Nationwide® is on your side

Guarding Against and Responding to Business Email Compromise Attacks

A business email compromise (BEC) attack involves a cybercriminal impersonating a seemingly legitimate source via email to gain their target's trust. The cybercriminal then leverages these emails to convince their target to wire money, share sensitive information or conduct other compromising activities, thus potentially resulting in substantial losses among affected businesses. BEC attacks caused $2.7 billion in losses across the United States in 2022. In total, global losses related to these attacks have surpassed $43 billion.[1]

Fortunately, businesses can reduce the risk of BEC attacks and subsequent potential losses by strengthening their digital defenses and purchasing cyber insurance coverage. This infographic outlines a BEC attack scenario, offers suggestions to help prevent such attacks and summarizes the associated cyber insurance claims process.

BEC attack scenario

While specific BEC attack methods can vary, these incidents often follow the same framework. While each attack is unique, here are the typical steps in a general BEC attack scenario:[2]

Research—First, a cybercriminal will choose a company to launch their BEC attack against and research this business to help create convincing emails and gain their target's trust during the attack. This may include analyzing the company's website, LinkedIn page and employees' online profiles.

Selection—Upon researching the business, the cybercriminal will use the information they collected to prepare for their attack. At this point, the cybercriminal selects an individual within the business as their primary target for the incident, likely someone with access to critical company resources.

Manipulation—Once they select their target, the cybercriminal will usually deploy malware to access their target's email account and monitor the target's digital interactions without their knowledge. The cybercriminal can then use this information to better impersonate a trusted sender and manipulate the target into performing compromising activities.

Discovery—After manipulating their target, the cybercriminal will aim to swiftly exit the affected company's network with the stolen assets. From there, it may take minutes, days or even weeks for the business to detect the attack. Such detection often occurs through internal reviews, unusual network behavior, unexpected financial transactions or stakeholder complaints.

Fallout—The impacted company may experience severe consequences from the BEC attack, such as missing or damaged data, disrupted supply chains, operational delays, reputational damage, legal ramifications and financial losses. In fact, BEC attacks cost an average of $4.9 million per incident.[3]

Prevention tips

Businesses should consider implementing the following cybersecurity measures to help enhance their digital defenses and minimize BEC attacks:[4]

- Provide routine training to educate employees on safe email practices and how to detect and respond to common BEC attack scenarios.
- Establish secure payment procedures and instruct employees who handle financial operations to validate invoices and fund transfer requests before proceeding, especially if these requests involve alternative procedures or changes in account numbers.
- Leverage access control policies (e.g., the principle of least privilege and multi-factor authentication) to confirm employees only utilize the resources needed to perform their jobs.
- Equip company systems with adequate security features (e.g., antivirus programs, virtual private networks, firewalls, email authentication technology, endpoint detection and response solutions, and patch management software) and upgrade these features when necessary.
- Back up critical data to secure locations on regular schedules and establish data recovery procedures to ensure swift restoration amid possible attacks.
- Develop a cyber incident response plan that outlines steps to promote timely remediation and keep losses to a minimum when attacks arise.
- Work with IT, legal counsel and insurance professionals to update cybersecurity measures and make coverage adjustments as needed.

The claims process

If a business falls victim to a BEC attack, cyber insurance may help a business minimize the financial fallout and bolster its recovery capabilities. Here's an outline of the typical claims process that a company may follow upon experiencing a BEC attack:

Notification and reporting—The business would immediately contact its cyber insurer and file a claim upon identifying an attack. At this time, the business would provide as much information as possible in a detailed report outlining the incident, related losses and any mitigation measures taken.

Evaluation and assessment—After receiving the necessary documentation and conducting an in-depth incident investigation, the cyber insurer will likely need to evaluate and assess the related claim. This entails reviewing the extent and validity of the claim based on applicable policy terms and conditions, as well as determining specific coverage capabilities.

Cooperation—While the cyber insurer is investigating the attack, the business would prioritize open communication and cooperation. This may include providing access to affected systems and sharing relevant documentation to help identify potential perpetrators.

Collaboration—Depending on the complexity and impact of the attack, the cyber insurer may need to consult the business for additional information to better support the associated claim and make certain coverage decisions. In this case, the business would work closely with the insurer and foster a strong sense of collaboration by exchanging evidence, clarifying details and addressing any questions or concerns to help reach the best possible claim resolution.

With BEC attacks on the rise, businesses can't afford to ignore the need for proper risk mitigation measures and cyber insurance. By implementing effective prevention tactics and coverage solutions, businesses can minimize their exposures and limit large-scale losses.

This document is a general overview and doesn't replace the need to consult cybersecurity experts and legal counsel for tailored guidance. Click here for more information on Nationwide's cyber risk management solutions and insurance offerings.

1 https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf
2 https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/business-email-compromise
3 https://www.ibm.com/topics/business-email-compromise
4 https://www.microsoft.com/en-us/security/business/security-101/what-is-business-email-compromise-bec

Nationwide®

The information contained in this page is intended for general informational purposes only and is not intended to provide legal or other expert advice. You should consult knowledgeable legal counsel or other knowledgeable experts as to any legal or technical questions you may have. Neither Nationwide nor its employees or agents shall be liable for the use of any information or statements made or contained in any information provided herein. This document may contain third-party websites solely for informational purposes and as a convenience to readers, but not as an endorsement by Nationwide of the entities referenced or the contents on such third-party websites. Nationwide is not responsible for the content of linked third-party websites and does not make any representations regarding the content or accuracy of materials on such linked websites. The opinions and positions expressed in this report are the authors' own and not necessarily of Nationwide.

Products, coverages, discounts, insurance terms, definitions and other descriptions are intended for informational purposes only and do not in any way replace or modify the definitions and information contained in individual insurance contracts, policies, and/or declarations pages from Nationwide-affiliated underwriting companies, which are controlling. Such products, coverages, terms and discounts may vary by state, and exclusions may apply. Products are underwritten by Nationwide Mutual Insurance Company and affiliated companies in Columbus, Ohio, and are subject to underwriting guidelines, review and approval. Availability varies by state. Nationwide, the Nationwide N and Eagle and Nationwide is on your side are service marks of Nationwide Mutual Insurance Company. © 2023 Nationwide.