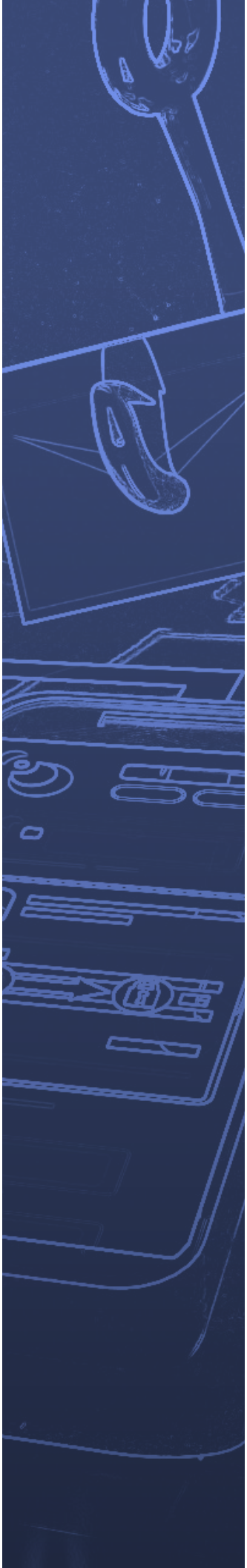
Cyber Incident
Response Scenario

BEC Scam

HORST
INSURANCE



Introduction

The way an organization responds to a cyber incident can make or break its operational, financial and reputational stability.

In the event of a poor response, an organization may encounter various consequences—including the exposure of sensitive data, compromised technology, widespread business disruptions, disgruntled stakeholders, lost customers and diminished market value. Fortunately, organizations can mitigate these damages through proper cyber incident response planning.

A cyber incident response plan establishes steps to ensure timely remediation amid cyberattacks and keep related losses to a minimum. Effective response planning requires coordination across an organization.

A solid response plan should outline the following:

- Who is part of the cyber incident response team (e.g., company executives, IT specialists, legal experts, media professionals and HR leaders)
- What roles and responsibilities each member of the response team must uphold during an incident
- When and how stakeholders and the public (if necessary) should be informed of an incident
- How the organization's key functions and operations will continue throughout an incident
- What forensic activities will be leveraged to identify the cause and prevent future incidents
- Which federal, state and local regulations the organization must follow when responding to an incident (e.g., reporting protocols)
- When and how the organization should seek assistance from additional parties to help recover from an incident (e.g., law enforcement)
- How an incident will be investigated

For cyber incident response plans to be successful, they should address a number of attack scenarios. By including different scenarios within their response plans, organizations can be ready to handle any type of attack and protect themselves from large-scale losses. One of the most important scenarios to include in a cyber incident response plan is a **business email compromise (BEC) scam**. Such a scam entails a cybercriminal utilizing social engineering tactics to impersonate a seemingly legitimate source (e.g., a company executive or supplier) via email and gain the trust of their target, ultimately convincing them to wire money, share sensitive information or engage in other compromising activities. Keep reading for an example of a BEC scam scenario and a summary of how a cyber incident response plan can address it.

Attack Scenario

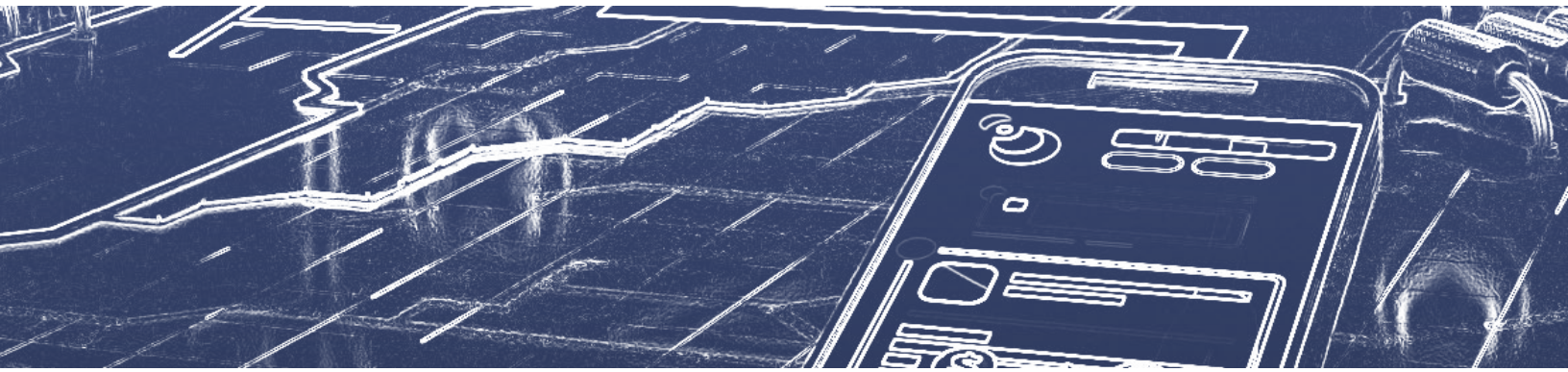
On Tuesday, an employee working in the finance department of a large organization received a **deceptive email** from an account claiming to be the company's chief financial officer (CFO).

In this email, the supposed CFO instructed the employee to conduct an **urgent wire transfer of $100,000** to a newly opened bank account in order to help close a confidential business deal. Believing the sender and their request to be legitimate, the employee decided to proceed with the transaction and promptly initiated the large-scale transfer of company funds.

In reality, the manipulative email came from a cybercriminal only posing as the organization's CFO, and the $100,000 wire transfer landed in the criminal's private bank account. By the time the employee realized that the request was fraudulent and they had been deceived, the transfer had already gone through, making recovery increasingly difficult. By Wednesday, the cybercriminal had already moved the funds and dispersed them across multiple accounts so they would be even harder to track. At this point, the employee had reported the incident to their manager. Facing significant financial losses, the organization needed to react swiftly to prevent possible business disruptions and limit further damage.

Response Plan Reaction

A **well-crafted cyber incident response plan** would guide the impacted organization in this particular BEC scam scenario through the following steps:



Detection and research—Upon receiving the employee's report of the BEC scam, the employer promptly assessed the situation to determine whether the incident posed a genuine threat. After validating the attack, additional research was conducted on the scope and severity of the incident by documenting which assets were affected and calculating potential losses. From there, the employer activated the cyber incident response team and notified necessary parties (e.g., local authorities and insurance professionals) to kickstart the investigation and the insurance claims process.

Reporting—Following incident detection and research, the cyber incident response team reached out to the organization's financial institution to report the BEC scam and establish that the large-scale wire transfer was a fraudulent transaction. The response team then had the financial institution temporarily freeze the organization's impacted bank account to prevent further transfers or loss of funds and put the institution in contact with the local authorities to provide any relevant information for the incident investigation. Due to the severity of the attack, the response team also reported the BEC scam to the FBI's Internet Crime Complaint Center (IC3), the nation's primary hub for handling digital crimes.

Containment—At this stage, the cyber incident response team assessed whether any company email accounts and other workplace systems were affected by the attack, as cybercriminals sometimes infiltrate their targets' technology before deploying social engineering tactics and sending deceptive emails during BEC scams. The response team then revoked access to any compromised accounts and isolated all affected systems to help minimize additional damage. During this containment, the response team still prioritized critical operations and limited possible business disruptions by developing temporary workarounds for impacted accounts and systems. Additionally, the response team relied on offline

communication methods (e.g., phone calls) throughout this process to reduce the risk of the cybercriminal responsible for the BEC scam intercepting any important conversations.

Recovery—After containment, the cyber incident response team repaired all compromised email accounts and affected systems, thus restoring these items to their original functionality. The response team then scanned the organization's larger network for any remaining vulnerabilities to ensure the cybercriminal wouldn't be able to relaunch the attack from a different digital avenue. Once the response team addressed any ongoing vulnerabilities, it consulted with legal counsel to discuss any regulatory ramifications of the incident and determine whether further steps could be taken to help recover the stolen funds. Because the BEC scam wasn't discovered for nearly 24 hours and the cybercriminal had already dispersed the funds, only a portion of the $100,000 wire transfer was recovered.

Communication—Following the recovery process, the cyber incident response team worked closely with the local authorities, the organization's financial institution, the IC3 and insurance professionals to provide any further information and documentation that would help these parties complete their investigation and resolve the associated insurance claim. The

response team also took this time to release a public statement regarding the BEC scam and communicate directly with any regulators or stakeholders who needed to be informed of the incident.

Post-incident analysis—Lastly, the employer conducted a post-incident analysis. This analysis focused on where the BEC scam originated; how it was detected; how effective the incident response plan was in handling this event; the different technical, operational and financial impacts of the incident; and whether any organizational failures played a role in the event (e.g., poor employee training and insufficient payment procedures). The results of the post-incident analysis ultimately guided the identification of the organization's cybersecurity weaknesses and supported its effort to fill possible gaps with bolstered defenses (e.g., enhanced employee education and secure wire transfer protocols with multiple payment verification options). This analysis also helped the employer make necessary updates to the cyber incident response plan, thus improving mitigation techniques for future cyber incidents and reducing related damage.

An organization's cyber incident response team typically comprises various experts and professionals across multiple fields. It's worth noting that, depending on an organization's size and in-house resources, its response team may include

either internal or external parties. In other words, larger organizations may have entirely in-house response teams, whereas small organizations with fewer resources may seek the assistance of third-party vendors. In any case, before hiring any vendors to help respond to cyber incidents, employers should consult their cyber insurers to determine whether any policy provisions include vendor-related stipulations or requirements; some insurers mandate policyholders to work with preselected vendors that offer negotiated rates, therefore limiting associated claim costs. In this particular BEC scam scenario, the impacted organization had various in-house experts due to its size and was able to utilize a largely internal response team.

Keep in mind that even with an effective cyber incident response plan in place, the affected organization still wasn't able to recoup the entirety of the stolen funds. Incidents like these highlight the importance of having ample commercial insurance coverage, which can provide much-needed financial protection when costly business losses arise. The policies that can offer coverage for BEC scams vary between insurers. Some insurers provide such coverage via crime insurance policies, whereas others offer this coverage through cyber insurance policies. Even with these traditional insurance offerings, insurers may issue certain policy requirements and restrictions, limiting overall coverage capabilities.

Furthermore, some insurers may only provide coverage for BEC scams through social engineering insurance, which is a specialized policy endorsement that can typically be added to a standard crime or cyber insurance policy. In this specific BEC scam scenario, the affected organization leveraged its social engineering endorsement on its traditional crime insurance policy to receive coverage for the remaining losses from the wire transfer. Regardless, employers should be sure to consult trusted insurance professionals to discuss their unique coverage needs and determine how their policies will respond to BEC scams.

Conclusion

Employers can adequately prepare for cyber incidents and reduce potential fallout through **proper response planning**.

Yet, they should understand that their response plans are always a work in progress; as operational needs change and cyber exposures evolve, response planning should follow suit. Several practices (e.g., tabletop exercises and penetration testing) can be leveraged to assess cyber incident response plans and make adjustments over time. In doing so, organizations can remain prepared for the latest cyberthreats and successfully navigate the ever-changing digital risk landscape.

Contact us today for further risk management guidance.