Cybersecurity Incident Response

Prepare to answer, "Now what do we do?"

By David E. Sems, CPA, CITP, CFF, and Paul G. Sems

As cybersecurity incidents continue to plague healthcare provider and payer organizations, having a clear, immediate response plan can mean the difference between a manageable incident and a catastrophic breach. Increasingly, for healthcare internal audit teams, understanding the first critical steps following a cybersecurity incident is essential for protecting your organization's operations, reputation, and legal standing.

This article focuses on two of the most prevalent and damaging cyber threats currently facing healthcare organizations: ransomware and business email compromise (BEC). Recent events underscore the urgency of proper incident response preparation, as healthcare organizations have become increasingly attractive targets for cybercriminals who recognize both the sensitivity of the data held and the critical nature of healthcare operations.

Healthcare: A targeted industry

The healthcare sector has experienced an unprecedented surge in cyberattacks over the past two years. According to the latest reports from the Department of Health and Human Services' Office for Civil Rights, healthcare data breaches reached an all-time high in 2024, with 14 data breaches involving more than one million healthcare records impacting nearly 237 million US residents—that's 70% of the country's population.

Perhaps the most devastating example of this trend was the Change Healthcare (a subsidiary of UnitedHealth Group) ransomware attack in February 2024, which has been described as a landmark cyberattack against the U.S. healthcare system. The attack affected an estimated 192.7 million individuals and resulted in costs exceeding $2.4 billion. The incident began when attackers associated with the ALPHV/BlackCat ransomware group exploited a remote access system that lacked multifactor authentication, highlighting how basic security oversights can lead to catastrophic consequences.

The golden hours: Why immediate response matters

Just like when a patient is having a heart attack, seconds

The first 24 to 48 hours following a cybersecurity incident are critical.

Cyber insurance policies often require prompt notification of incidents, sometimes within hours or days of discovery.

count. This is no different in the cybersecurity world. The first 24 to 48 hours following a cybersecurity incident are critical. During this period, evidence can be lost, legal obligations may be triggered, and the scope of the incident can expand dramatically if not adequately contained. For healthcare organizations, the stakes are particularly high given HIPAA requirements, patient safety concerns, and the potential for significant operational disruption.

Recent incident data demonstrate the financial impact of delayed response. The daily losses from ransomware attacks are staggering—almost a million dollars a day. However, it is not just monetary damages; there are other real-world impacts.

Internal auditors must understand that cybersecurity incidents in healthcare can have direct implications for patient care and safety. Recent research suggests that ransomware attacks on hospitals can have a spillover effect on neighboring hospitals, overwhelming their systems and resulting in an 81% increase in cardiac arrest cases.

One of the top vectors of attack for ransomware deployment is business email compromise (BEC). BEC is a type of scam in which criminals use fake or hacked email accounts to impersonate trustworthy individuals in a business, such as a supervisor or a regular supplier, to trick employees into sending money or sharing sensitive information. A 2023 study by Ponemon found that 66% of healthcare firms hit by BEC reported care disruptions, with a 23% increase in patient mortality.

Universal first steps: The foundation response

Regardless of the type of incident, the following four immediate actions should be taken. These steps form the foundation of any effective incident response and should be initiated simultaneously rather than sequentially, to maximize the preservation of evidence and minimize ongoing damage.

Contact your legal team

The first step is to contact your legal team immediately, whether it is your in-house counsel or an outside cybersecurity attorney. Getting the legal department involved early isn't just about following the rules; it also makes sure anything you discuss about the incident is protected and can't be easily shared in a lawsuit or investigation. Plus, your lawyers will help you navigate the tricky requirements for notifying people and agencies, whether it's under HIPAA, state data breach laws, or other regulations, which can vary a lot depending on where you're located.

Contact your cyber insurance carrier

Simultaneously, you must contact your cyber insurance carrier. Cyber insurance policies often require prompt notification of incidents, sometimes within hours or days of discovery. Early contact with your carrier preserves coverage rights under the policy and frequently provides access to pre-approved incident response vendors who can be deployed immediately.

Engage a professional incident response team

The third critical step is to engage a professional incident response team. Unless your organization has dedicated cybersecurity incident response capabilities available around the clock, contact an external incident response firm immediately. These professionals offer 24/7 emergency response capabilities and possess specialized tools and expertise in forensic analysis that many healthcare organizations lack internally.

Isolate, don't eliminate

The fourth concept is perhaps the most counterintuitive but critically important: isolate, don't eliminate. Avoid shutting down affected systems unless necessary for immediate safety reasons. Instead, disconnect affected systems from the network to allow for proper live preservation using forensic techniques. This approach preserves items that could otherwise be irretrievably lost, including RAM and system logs.

Incident response first steps:

- Contact your legal team
- Contact your cyber insurance carrier
- Engage a professional incident response team
- Isolate, don't eliminate

Ransomware with data disclosure: The modern threat landscape

Ransomware attacks have evolved significantly beyond simple encryption to include data exfiltration and threats of public disclosure. This evolution has made ransomware incidents exponentially more complex from both a technical and regulatory perspective. Modern ransomware groups operate sophisticated business models, often maintaining customer service departments and negotiation protocols that rival legitimate businesses in their professionalism.

The Change Healthcare incident exemplifies this evolution. The attackers not only encrypted systems but also stole approximately four terabytes of data. How much is four terabytes? Printing that on paper would be 2 billion sheets; stacked, it would be 124 miles high! When UnitedHealth Group paid the $22 million ransom, it was discovered that the ransomware group had given the stolen data to another hacker group. This other hacker group then approached, seeking an additional ransom payment, illustrating how data theft can create ongoing exposure even after initial ransom payments have been made.

As mentioned previously, disconnecting the systems from network access while allowing forensic analysis to be performed will likely result in better data for discovering how the breach occurred and possibly lead to a greater chance of recovery.

The assessment phase requires careful coordination between technical and legal teams.

Healthcare organizations must recognize that ransomware incidents with data components often trigger multiple regulatory frameworks simultaneously. For example, under the HIPAA Breach Notification Rule (45 CFR §§ 164.400–414), covered entities are required to report any breaches involving unsecured electronic protected health information or physical records containing protected health information, typically within 60 days.

Business email compromise: The billion-dollar healthcare threat

BEC attacks have emerged as one of the most common and financially damaging threats to the healthcare sector. The FBI's latest report on cybercrime identifies BEC as causing over $55 billion in global losses between 2013 and 2023. Healthcare organizations are particularly vulnerable to BEC attacks due to their high-value financial transactions, complex vendor relationships, and email-dependent workflows that handle everything from health plan member and patient records to billing coordination.

BEC attacks targeting healthcare organizations have evolved beyond the traditional CEO fraud model to exploit industry-specific vulnerabilities. For example, cybercriminals are now sophisticated in their social engineering, pretending to be management and requesting detailed accounting reports from accounts receivable, which they then use to send fake payment statements to patients with past-due balances.

When a BEC attack is suspected, particularly one involving financial fraud, immediate notification to the FBI becomes crucial. The FBI's Recovery Asset Team can be reached by phone at 1-855-292-3937 or via email at RAT@fbi.gov. This team specializes in freezing fraudulent transactions and potentially recovering funds. Of course, time is of the essence.

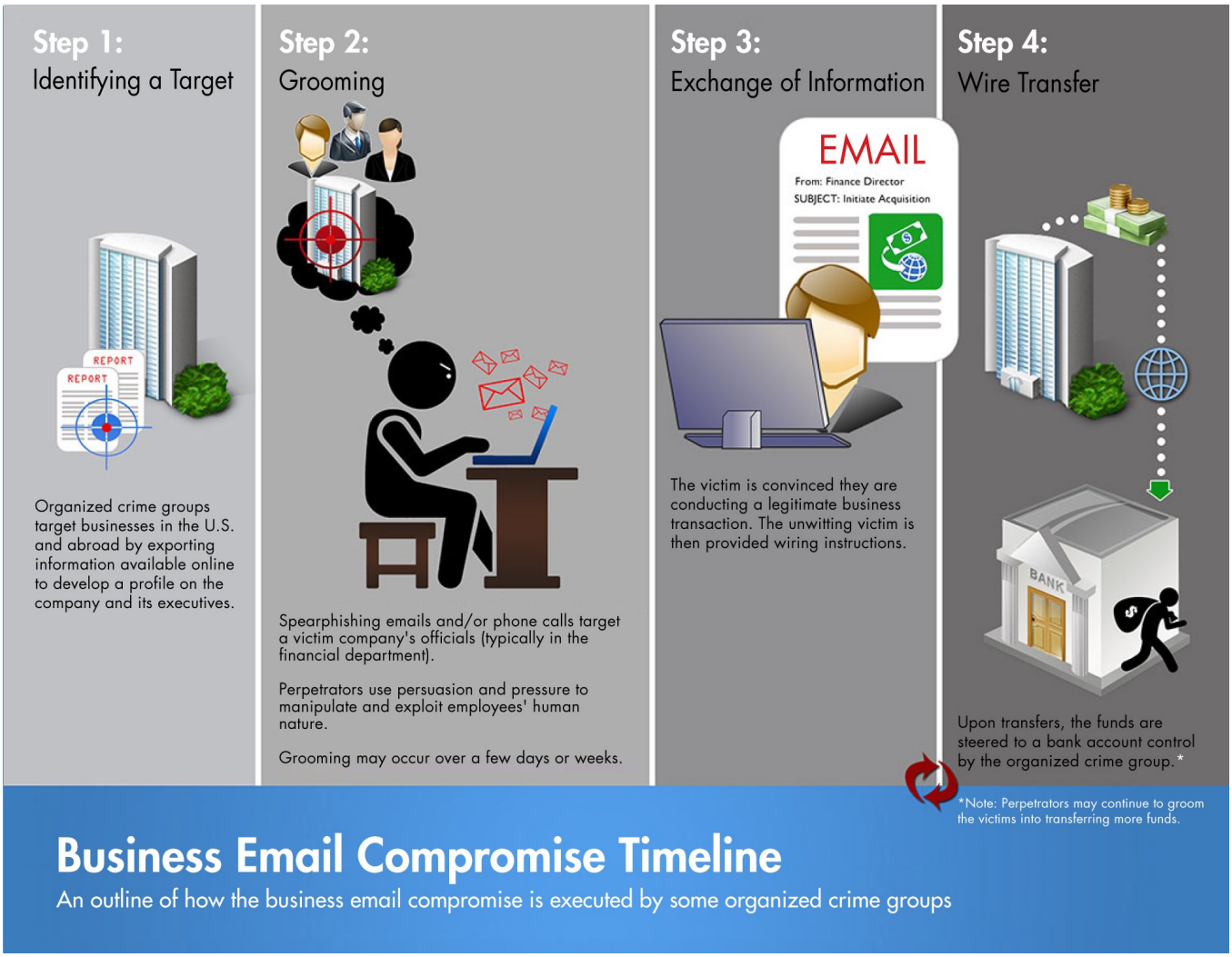
The specific BEC response protocol requires the immediate preservation of all email evidence, without deleting suspicious communications. Identify compromised accounts and reset credentials immediately, ensuring that forensic evidence is captured before making any changes. This can be a challenge, but many enterprise email systems offer options to assist with these tasks. Ensure your organization is paying attention to this critical area and making strategic investments in it.

The forensic investigation phase should focus on understanding the attack vectors to close holes and prevent future attacks. Maintaining accurate email logs and authentication records is crucial in determining how the compromise occurred. Auditors should thoroughly test these logs and records to ensure they are in place, stored for a reasonable period, and easily accessible before an event occurs.

Critical investigation principle: understand before you recover

A key part of handling a security incident is understanding what caused it before trying to fix it. If recovery begins too

Ransomware attacks on hospitals can have a spillover effect on neighboring hospitals, overwhelming their systems.



Source: https://www.fbi.gov/image-repository/business-email-compromise-timeline-050222.jpg

soon, the same weaknesses that allowed the attack may still be present, making it easy for the attacker to return. Skilled attackers often establish hidden methods to regain access to systems, such as secret accounts or backup attack methods that are difficult to detect. Rushing to recover can also erase evidence about how the attack happened, making it harder to protect the system from future threats.

An investigation-first approach means conducting a thorough analysis to understand exactly what happened during the attack before initiating any recovery. This analysis needs to identify all the methods by which attackers gained access and every system they compromised, not just the obvious entry points. Recording the signs of the attack helps security teams spot similar attacks in the future and understand the specific methods the attackers used. Before turning any systems back on, the team must confirm that the attackers are entirely gone.

This careful approach also includes implementing security improvements based on lessons learned from the incident. Organizations that skip this step often get attacked again using the same methods within weeks or months. Since the attackers already know the network layout and where the valuable information is, they can quickly break back in if the security weaknesses aren't fixed.

Understanding and testing cybersecurity controls

You, as internal auditors, are key to helping healthcare organizations prepare for and address cybersecurity threats. In addition to your many responsibilities, you must also understand the cyber risks the organization faces, verify

The Change Healthcare incident demonstrates how single-point failures in basic controls can undermine an entire security program.

whether current security measures are effective, and ensure that the incident response plan covers all necessary aspects and is practiced regularly.

Risk assessment forms the foundation of effective cybersecurity auditing in healthcare organizations. Internal auditors must identify and catalog the organization's most critical assets, including member and patient data repositories, electronic health record systems, financial systems, and operational technology that directly impacts patient care. This asset inventory must extend beyond traditional IT systems to include Internet of Medical Things devices, telemedicine platforms, and cloud-based services that may contain protected health information.

The regulatory landscape affecting healthcare cybersecurity continues to evolve rapidly. Specifically, the 2024 HIPAA Security Rule to Strengthen the Cybersecurity of Electronic Protected Health from the Department of Health and Human Services proposes the following:

- Revise standards to better protect electronic protected health information (ePHI), including increasing cybersecurity by directly addressing recent cyberattacks, enforcement deficiencies, and evolving best practices.
- Codify various critical activities (such as risk analyses, technology asset inventories, and mapping ePHI flows) that were previously less formalized, increasing the expectation for demonstrable preventive controls.
- Shift previously "addressable" safeguards to "required"— regulated entities must "inventory technology assets and map the movement of ePHI," and implement mechanisms (such as encryption with fewer exceptions) without the prior flexibility to opt out, and must provide documentation as proof during investigations or audits.

Control testing in the healthcare cybersecurity context requires both technical assessment and operational validation. Technical controls, such as multifactor authentication, encryption standards, and network segmentation, must be evaluated not only for their presence but also for proper implementation and effectiveness.

The Change Healthcare incident, where a lack of multifactor authentication on a critical system enabled a catastrophic breach, demonstrates how single-point failures in basic controls can undermine an entire security program.

Regulatory framework alignment and compliance testing

Effective cybersecurity incident response in healthcare must align with established frameworks while meeting specific regulatory requirements that extend beyond general cybersecurity guidance. The NIST Cybersecurity Framework provides a structured approach through its five core functions: Identify, Protect, Detect, Respond, and Recover. However, healthcare organizations must overlay HIPAA requirements, state breach notification laws, and industry-specific guidance onto this framework.

Another standard to consider when implementing a cybersecurity program is the SANS Incident Response. This method offers a structured approach that is well suited for healthcare organizations. It includes six phases: Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned. Each phase has specific considerations for healthcare that internal auditors must understand and verify.

Internal auditors should confirm that incident response teams are familiar with HIPAA breach notification rules, including the four-factor test that determines whether an incident must be reported. This test examines the type of member and patient information involved, who accessed it without authorization, whether the information was actually viewed or taken, and the extent to which the risk has been mitigated.

Documentation, communication, and stakeholder management

Effective incident response requires detailed documentation that serves several important purposes:

- analyzing what happened,
- meeting regulatory requirements,
- protecting the organization legally, and
- learning from the experience.

Internal auditors must ensure that incident response teams are aware of the records to be kept and maintain them throughout the entire incident.

Documentation during cyber incidents must be thorough yet completed quickly. Initial response actions should be recorded with timestamps, the people making decisions should be identified, and the reasons for important decisions should be documented. This documentation becomes essential for reviewing what happened afterward and may be needed for regulatory reports or legal cases.

Managing communication during incidents is particularly challenging for healthcare organizations because different groups require different types of information. Patients and/or members, staff, regulators, insurance companies, vendors, and the media may all need different kinds of updates at various stages of the response process.

It's essential for internal auditors to regularly verify that the organization is prepared to comply with all applicable notification rules, particularly in high-stress situations. They should make sure contact details for anyone who might be affected are both up-to-date and complete, that the notification templates meet legal requirements, and that the team can quickly send out large batches of notifications when needed.

Long-term protection strategies

While immediate incident response focuses on stopping the attack and recovering, internal auditors must also check how the organization builds long-term cybersecurity strength. This includes both prevention measures and the organization's ability to improve its security based on lessons learned from past incidents and current threat information.

Email security is crucial, as approximately 90% of cyberattacks begin with email. Internal auditors should check whether the organization uses advanced email authentication methods that verify legitimate senders and block fake emails, which are now considered basic defenses by major security standards organizations. New AI tools can help immensely in this area. For example, Darktrace/EMAIL is an advanced AI email security solution that scans every email and builds advanced AI rules on the fly, helping deter BEC incidents.

The healthcare industry's increasing reliance on cloud services, such as Office 365, and internet-connected medical devices and sensors, presents new ways for attackers to compromise security. Internal auditors must understand these emerging technologies and their associated risks to properly evaluate organizational protections.

Since most attacks originate at the human behavioral level rather than through direct physical means, training becomes increasingly important. Training programs must keep pace, and internal auditors should verify whether the training content is current and whether it's being delivered effectively.

Conclusion

The cybersecurity challenges facing healthcare organizations will continue to evolve as technology advances and threat actors adapt their methodologies. Internal auditors play a crucial role in helping organizations build and maintain the resilience necessary to fulfill their mission while protecting the sensitive information entrusted to their care. Through comprehensive testing, continuous monitoring, and proactive risk assessment, internal audit functions can help ensure that healthcare organizations are prepared for cyber incident occurrences that are no longer a matter of if, but when. **NP**

David E. Sems, CPA, CITP, CFF, is a recognized expert in cybersecurity and digital forensics, with over 20 years of experience investigating complex cybercrimes, leading global forensic technology teams, and advising law enforcement and corporations on matters including hacking, data theft, and advanced analytics. David can be reached at David@semsassociates.com and 440-941-7367.

Paul G. Sems brings extensive experience in cybersecurity, risk management, and healthcare compliance to his role as a trusted advisor to healthcare organizations. His expertise spans incident response, regulatory compliance, and strategic cybersecurity planning, helping organizations navigate the complex landscape of healthcare cybersecurity.