# Preparing for and Managing a Cyber Attack

It is a fact of modern life that even organizations that have implemented cybersecurity defenses and safeguards still suffer significant cyber events. Human error, software vulnerabilities, and the ingenuity of threat actors ensure that the risk will never be completely eliminated. Consequently, organizations need to understand what to expect and be fully prepared for when the event happens.

## INCIDENT RESPONSE PLANNING

An incident response plan (IRP) is critical to managing a cyber event before the event occurs.

Why does an organization need an IRP? Cyber events are terra incognita for the vast majority of managers. They have never been involved in one and don't know what to expect or how to respond. Therefore, an organization and its leadership must create an IRP that considers what the organization is likely to face, creates response procedures, and assigns responsibility for carrying out those procedures. Cyber events happen extremely quickly and put management under immense pressure. Developing an organized response, under those circumstances, is tremendously stressful and prone to multiple small and potentially large failures. A well-constructed IRP will avoid that.

Many different people will be involved, including third-party vendors who will be needed to assist. Coordination and communication are critical. Effective coordination between all parties is a key factor in reducing the overall cost of an event. A 12-month study by a global cyber security firm found the common thread to a higher overall cost of an event was the "leadership teams' lack of prior awareness of critical decision-making processes in advance of an incident."[1]

Organizations should work with legal counsel experienced in creating incident response plans. While there are many vendors that can help with IRPs, the legal and regulatory environments the organization operates in may affect what needs to happen when a cyber event occurs.

Selection of third-party vendors to assist with event response should take place before a cyber event takes place. In most cyber events, organizations will need legal counsel and forensic investigators to determine the nature and extent of the event. Those firms should be selected in advance. In the high-pressure and fast-moving circumstances of a cyber event it isn't easy to find the time to thoughtfully select event response partners.

If the organization has cyber insurance, it is essential to work with the insurer on vendor selection. Insurers have lots of experience with cyber events and can make excellent recommendations. Also, some cyber policies require organizations to choose from the insurer's panel of service providers. The insurer's consent will be necessary to retain any firm.

Organizations that buy cyber insurance may have access to free and discounted resources provided by their insurer that can help with incident response planning.

## INCIDENT RESPONSE

No two cyber incidents are the same. Each will be different depending on the nature of the event (e.g. a small data breach vs. a ransomware attack), the size of the event, the complexity of the attack, the universe of affected parties, the extent to which regulators and law enforcement are involved, and the magnitude of financial losses to the organization and third parties. Nevertheless, there are commonalities that organizations need to understand and manage well.

1. **IRP Activation**
   Activation of the IRP may be difficult if those responsible for incident response aren't familiar with it. An organization should regularly rehearse its IRP through a "tabletop" exercise that simulates a cyber event
2. **Triage**
   This is the process of making an initial determination of what happened. This is usually performed by IT staff
3. **Notice to cyber insurer(s)**
   Notice must be given as soon as possible after a cyber event is discovered. Cyber insurers that provide a hotline for insureds to call typically want them to use it so that they receive good advice from the beginning of the event
4. **Retain event response vendors**
   It is usually best to start with legal counsel. Experienced counsel can coordinate the organization's incident response. They can also retain other vendors so that the attorney-client privilege extends to their work. As a reminder, where cyber insurance is in place the insurer must consent to each vendor retained
5. **Notify law enforcement and/or regulators**
   This should only be done after consulting with legal counsel. Notification may or may not be required by law, and where optional, it may or may not be in the organization's interest to do so

Depending on the type of event, many other aspects of incident response may be needed. Those may include notification of individuals affected by a data breach, providing credit and identity monitoring to those individuals, and retaining a public relations firm to help reduce damage to the organization's reputation resulting from the cyber event.

## THE ROLE OF CYBER INSURANCE IN INCIDENT MANAGEMENT

Cyber insurance can be an incredible resource when a cyber event happens. While covering losses is important, the insurer's experience with similar events may be the most essential benefit of a cyber policy for many organizations. A clear understanding of the benefits of the policy and most importantly, how to quickly access are essential.

## CASE STUDY

A national wholesale company became the victim of a ransomware attack at the start of its busiest season. While it took a few days to understand the full scope of the damage from the malware attack, the disruption took months and the round-the-clock work of a dedicated incident response team to fully recover.

Because of their recent cyber policy renewal, an extensive process, the company had an action plan to put into action. They called their insurer and were immediately connected with an attorney who assembled the incident response team. This team held daily meetings for several weeks, covering every detail of the response, from tech support to regulatory compliance, and communications to ransom negotiations. The client said they could not have done all that work without the insurer's support.

The company's president, a C-suite veteran, admitted that the entirety of the cyber incident was one of the most stressful events of his career. Only the COVID-19 pandemic compared to its sheer intensity. From the first call to the insurer, he realized the company was fortunate to have a cyber policy to help navigate throughout their recovery. **"This insurance was one of the best investments we've ever made. Without it, the event could've been a complete catastrophe."**

The president said it took several weeks for systems to be functional and many more months for a complete recovery.

## FINAL WORD

Being unprepared for a cyber event will make a bad situation exponentially worse. In many cases an organization's degree of preparedness is the greatest factor in the extent of an event's disruption and cost. Devoting the necessary time and resources to response planning will help the organization resolve an event more quickly, with less stress and distraction of senior management, and reduce potential financial losses. Cyber insurers, and cyber policies, can be a strong helping hand before, during, and after the event.

*This is the second article in our cyber risk management series. The first article focused on* ***protecting your organization from cyber-attacks****.*


CONTRIBUTORS:

- **Tim Burke,** *Executive Vice President, Cyber/Commercial Client Advantage*
- **William Boeck,** *Executive Vice President, Cyber Product Leader Client Advantage*
- **Angela Thompson,** *Senior Marketing Specialist, Market Intelligence & Insights*
- **Brian Spinner,** *Senior Marketing Coordinator, Market Intelligence & Insights*



SOURCES:

[1] Airmic. (2024, September 10). Cyber Claims, Guide 2024. Airmic-Baker-Tilly. https://www.airmic.com/technical/library/cyber-claims