed at the determination of the AML Compliance Manager or Regulatory Compliance Manager.
- Notify internal staff and/or departments in lieu of blocking accounts as needed.

8.4 Supporting Responders

Supporting Responders are not permanent SIRT members; however, these individuals may be asked to assist with a SIRT investigation because they have expertise in a particular subject matter. The Incident Commander and/or Incident Coordinator may request the assistance of Supporting Responders. If their assistance is required, they will become part of the SIRT for the particular investigation they are assisting with. The Incident Commander is the only SIRT member authorized to discontinue the assistance of the Supporting Responders.

8.4.1 Incident Coordinator Responders Core Responsibilities

The Incident Coordinator is responsible for resolving day-to-day production problems and leverages other support groups within the business such as the application support group.

The Head of Infrastructure will serve as the Primary Incident Coordinator. The Manager of Development Services will serve as the Secondary Incident Coordinator.

- Serve as the single POC to the Incident Commander for all technical actions.
- Identify and request supporting responders as needed.
- Assess the scope of the Security Incident damage, if any.
- Provide a systematic approach for technical actions when numerous technology platforms could be impacted by a Security Incident.
- Control and contain the Security Incident, to the extent possible.
- Collect, document, and preserve forensic evidence related to the Security Incident.
- Maintain a chain of custody for all computing evidence obtained during Security Incidents.
- Interview individuals who may have information relevant to the Security Incident.
- Identify root cause and/or source, the extend of the damage, and recommend counter measures or mitigation solutions to reduce or stop any additional damage.
- Conduct problem analysis to determine whether any failure in Company's Infrastructure or computing environment may have enabled the Event to occur.
- Audit mission-critical systems to ensure they are current with service packs and patches.
- Recommend solutions that are designed to aid in the prevention of similar Security Incidents from recurring in the future. All recommendations need to take into consideration the business impact that would be incurred if any recommendations are approved and implemented.
- Monitor recovery efforts.

8.4.2 Sr. Reviewing Executive Responders Core Responsibilities

A Senior Reviewing Executive will be indirectly involved during investigations of Security Incidents so he or she can provide impartial oversight to help protect the interests of the Company. If the Incident Commander is busy running the S-IRP, the Reviewing Senior Executive will provide Senior Management with any relevant updates regarding IR efforts.

The CCO will serve as the Primary Reviewing Senior Executive. The CIO will serve as the Secondary Reviewing Senior Executive.

- Update Senior Management and business managers as needed regarding the ongoing investigation and IR efforts
- Work with Senior Management to obtain the services of external resources as needed
- Prioritize the Security Incident within the Company, or direct more senior and/or capable leadership and/or resources to the IR efforts
- Provide objective oversight of the IR efforts
- Review reports generated by the Incident Commander as needed

8.4.3 Information Technology (IT) Responders Core Responsibilities

- Provide the necessary technical support to enable and effective response such as platform, application, database, and network support

8.4.4 Security Operations Center (SOC) Responders Core Responsibilities

- Serve as central POC for suspected Security Incidents derived from Company network traffic or Advisor networks that are externally reviewed through Managed Security Service Providers (MSSPs)
- Manage the day-to-day monitoring of resources and/or systems for potential security compromises

8.4.5 Qualified Security Assessor (QSA) Responders Core Responsibilities

- Serve as central POC for suspected Security Incidents involving cardholder and/or sensitive authentication data

8.4.6 Forensic Responders Core Responsibilities

- Oversee all Forensic investigation requirements and efforts performed by any third-party resources
- Provide expert guidance related to securing electronic or physical evidence procedures, when appropriate
- Provide expert forensic examination of computing resources and/or forensic images captured during response efforts
- Ensure all evidence was collected throughout the Security Incident's lifecycle from SIRT members upon deactivation of the SIRT
- Ensure the procedures for Digital Evidence Chain of Custody are followed by the SIRT

8.4.7 Disaster Recovery (DR) Responders Core Responsibilities

- Maintain awareness of the situational throughout the entire IR lifecycle for affected technologies identified within the Company's Disaster Recovery/Business Continuity (DR/BC) Plan.
- Coordination with affected technology groups to ensure they are capable of rapid transition to DR/BC mode.
- Assess each affected piece of technology to determine a solution in the event any physical assets must be seized by or provided to Law Enforcement (LE).

8.4.8 Communications Responders Core Responsibilities

- Serve as the POC for all requests for information from any source.
- Coordinate the release of information to the public
- Provide ongoing advice and awareness regarding the release of communications or documents to the public.
- Manage crisis communications to limit exposure to the Company and its Advisors
- Create and distribute internal communications for Company to help manage the impact of public awareness of Security Incidents.
- Assist in drafting and finalizing notification documents with the Legal Responder and Incident Administrator.

8.4.9 Risk and Compliance Responders Core Responsibilities

- Ensure that all statutory and contractual obligations are met in a timely manner.
- Perform Internal Controls evaluation.
- Facilitate policy updates and/or changes as needed.
- Provide ongoing advice and awareness regarding the release of communications or documents to regulators and/or law enforcement.
- Ensure all reporting requirements are addressed by the SIRT for SEC, FINRA, Federal, State, and Local Laws.
- Identify and track Risks as well as Issues and Corrective Actions.
- Evaluate Incidents as needed as part of the ROC bi-monthly meetings.

8.4.10 Finance Responders Core Responsibilities

- Ensure that all Sarbanes-Oxley Act (SOX) requirements are met during the lifecycle of the Security Incident such as evidence tampering and whistleblower protections
- Analyze cost savings and/or reforecast budgets if emergency funding is needed
- Track expenses during the lifecycle of the Security Incident

8.4.11 Legal Responders Core Responsibilities

- Provide ongoing legal counsel during Security Incidents

- Evaluate legal privacy implications of Security Incidents
- Evaluate SIRT actions to take into consideration post-event litigation and/or criminal prosecution
- Aid in the determination of whether to notify law enforcement. Serve as the liaison to law enforcement if it becomes involved in the investigation of Security Incidents.
- Provide guidance regarding other legal and contractual obligations stemming from Security Incidents.
- Draft and finalize notification documents with the assistance of the Incident Administrator and Communications Responder.
- Notify Insurance Carriers and keep them informed on the progress of the Security Incident.

8.4.12 Operations Responders Core Responsibilities

- Evaluate the operational impact of Security Events based on Advisor and Company Constituencies needs; update SIRT as needed.
- Liaise with outside entities such as clearing firms, banks, and regulators.
- Perform general field support
- Recommend the addition of additional controls and/or processes as necessary with coordination from Risk and Compliance Responders.
- Implement additional controls and/or processes upon approval by Senior Management or Risk Management.

8.4.13 Sales Responders Core Responsibilities

- Evaluate the potential business impact of SIRT response efforts and provide this information to the SIRT.
- Work with Disaster Recovery Responders to coordinate between IT and affected business unit(s) in the event of a disruption to the business operations that may require a Disaster Recovery / Business Continuity action.

8.4.14 Human Resource Responders Core Responsibilities

- Handle all employment related circumstances resulting from Security Incidents

8.4.15 Law Enforcement Responders Core Responsibilities

- Serve as central POC for suspected Security Incidents when law enforcement notification is required (criminal activity for federal, state, local, and international laws).

8.5 Help Desk

The Help Desk will serve as the central POC for reporting Security Incidents. The Help Desk will be available (Monday through Saturday 06:00am – 07:00pm and Sunday 07:00am – 04:00pm) for communications and Security Incident Reporting. Additionally the Incident Administrator will serve as an additional POC by monitoring the acmesecurity@acme.com mailbox Monday through Friday between 08:00am and 05:00pm.

8.5.1 Responsibilities

- Monitor Acme computing resources for reports of suspected and/or confirmed Security Incidents
- Complete Security Incident Intake Forms and select the appropriate severity level.
- Notify the Incident Commander upon completion of Security Incident Intake Forms or as soon as reasonably practicable
- Email completed Security Incident Intake Forms to the Incident Commander as directed by the Incident Commander.
- Receive calls from Advisors on potential Security Incidents.

8.6 Employees, Advisors, etc.

Anyone who observes and/or is informed of a suspected or confirmed Security Incident is responsible for reporting such information immediately.

8.6.1 Responsibilities

- Report suspected or confirmed Security Incidents within 2 hours of obtaining information or as soon as reasonably practicable. See sections 3.4 and 5.3.3 for more information on how to report.

9 Security Incident Tracking

The SIRT will log, track and document the investigation and resolution of all Security Incidents by submitting a Security Incident Intake Form at https://incidentintake.acme.com. Data for a particular Security Incident will only be available to the SIRT members, and upon request and/or approval of the CISO and/or CCO.

Security Incidents will follow the following lifecycle status:

- Initial (Indicates the ticket is in the initial detection and reporting process)
- Follow-Up (Indicates the ticket is ready for the CISO and/or Deputy CISO to review)
- Secondary (Indicates the ticket is ready for the SIRT to review)
- Collection (Indicates the ticket is ready for Containment, Eradication and Recovery efforts)
- Closed (Indicates the Core SIRT has agreed the matter as closed)

Process to log a new Security Incident Intake Form:

1. Navigate to https://incidentintake.acme.com
2. Click on “Create New”
3. Enter all required information for all tabs
   a. You may select “Save for Later” to come back at a later time
   b. You will also be presented a warning message in the event all required fields are not completed
4. Click “Submit” to send the form to the next stage for review

Process for Follow-Up and Secondary Analysis:

1. Navigate to https://incidentintake.acme.com
2. Click on “Edit Incident” for the appropriate Security Incident
3. Enter all required information for all tabs
   a. You may select “Save for Later” to come back at a late time
   b. You will also be presented a warning message in the event all required fields are not completed
4. Click “Submit” to send the form to the next stage for review

Process for Collection:

1. Navigate to https://incidentintake.acme.com
2. Click on “Edit Incident” for the appropriate Security Incident
3. Click on “Attachments” and navigate to the appropriate section
4. Enter information for all required fields
5. Click “Submit” to save your information
6. Repeated steps 3, 4, and 5for all appropriate sections

10 Security Incident Closure

Once the affected systems or resources have been returned to normal operations, the SIRT will verify that all corrective and/or preventative tasks are complete and that local services have been restored. In cases where Security Incident response efforts are partially outsourced to third-parties, the Incident Commander will monitor and document the Security Incident resolution.

If a Security Incident is rated as a “Confirmed Incident” with a “Level 6 or 5” severity, the Incident Commander must obtain approval from the SIRT to close the Security Incident.

Process for Closing

1. Navigate to https://incidentintake.acme.com
2. Click on “Edit Incident” for the appropriate Security Incident
3. Click on “Attachments” and navigate to the “Incident Closure Form”
4. Enter information for all required fields
5. Click “Submit” to save your information
6. Click “Browse Existing”
7. Select the drop down arrow next to “Edit Incident” for the appropriate Security Incident
8. Click “Close Case”
    a. You will be presented the following message “You are attempting to close this incident. This action cannot be undone and will mark all aspects of the incident as read only. Are you sure you want to close the incident?
9. Select the “Ok” to close the Security Incident

At any time the CISO, CCO, or Chief Executive Officer (CEO) may terminate a Security Incident investigation, regardless of Security Incident severity rating. If a Security Incident is turned over to a law enforcement agency, the SIRT investigation will, in most cases, be suspended; however the CISO and Legal Counsel will attempt to obtain updates from Law Enforcement regarding the matter.

Prior to closing any Security Incident involving potential disclosure of NPPI, PII, or other information that was deemed to not constitute NPPI or PII, the Legal Responder needs to conduct a follow up review of the conclusion to confirm that the information involved has been correctly categorized.

10.1 Final Reports

The SIRT prepares Final Reports. These reports (electronic and physical) are maintained by the CISO.

10.2 Third-Party Reports

The Incident Commander and/or SIRT must confer with Legal Responders prior to engaging any third-party vendor that may produce third-party reports. Any report that is prepared by a Qualified Security Assessor (QSA) or an outside computing forensics firm must be addressed to Legal Counsel and marked as “Attorney-Client Privileged and Work Product Protected.”

11 SIRT Training

Core SIRT members will receive incident response training as needed. The CISO and Legal Counsel need to provide input in advance of any training to ensure the incident response training elements are current.

The following training topics need to be considered in the training venue:

- State and Federal Privacy Law
- Company Polices relevant to recent security incident trends
- Best practices for conducting incident handling and investigations
- Best practices for evidence preservation.
- Hardware and software tools used by the SIRT

11.1 Advanced Training and Skills Requirements

Incident Commanders, Coordinators, and Administrators may be required to complete additional training to ensure Incident Handling processes meet industry acceptance as an Incident Handler.

12 SIRT Exercises

The SIRT will conduct an annual exercise that simulates a Security Incident. The purpose of the exercise will be to maintain the skills and knowledge of the SIRT members. Exercises will involve all core SIRT members and Supporting Responders will be selected to participate as required by the nature of the exercise. At the conclusion of the exercise, the Incident Commander in coordination with the SIRT members will prepare a brief report to distribute to the ISSC and ROC evaluating the exercise within 30 days of completion. Any skill and/or knowledge area that needs to be improved as well as procedural enhancements will be identified in the report.

13 Security Incident Metric Reporting

The reports identified in this section will be generated based on information within the Security Incident tracking system. Where possible, these reports will be generated and distributed automatically:

- **Annually – ID Theft Prevention Status Report**: Security Incident Metric Reporting and data from the Security Incident tracking system will be utilized to supplement the Firm's ID Theft Prevention Program and the reporting requirements as follows (the following portion was taken from the ID Theft Prevention Program Document):

> *Our firm is responsible for developing, implementing and administering our ITPP and will report annually to Senior Management on compliance with the FTC's Red Flags Rule. The report will address the effectiveness of our ITPP in addressing the risk of identity theft in connection with covered account openings, existing accounts, and service provider arrangements, significant incidents involving identity theft and management's response and recommendations for material changes to our ITPP. Acme will document and report on the effectiveness of ID Theft Prevention Program activities utilizing the annual ID Theft Prevention Status Report. The report will include:*
>
> - ➢ *Significant incidents (# of incidents, victims impacted and exposure) involving identity theft and management's response*
> - ➢ *Identity theft control and operating procedure effectiveness*
> - ➢ *Summary of service provider arrangements including any changes to Service provider arrangements*
> - ➢ *Summary of recommendations for material changes to the program*
>
> *This annual program performance report will be issued by the Risk Management department by January 31 of each year.*
>
> *Acme Compliance is responsible for reporting to Acme Senior Management on the effectiveness of the Program and on the general state of ID Theft within the firm. As a result, the ID Theft Prevention Status Report will be issued and incorporated into our Annual CEO Certification Process that is reviewed with Senior Management.*

13.1 Out-of-band Communications

While the SIRT may provide status updates, it may need to prepare for multiple communication methods, particularly out-of-band communications (e.g., in person, paper). This is necessary in some instances where systems may be compromised that would give intruders an advanced warning that a Security Incident has been identified and that Security Incident response efforts were underway. The Incident Commander will determine if out-of-band communications are necessary prior to activation of the SIRT and thereafter as needed.

13.2 Board of Directors Reporting

All Security Incidents rated as “Confirmed Incidents” with a “Level 6” severity rating will be presented to the Acme Board of Directors no less than annually by the CISO or CCO and included in the annual CEO Certification process.

13.3 Collecting Security Incident Data

Collecting data during Security Incidents will help enhance the Information Security program. The information gathered may: (i) indicate the existence of systemic security weaknesses and threats; and (ii) evidence changes in Security Incident trends, which could feed into the Enterprise Risk Assessment process and lead to the implementation of additional controls.

The following metrics at a minimum must be collected by the Incident Administrator:

- Number of Security Incidents broken down by incident levels that were handled on an annual basis.
- Each SIRT member must track the time spent on each Security Incident and relay this information to the Incident Administrator.
- The lifespan of a Security Incident from the time of discovery through the lessons learned.
- Length of time it took the SIRT to respond to the initial report from the detector?
- Identify recurring Security Incidents.
- Estimate monetary damages stemming directly from Security Incidents.

14 Security Incident External Reporting

Reporting Security Incidents externally may be required. Every Security Incident needs to be evaluated in this regard.

14.1 Insurance Reporting

The SIRT must consult with Legal Counsel for any “Confirmed Incidents’ with a “Level 6 or 5” severity to determine whether the matter must be reported to any of the Company’s Insurers.

14.2 Suspicious Activity Reporting

The Company’s obligations to file a suspicious activity report (SAR) and/or to notify appropriate law enforcement authorities are set forth in the Company’s Bank Secrecy Act / Anti-Money Laundering (AML) Internal Compliance Program. The AML Responder will initially determine (or the Regulatory Compliance Manager as the delegate) whether a Security Incident triggers the completion of a SAR and bring to the AML Committee for additional review and/or discussion. The AML Responder will consult with the Legal Responder where applicable and receive support from the CISO to ensure the appropriate technical data (IP addresses, hash values, registrar information, etc.) is included in the reporting process.

14.3 Constituent Notification

Certain Security Incidents will require notification to Company Constituents. The SIRT will consult with the Legal Responders to provide factual information regarding Security Incidents. Legal Responders will determine whether any notifications (e.g., privacy or regulatory) are required in accordance with applicable laws and regulations and the manner in which notifications must be made, draft and finalize notification documents, and assist in mailing such documents along with the assistance of the Incident Administrator and Communications Responder

14.4 Payment Card Industry Reporting

A certified QSA may need to be consulted in order to identify specific requirements and steps for reporting suspected and/or confirmed Security Incidents involving cardholder data and/or sensitive authentication data as they are specific to each payment card brand.

The specifics can be found at the following locations:

Brand	Additional Information
Visa	http://usa.visa.com/merchants/protect-your-business/cisp/if-compromised.jsp http://usa.visa.com/download/merchants/cisp-what-to-do-if-compromised.pdf
MasterCard	http://www.mastercard.com/us/merchant/pdf/Account_Data_Compromise_User_Guide.pdf
Discover	https://www.discover.com/credit-cards/member-benefits/security-center/keep-secure/understand-fraud.html
American Express	https://www209.americanexpress.com/merchant/services/en_US/data-security?intlink=US

14.5 Credit Monitoring

The SIRT will consult with Legal Responders to determine whether a Security Incident triggers a legal requirement to provide credit monitoring to Company Constituents who are impacted by a Security Incident.

If a Security Incident was triggered by an Advisor’s actions and credit monitoring is required, the CCO may require Advisor’s to pay for all credit monitoring services provided to his or her clients. The Legal Responders, with the assistance of Incident Administrator and Communications Responder will draft and finalize all notification documents which may include credit monitoring details. The Incident Administrator is responsible for mailing all notification documents. See the Acme ID Theft Referral Procedures for details.

14.6 Claims for Reimbursements

The SIRT must consult with Legal Counsel to determine whether any of the Company’s Insurers will reimburse Company for expenses incurred as a result of Security Incidents.

14.6.1 Reimbursement Request by an Affected Constituent

Whenever a Security Incident occurs, an affected Company Constituent may ask the Company to cover expenses (or reimbursement) related to the Security Incident. The Company may by law, rule and/or regulation be required to reimburse the requesting Constituent. If reimbursement is not required, the Company may choose to reimburse an affected Constituent for his or her entire, and/or portion of the, loss suffered as a direct result of the Security Incident. The determination as to whether such voluntary reimbursement will occur will be made by Senior Management, with the advice of Legal Responders.

14.6.2 Company Reimbursement or other Request

The SIRT is required to keep track of all expenses incurred as a result of a Security Incident and provide this information to the Finance Responder and Legal Responders.

The Legal Responders will review all relevant insurance policies and contracts to determine the appropriate method for obtaining reimbursement for expenses and liabilities stemming from Security Incidents. Legal Responders will provide this information to Senior Management to determine the best course of action for seeking these funds.

15 External Information Sharing

The sharing of information and threat intelligence aids the financial community as a whole. Customer’s trust may be lost if Security Incidents occur. Therefore efforts need to be made to minimize the impact to consumer trust thus the sharing of information. The CISO or Incident Commander will review all information prior to being shared.

15.1 InfraGard

InfraGard is a partnership between the Federal Bureau of Investigations (FBI) and the private sector dedicated to sharing information and intelligence to prevent hostile acts against the United States and the 16 critical infrastructures that make up the backbone of United States (U.S.) economy, security, and health stemming from Presidential Policy Directive 21 (PPD-21) on Critical Infrastructure Security and Resilience.

The FBI has developed Malware Investigator as a resource that Incident Handlers can submit suspected malware files and within as little as an hour, receives detailed technical information about what the malware does and what it may be targeting. The Malware Investigator is only available through established FBI partnerships such as InfraGard.

15.2 Financial Services Information Sharing and Analysis Center

The Company is a current member of the Financial Services Information Sharing and Analysis Center (FS-ISAC) which is dedicated to providing collaboration for critical security threats facing the global financial services sector and sharing cyber and physical threat intelligence. Coordination with the FS-ISAC is recommended by the U.S. Department of Treasury, the lead agency for the Financial Service Critical Infrastructure identified in PPD-21.

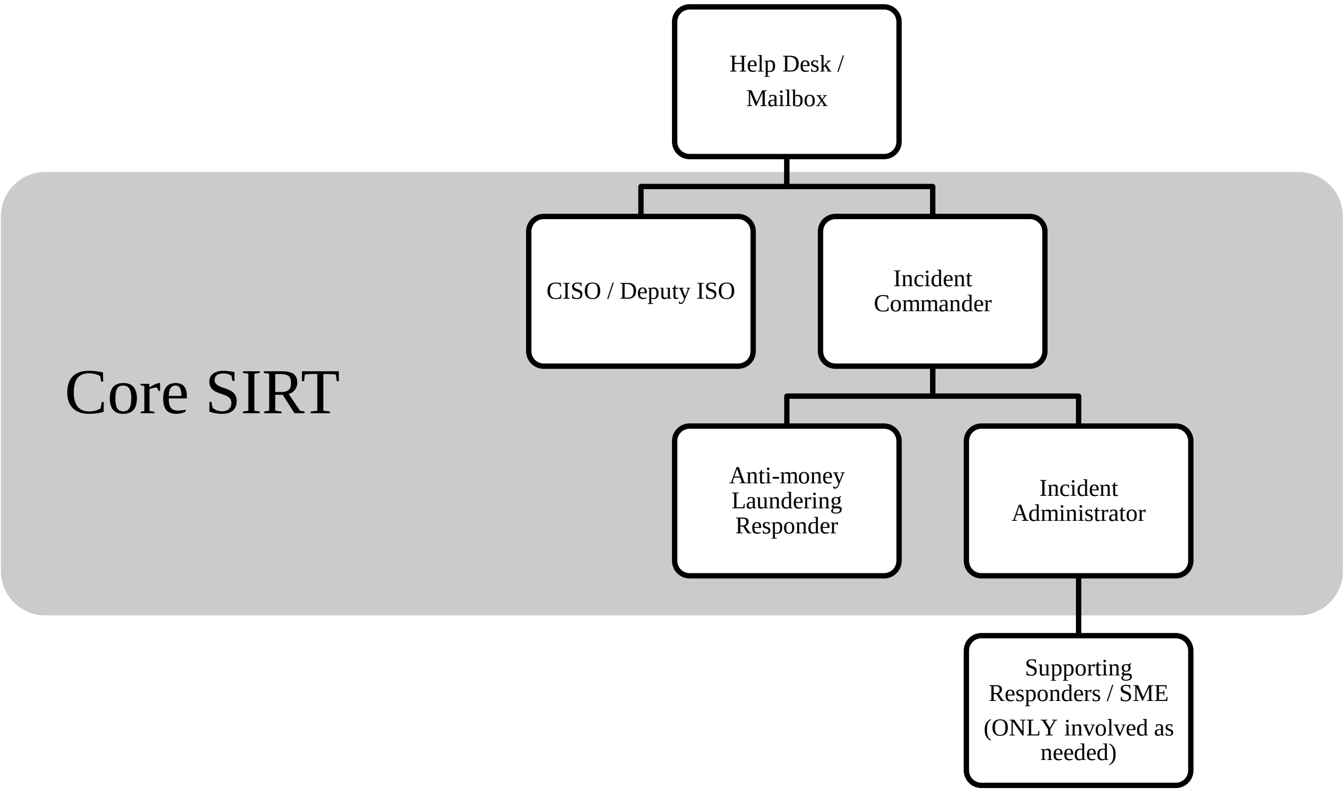
15.3 Data Sets To Consider For Sharing

The following data sets need to be considered for distribution to those entities listed within this section:

- Malicious payloads and hash values
- Attacking IP addresses and associated domain names
- Command and Control IP addresses and associated domain names
- Dropper IP addresses and associated domain names
- Threat vector and associated vulnerability exploit

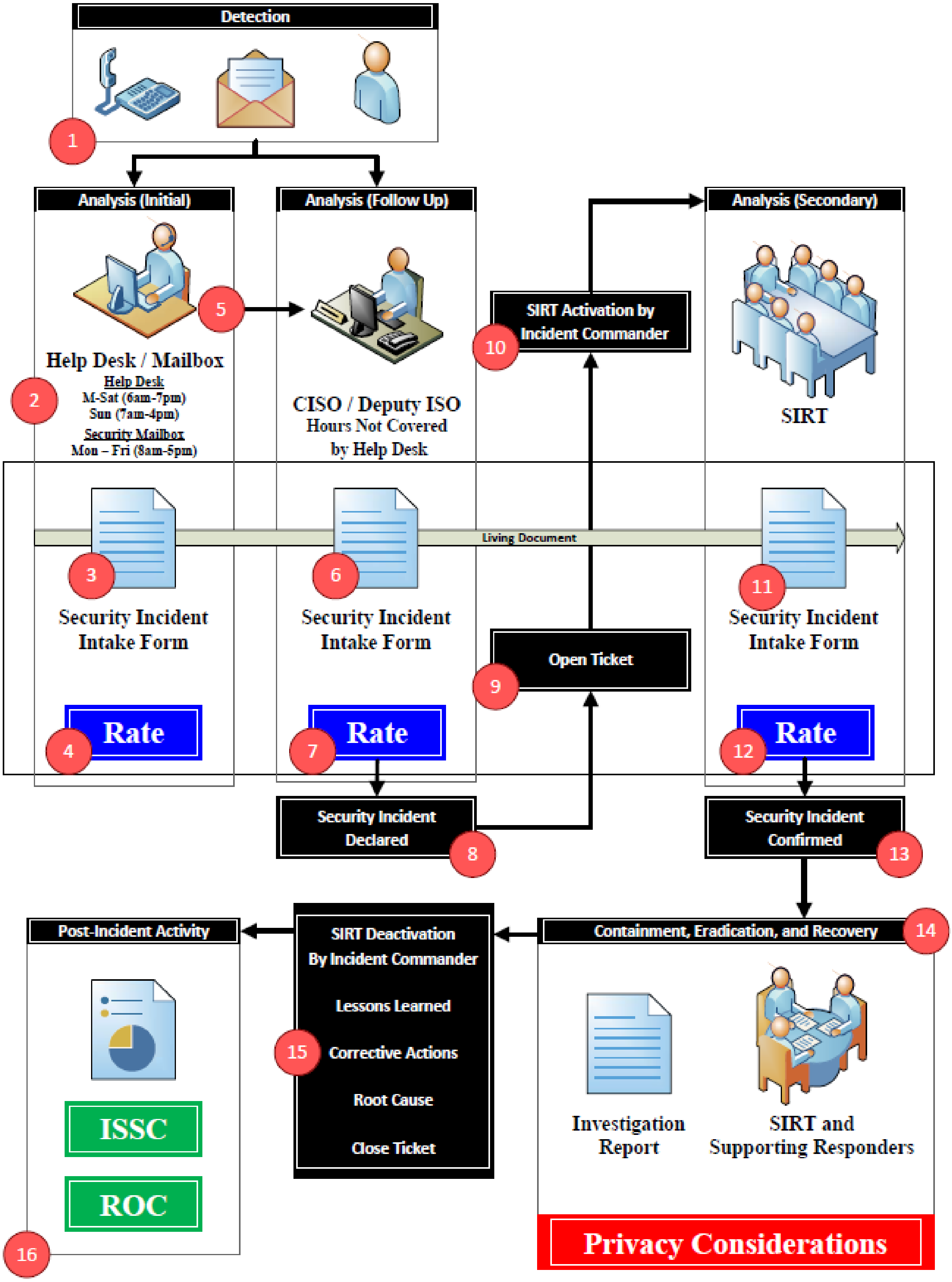
16 SIRT Organizational Structure

The following diagram represents the makeup of the SIRT and the designation of the core SIRT



17 Workflow Activity

The following diagram depicts the flow of activities regarding the escalation of an Event.


Detection
1
Analysis (Initial)
Analysis (Follow Up)
Analysis (Secondary)
5
Help Desk / Mailbox
Help Desk
M-Sat (6am-7pm)
Sun (7am-4pm)
Security Mailbox
Mon – Fri (8am-5pm)
2
CISO / Deputy ISO
Hours Not Covered
by Help Desk
SIRT Activation by
Incident Commander
10
SIRT
Living Document
3
Security Incident
Intake Form
6
Security Incident
Intake Form
11
Security Incident
Intake Form
Open Ticket
9
Rate
4
Rate
7
Rate
12
Security Incident
Declared
8
Security Incident
Confirmed
13
Post-Incident Activity
SIRT Deactivation
By Incident Commander
Lessons Learned
15
Corrective Actions
Root Cause
Close Ticket
Containment, Eradication, and Recovery
14
Investigation
Report
SIRT and
Supporting Responders
ISSC
ROC
16
Privacy Considerations