NASAA
Cybersecurity Committee

Incident Response Tips for Investment Firms

Acknowledgements

We would like to extend our sincere gratitude to the following individuals for their invaluable contributions to this paper:

John Yaros (ID)
Aaron Rodebeck (IN)
Rosemary Gonzalez (NJ)
Philip Carey (OK)
Grant Loyle (WA)
Erica Stebbins (CT)

NASAA Cybersecurity Committee Members:

John Yaros (ID)
Aaron Rodebeck (IN)
Rosemary Gonzalez (NJ)
Philip Carey (OK)
Grant Loyle (WA)
Erica Stebbins (CT)
Dan Klukas (KS)
Matthew Libby (MA)
AJ Sipherd (NE)
Fennie Wang (NY)
Kit Chao (CA)
Sasha Andersen (AZ)
Nicole West (DC)
Clay Johnson (KS)

NASAA
Cybersecurity Committee
Incident Response Tips for Investment Firms

Introduction to Incident Response

Every investment firm connected to the internet is a potential target for illicit cyber actors, which makes having an incident response plan critical to the survival of any firm that becomes a victim. Successful cyberattacks and breaches can lead to a chaotic situation for a firm unless they have a reliable incident response plan in place to provide a structured approach for responding, managing, and mitigating cybersecurity incidents that will limit the damage of an attack.

The longer a cyber incident persists, the more damage an illicit actor can inflict on a victim's financial assets, business operations, and reputation. An incident response plan enables a firm to take swift effective action that can help protect their business and clients from worst case scenarios. The development of a strong incident response plan can limit the disruption value of a cyberattack and help restore business operations in a timely manner to the frustration of illicit actors and the benefit of a firm and its clients.

By creating and periodically updating a cyber incident response plan, a firm can incorporate best practices that will prepare them to effectively protect their assets and operations. An investment firm's incident response plan should account for potential cyber risks/vulnerabilities and layout comprehensive processes and procedures that will act as a blueprint for responding to various types of known cyberattack methodologies.

Communication

When a cybersecurity incident occurs, it is essential for a firm to have a plan in place that defines employee roles and responsibilities for incident response. The following key steps should be taken:

- Prior to an incident, define who will execute the incident response plan and identify the Security Incident Response Team (SIRT) – the team that will handle and resolve any security incidents, "Occurrences that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies"[i], whether internal and/or external.
- Use the Security Operations Center (e.g., Helpdesk or Hotline) to act as the first line of defense in a cybersecurity incident since their role is to work and conduct triage for cybersecurity incidents.
- Ensure that there is a Security Incident Manager (SIM) available to facilitate incident response with key stakeholders.
- Depending on the size of a firm, either a Chief Technology Officer ("CTO") or another party (internal or external) should be accessible to provide expert technical analysis.
- A SIRT contact list should be created that contains all relevant contact information (e.g., office number, mobile number, and email address etc.) for communication purposes.
- Communication is vital for classifying incidents as low, medium, or high security threats. Each classification should have its own processes and procedures for communicating essential information.

Information sharing is crucial to a successful incident response strategy. A firm needs to circulate key incident information, both internally and externally, to relevant stakeholders to ensure situational awareness and carry out an effective incident response strategy. This will help a firm prevent, mitigate, and recover from a harmful cyberattack. An incident response plan should have information sharing mechanisms in place that address:

Updating Staff and Legal Stakeholders- Any incident response plan should develop information sharing processes for informing staff of an incident and to inform them of their roles and responsibilities during the event. It is also important for a firm to have their legal team receiving necessary information to best protect the firm and its clients.

Contact Law Enforcement, Regulators, and Support Agencies- Firms should know how and when to contact key law enforcement partners such as the Federal Bureau of Investigations, Secret Service, and state/local police to help investigate cybercrimes. Furthermore, federal/state financial regulators and other operational support agencies such as the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency should be brought in for support to better protect the firm and its clients.

Public Relations Strategy- Engaging with the public is often critical for firms to maintain the trust of their clients and to protect against the reputational harm a cyber incident can cause. Firms should look to:

- Prepare holding statements for the media.
- Monitor media, message boards, and social media for information and misinformation relating to the incident.
- Adapt messaging to develop short, medium, and long-term messaging as required to address the incident.
- Decide when, how, and if to disable a firm's website and/or other information sharing channels to prevent further damage.[ii] [iii] [iv]

Redundancy

Redundancy seeks to make sure there are no single points of failure in an office IT environment. Cybersecurity redundancy is crucial in safeguarding data integrity and operational continuity against potential threats and disruptions. Below are four implementable practices that firms can apply to enhance their preparedness if a data breach or cybersecurity incident occurs.

Retain Synchronized Data in Multiple Locations – Synchronizing copies of data across multiple locations within a database or storage system ensures that in case of data corruption or loss, a redundant set is readily available for seamless restoration. This redundancy not only enhances data availability but also mitigates risks associated with localized failures or cyber-attacks targeting specific data repositories.

Implement a Data Backup Strategy – To enable business continuity during a cyber incident it is important to have and maintain access to relevant data. By keeping multiple copies of data on various storage devices/media and ensuring that the data is in different locations a firm can protect itself from losing access to the data it relies upon for business operations. A simple and time-tested strategy to start with is the 3-2-1 backup rule that encourages a firm to maintain three copies of its data on two types of storage devices/media with one copy being offsite and perhaps offline.

Redundant Power Supply for Servers - A firm may wish to have a redundant power supply for its servers to ensure business operations are not interrupted due to a cyber incident or in the event that its primary power supply malfunctions. Internal servers store critical client data and financial information, which can make downtime costly in terms of lost productivity and client confidence. By investing in a redundant power supply system, the firm protects against power outages or failures in its primary power source.

Use Virtual Machines to Continue Digital Operations - Leveraging virtual machines that can be brought online quickly can be crucial in maintaining operational continuity and data security. Having access to a virtual machine system can enable a firm to replicate their computing environment in a virtualized form, ensuring that critical applications and data remain accessible even in the event of a hardware failure or other type of compromise. Using a virtual machine may provide a firm with the ability to recover from hardware failures, cyberattacks, or other unforeseen disruptions, thereby minimizing downtime and potential data loss.

By adopting these cybersecurity redundancy practices, firms can defend against cyber threats, ensuring robust data protection, operational continuity, and rapid recovery capabilities in the event of a data breach or cybersecurity event. By prioritizing redundancy measures, firms can safeguard their assets, maintain user trust, and sustain operational resilience in an increasingly interconnected digital landscape.

Containment

An incident response plan is critical for managing cyber incidents and mitigating potential damage to sensitive data and vital digital infrastructure/assets. The containment phase of incident response helps prevent the spread of threats from one area of a firm's network/information technology (IT) framework to another.

A recent study highlights that nearly 46% of organizations are unable to contain a threat in less than thirty minutes after an initial compromise, and over 90% of respondents are not fully confident that their organization is able to identify the root cause of a cyberattack.[v]

When under attack there are three important goals in the containment phase that a firm should look to achieve:

- Prevent damages or losses to IT assets.
- Isolate any compromised systems.
- Identify & determine the extent of the breach.

To properly contain a cybersecurity incident a firm should develop processes and procedures that account for the following:

1) Activate a Communications Strategy to Respond Quickly

Inform Key Personnel- When taking actions that impact critical operations, such as shutting down systems or disconnecting networks, make sure to communicate with key stakeholders. It is imperative that everyone is aware of the situation and their roles and responsibilities during the incident.

Act Swiftly- In urgent situations, a firm's incident response plan should be activated immediately, and SIRT members should communicate with each other as quickly as possible to take action in an effort to protect critical systems and sensitive data.

2) Customize Plans for Different Attack Methodologies

Understand the Incident- Different incidents require different containment strategies. For example, handling email-borne malware differs from dealing with a Distributed Denial of Service (DDoS) attack. It is critical to prepare and understand how to respond to various types of incidents.

Identify an Appropriate Response- Upon gaining an understanding of the incident the SIRT should activate a plan that accounts for:

- Potential Damage: Assess the possible damage and theft of resources.
- Evidence Preservation: Determine the need to preserve evidence for an
- investigation.
- Service Availability: Consider the impact on the firm's services and clients to determine if a contingency plan needs to be put into action.
- Resources and Time: Evaluate the time and resources needed to implement
- the containment strategy and adjust as necessary.
- Effectiveness: Aim for either partial or full containment, depending on what
- is feasible and most effective.
- Solution Duration: Decide whether the solution will be an emergency
- workaround, a temporary fix, or a permanent resolution.

3) Seek to Eradicate the Threat

Identify and Remove Threats- Once an incident response plan is activated for a specific threat a firm should:

- Identify the Specific Components of the Attack: Start by identifying all parts of the incident, such as malware or breached user accounts. Once the components are analyzed a firm can develop an eradication strategy.
- Document Everything: Keep a detailed record of what the firms finds. This helps in tracking the eradication process and ensuring nothing is overlooked.
- Remove Threats: Focus on eliminating identified threats. This might involve deleting malware, disabling compromised accounts, and addressing any other components of the incident.
- Address Vulnerabilities: After removing the threats, look for any vulnerabilities that were exploited and fix them to prevent future incidents.

Adapt to the Situation- Cyberattacks are fluid situations and will require adjustments that will make it vital to have a decision-making process in place. The SIRT should determine and implement an eradication strategy. Some incidents might not require full eradication, or the eradication might take place alongside recovery efforts. Be flexible and adapt your approach based on the specifics of the incident.

4) Establish Recovery Measures

It is important for a firm to have a plan in place for restoring its operations to ensure critical functions and services are brought back to life in a responsible, cautious, and timely manner. To recover properly the following steps should be taken:

A) System Restoration

Focus on Critical Systems- After understanding the extent of the damage, a firm should start its recovery by restoring its most critical systems and services to ensure essential operations are up and running as soon as possible. Critical systems and services should already be identified in a firm's incident response plan.
Verify System Functionality- As you restore each system, confirm that it is functioning correctly before moving on to the next one.

B) Enhance Security

Apply Updates and Patches- Ensure systems receive the most recent patches and security updates to close vulnerabilities and attack vectors. This will help prevent similar cyber incidents in the future.

Review and Strengthen Security Measures- Analyze how the cyber breach occurred and ensure that security measures are updated accordingly. This could include updating firewall rules, changing passwords, and tightening access controls.
Monitor Systems Closely- Keep a close watch on your systems for any signs of recurring issues or new threats. Illicit cyber actors may use malware or other tools to maintain or gain access/control over systems within a firm.

C) Learn and Improve
Conduct a Post-Incident Review- After an incident, review the facts to identify what exactly happened and why. Additionally, a firm should review its incident response to identify potential improvements. This analysis helps to improve future responses.
Update Policies and Procedures- Use incident findings to update a firm's incident response policies and procedures to better handle similar situations in the future.
Provide Training and Raise Awareness- Ensure that members of a firm and SIRT understand any new processes and procedures being implemented and provide necessary training. This is critical for efficient and effective responses to future cybersecurity incidents.

These containment steps will help provide a structured approach for containing a cyber incident that will help minimize business disruptions while protecting critical assets. [vi]

Third-Party Dependency Risks

Firms often depend on third-party vendors, technology platforms, and tools to accomplish their goals, and an incident response strategy needs to account for these dependencies. By taking inventory of third-party risks and developing a plan to address them a firm can better protect itself and its clients. Account takeover (ATO) and cloud risks are some key third-party dependency risks firms should account for in their operations.

ACCOUNT TAKEOVER RISKS

Many investment firms/advisers conduct transactions on third party brokerage platforms making it important for them to prepare for potential account takeover (ATO) attacks in which bad actors gain unauthorized access to financial accounts. ATO schemes often involve illicit actors using compromised customer information (e.g., logins and passwords) to access bank/brokerage accounts for the purpose of conducting illegitimate funds transfers, retail purchases, and trading activity. Bad actors use various online methods to acquire customer information for ATOs including software exploits, phishing emails/text messages, malware, trojan horses, social engineering schemes, and other techniques.

Here are some actions all firms/advisers should take to protect against ATOs:

- Strong and Frequently Updated Private Passwords- Passwords should be at least 8 characters long and use a mix of letters, numbers, and special characters. Passwords should not be shared and should be changed periodically.
- Use Multi-Factor Authentication- Using multiple forms of authentication provides another layer of protection from illicit actors.
- Install Antivirus/Spyware Software- These types of software can help identify and protect against potential vulnerabilities and malware threats.
- Update Software- Make sure the most recent security patches are implemented to protect against vulnerabilities and exploits from cybercriminals.
- Don't Click on Links or Download Files/Software from Unknown Sources- Phishing and malware schemes depend on these actions.
- Confirm Secure Web Connection for Financial Accounts- During logins make sure the website starts with https:// and has a closed padlock on the status bar.

Here are actions that should be taken if an ATO occurs:

- Contact Financial Platform- The financial platform where an ATO occurs should be made aware immediately, so they can freeze/close the account(s) and limit damage.
- Alert Clients- Once an ATO occurs a bad actor may have access to contacts or business associates and attempt to conduct further criminal actions.
- Review Financial Activity and Accounts- Identify what activity is potentially fraudulent and make sure other financial accounts are not affected.
- Change Passwords- When accounts are compromised it is critical to change passwords immediately to limit a bad actor's access to accounts.
- Check Credit Reports- Identify potential suspicious activity/fraudulent accounts and seek to have them frozen or closed.[vii]

Cloud Risks

Cloud computing is an essential part of business operations for most investment firms/advisers, but the convenience firms receive from being able to store and access their data from anywhere creates cyber risks. To prepare and respond to the risks posed by cloud computing investment firms/advisers should:

- Understand Security Responsibilities and Implement Strong Authentication- Be aware of customer data, device, and identity responsibilities in the cloud and ensure that multi-factor authentication is in place.
- Inventory Data and Implement Encryption- Know where sensitive data is located and ensure that data is encrypted when resting or in transit.
- Change Passwords Immediately- When a breach occurs seek to change passwords to better protect data as the cloud provider works to isolate the breach.
- Take Incident Notes and Keep Offline Data Backup Available– Take notes of everything that happens during an incident (e.g., screenshots) and make sure that data backups are readily accessible both online and offline.
- Know Reporting Procedures for Cloud Service Providers and Clients- Know where and how to report incidents to cloud providers and how to communicate breaches to clients. This should be part of a firm's/adviser's incident response plan.[viii]

These steps can help a firm protect itself from third-party dependency risks pertaining to ATOs and cloud solutions that will protect the firm, its clients, and sensitive information from illicit cyber actors.

Incident Response Plans are Crucial for Protecting Investment Firms

In order to make timely decisions, maintain business operations, and safeguard sensitive information during a cyber incident it is important for firms to develop and implement an incident response plan and strategy. Incident response plans should act as living documents and be updated periodically to address new risks and potential vulnerabilities. Successful cybersecurity incident response plans should address the following:

- Communication- A firm must define internal and external roles and responsibilities during a cyberattack and develop channels and mechanisms for safe and proper communication. Communication consists of sharing vital information with staff, legal stakeholders, law enforcement, regulators/support agencies, and the public.

- Redundancy- Access to essential information and systems will allow a business to continue operating before, during, and after a cyber incident, which makes a redundancy strategy critical to firms and their clients. Backing up and synchronizing key data, maintaining access to redundant power supplies, conducting inventory management of digital infrastructure/assets/services, and ensuring contingency plans are in place to allow business activity to continue when an attack occurs should be a priority for all firms.

- Containment- To mitigate the effects of a cyberattack a firm needs to activate its incident response plan with a focus on understanding the attack, communicating with key stakeholders, identifying an appropriate response, isolating and eradicating threats, and restoring systems. A solid containment strategy will help a firm manage an incident, protect key assets/information, enable business continuity, and protect a firm's reputation.

- Third-Party Dependencies- Identifying and taking inventory of the digital platforms, tools, and resources a firm is dependent upon that are controlled by a third-party is important for understanding the potential external risks, vulnerabilities, and business continuity issues a firm may encounter if a cyberattack occurs. Developing a contingency plan in case a third-party dependency is compromised is vital for protecting sensitive information and business operations and should be incorporated into a firm's incident response plan.

A well-designed cyber incident response strategy/plan can help a firm successfully navigate a cyber incident, while also protecting its business and clients from harm. Knowing what to do during a cyberattack takes preparation and training and by incorporating best practices a firm will be ready to effectively manage cyber incidents that have the ability to significantly affect their businesses.

---

[i] security incident - Glossary | CSRC (nist.gov)
[ii] https://www.splunk.com/en_us/pdfs/gated/white-paper/develop-an-incident-response-plan.pdf
[iii] https://www.cpajournal.com/2019/12/16/how-to-create-an-incident-response-plan/
[iv] Thompson, E (2018). Cybersecurity Incident Response: How to Contain, Eradicate, and Recover from Incidents (1st ed.). Apress
[v] https://commsec.ie/the-importance-of-incident-containment-during-a-cyberattack/
[vi] https://learn.saylor.org/mod/book/view.php?id=29706&chapterid=5350
[vii] https://www.finance.idaho.gov/wp-content/uploads/about/press-releases/documents/2023/2023-DOF-PR-Account-Takeover-Fraud.pdf
[viii] https://www.simplyclouds.com/blog/what-to-do-if-your-cloud-accounts-are-hacked