Preparing for a Cyber Incident

ABA Cybersecurity Legal Task Force

3/18/2023

Maureen Kelly, Co-Chair, ABA Cybersecurity Legal Task Force

Claudia Rast, Co-Chair, ABA Cybersecurity Legal Task Force

Alex Thierer, Staff Attorney, ABA Cybersecurity Legal Task Force

In January 2023 in the first of three articles on cybersecurity, we discussed keys to establishing an effective cybersecurity program. In this second article, we turn our attention to the importance of being prepared for a cyber incident.

As with any crisis, an organization must actively prepare for a cyber incident. With a Cyber Incident Response Plan ("IRP") customized to your organization, you have the benefit of making crucial, time-pressured decisions in the heat of the moment by following a plan that has laid out the issues likely to arise. To quote Benjamin Franklin, "By failing to prepare, you are preparing to fail." Development of a Cyber Incident Response Plan can enable your organization to weather a cyber incident as effectively as possible and limit the scope and impact of an incident.

President Biden emphasized the importance of cyber incident response planning in his May 2021 "Executive Order on Improving the Nation's Cybersecurity"[1]. Specifically, he called on the Department of Homeland Security, acting through the Cybersecurity & Infrastructure Security Agency (CISA) to develop a standardized cybersecurity incident response playbook to apply to all civilian federal agency cyber incidents.[2]

Increasingly, particularly given the COVID-19 pandemic, entities are understanding the need to plan for resilience in the face of a wide array of potential crises or disruptions, and are creating and maintaining crisis management and/or business continuity plans. If your entity already has a current crisis management or business continuity plan, you will need to make sure that your IRP works in concert with these other plans in the event of a major cyber event. If your organization has not yet created a crisis management or business continuity plan, your IRP can address the unique issues those plans cover. Chapter 15 of the recently released 3rd edition of The ABA Cybersecurity Handbook,[3] entitled "Achieving Preparedness through Standards and Planning and Best Practices for Incident Response" includes an excellent overview of risk management and incident response planning. This chapter includes the following key five planning tips:

[1] Executive Order on Improving the Nation's Cybersecurity, (May 12, 2021) Executive Order on Improving the Nation's Cybersecurity | The White House

[2] Id. at Section 6.

[3] The *ABA Cybersecurity Handbook* (3d. Edition) can be found here.

1. Establish a core planning team with executive management support.
2. Identify your entity's core capabilities and associated risks and risk mitigation (including insurance) by reviewing internal and external dependencies.
3. Develop a plan to best manage what happens as a result of a cyber incident or other disruptive activity.
4. Implement the plan into everyday operations, including through employee training and exercises.
5. Ensure continual improvement in the work environment.

What Is a Cyber Incident Response Plan?

A Cyber Incident Response Plan should lay out the steps the organization should take if it were to face a cyber incident, such as a ransomware event. At its core, it is an action plan. It must be actionable*, i.e.,* outline practical steps that can be taken. To be comprehensive, the IRP must be multi-disciplinary as cyber incidents are not solely the responsibility of your entity's information technology personnel. Rather, the IRP should include input by various other business operations that will be called upon during a cyber incident such as executive management, human resources, legal, supply chain and financial personnel along with information technology and information security personnel. Depending on the size and makeup of your organization, some of these functions may be performed by outside vendors.

What Should a Cyber Incident Response Plan Cover?

The National Institute of Standards and Technology (NIST), which publishes many cybersecurity guidelines in the US, including its widely used Cybersecurity Framework, has issued a helpful cybersecurity response guide[4] that provides comprehensive guidance through the entire life cycle of incident response. This NIST guide is predicated on 4 incident response phases:

(i) preparation;
(ii) detection and analysis;
(iii) containment, eradication and recover; and
(iv) post incident recovery.

The SANS Institute maintains similar cybersecurity guidance that is based on 7 response phases, the major difference being that the SANS model breaks the NIST third phase, i.e., containment, eradication and recovery, into 3 distinct phases.

In addition to the IRP guidance available from these and other organizations when drafting a Cybersecurity IRP, CISA has published the Cybersecurity Incident Response Playbook[5] on its website as required by the above-mentioned Cybersecurity Executive Order. On its website, CISA "encourages private sector" use of the playbook's response processes and procedures, noting specifically that non-federal entities can use its checklists for both incident response and incident response preparation.[6]

Key Incident Response Plan Components

[4] NIST SP 800—61, Computer Security Incident Handling Guide (rev.2). This guide was first published in 2004.
[5] **Federal Government Cybersecurity Incident & Vulnerability Response Playbooks (cisa.gov)**
[6] Cyber Incident Response | CISA

An effective Cybersecurity Incident Response Plan will address the technical steps required throughout the life cycle of a cyber incident to properly uncover, mitigate, contain, and recover from a cyber incident, but it also must identify the roles and responsibilities of both IT and non-technical personnel. Key components of such a plan include:

1. Development of relevant company policies, procedures, processes and checklists, etc. addressing such key questions as to what initial steps must be taken after discovery of an event, including who must be notified (which is likely to vary depending on the type and scope of the event)
2. Identification of who will be responsible for taking which actions (including documentation) and when and what approvals or notifications are pre-requisites throughout the event. Emergency contact lists should be kept up to date and distributed to personnel.
3. Training and testing on the policies, procedures, processes, checklists, etc. tailored to the individual's responsibilities. Key members of the response team should participate in regular table tops or drills, and lesson learned from such exercises should be incorporated into the Cyber Incident Response Plan and accompanying documentation.
4. Identification of all potential legal, contractual, customer or other obligations that may arise as a result of the potential incident based on the systems and data impacted. For example, does your insurance provider need to be notified Based on analysis of risks, entities should analyze the potential notification obligations and triggers as part of the preparation stage.
5. Logistics planning regarding such practical issues of a war room and how the response team will communicate if all systems are down.
6. A communication plan that addresses both potential internal (*e.g.,* employee, executive management, boards) and external communications (e.g., customer, law enforcement, regulatory, public releases, etc.).
7. Identification of potential third party experts or consultants, whether existing or newly required as part of incident response (e.g., forensic firms, law firms, ransomware services, crisis management experts, identity theft and data breach service providers). Entities should maintain a contact list and explore whether it makes sense to negotiate advance agreements with certain expert service providers.

Benefit of Incident Response Planning: Pro-active, Advance Consideration of Decisions That Could Be Faced

When an entity experiences any sort of crisis or disruption, it needs to make timely decisions on many questions unique to day-to-day operations. A benefit of developing a comprehensive, multi-functional Cybersecurity Cyber Incident Response Plan is that executive management can weigh potential decisions in advance.

For example, assuming no relevant legal obligation is triggered, a victim of a cyber event often will be faced with the question whether to notify law enforcement or other federal, state or local authorities, and if yes, which ones. This is a good question for an entity to discuss in advance and explore the benefits and potential risks association with making such notifications. As part of this process, an entity can reach out in advance of an event to understand what support these agencies can provide and how best to reach out if faced with a cyber incident.

Another notable answer that executive management may discuss in advance is whether and under what circumstances it would consider paying a ransom to a malicious actor. While the company may not be able to make an absolute decision in advance absent knowing the specifics of a specific event (e.g., availability, scope and quality of back up data, how much time will it take to recover, potential legal impediments) it could develop a checklist of considerations and potential parameters for making such a decision.

As part of this preparation activity, the company will want to understand any applicable legal restrictions on paying ransomware, including the Department of the Treasury's guidance that its Office of Foreign Controls (OFAC) may initiate an enforcement action against the entity if a ransomware payment were to violate US sanctions lists. The US has been adding both known foreign ransomware groups and individual actors to such lists.

Conclusion

As discussed in the January article, even entities with effective cyber programs may, and likely will, experience a hostile cyber incident. A Cyber Incident Response Plan can enable your organization to weather a cyber incident as effectively as possible and limit the scope and impact of an incident on your organization, employees, clients, and operations. Authorities like executive orders, NIST, SANS, and CISA can all provide guidance when preparing a response plan, but the responsibility lies with leadership to ensure that the response plan is tailored and effective to the needs of the organization.