Strengthening internal controls to prevent and mitigate cyberfraud

SEC crackdown on cyberfraud looms large

Prepared by:

Greg Naviloff, Director, RSM US LLP
greg.naviloff@rsmus.com, +1 617 241 1208

Chris Ekimoff, Director, RSM US LLP
chris.ekimoff@rsmus.com, +1 571 341 4195

Alain Marcuse, Director, RSM US LLP
alain.marcuse@rsmus.com, +1 617 241 2398

March 2019

On Oct. 16, 2018, the U.S. Securities and Exchange Commission (SEC) issued a report[1] stating that inadequate prevention of cyber-related fraud may violate the internal accounting control provisions of the Securities Exchange Act of 1934. This report summarizes the SEC's investigations of nine issuers spanning numerous industry sectors that lost millions of dollars as a direct result of cyber-related frauds.

The report goes on to indicate that in typical frauds, company employees received a targeted phishing email appearing to be from a company executive or a major vendor, either from a spoofed address or from a compromised account. The email directed the victim to wire large sums of money to, or pay invoices to, seemingly legitimate accounts that were actually controlled by the fraudster. The FBI estimates that these business email compromise (BEC) attacks have caused over $5 billion in losses since 2013, with an additional $675 million in adjusted losses in 2017 alone.

While the SEC has declined to pursue enforcement action in these matters to date, the report reminded companies of their control requirements and has left open the potential for future enforcement actions. The Commission is advising issuers that "internal accounting controls may need to be reassessed in light of emerging risks, including risks arising from cyber-related frauds."

These statements by the SEC indicate a shift towards stricter practices to address cyberthreats, underscoring the importance for internal education.

The SEC made it clear that public companies subject to section 13(b)(2)(B) of the Securities Exchange Act—the federal securities law provision covering internal controls—have an obligation to assess and calibrate internal accounting controls for the risk of cyberfrauds and adjust policies and procedures accordingly.

1. "Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934 Regarding Certain Cyber-Related Frauds Perpetrated Against Public Companies and Related Internal Accounting Controls Requirements," Securities and Exchange Commission, accessed Feb. 25, 2019, https://www.sec.gov/litigation/investreport/34-84429.pdf.

What should public companies be doing?

While the SEC has not issued specific guidance on what companies should do, our financial and technical advisors have provided the following key recommendations. These recommendations are focused on prevention and detection of cyberfraud to mitigate potential reputational harm, financial loss or potential enforcement actions.

To combat a cyberattack like the one described within the SEC's report, an organization needs to ensure the highlighted prevention measures below are in place. In addition, processes and controls over vendor payments and payroll processing should be implemented and strictly followed. The preventative measures around vendor payments and processing are listed below as well.

General prevention measures

- Develop a fraud risk management program including the principals established within the revised 2013 Committee of Sponsoring Organizations of the Treadway Commission (COSO) framework as well as the joint COSO and the Association of Certified Fraud Examiners (ACFE) Fraud Risk Management Guide which begins with a comprehensive fraud risk assessment.
- Employ commercially available tools designed to help combat these attacks, including the performance of the tasks highlighted below:
  - Email addresses for those emails received from third parties should be flagged as "external."
  - External emails received from an address that has the name of key executives in the email address (e.g., an email from CEO.name@gmail.com) should be blocked. Emails with common misspellings and derivatives of the company's own domain name should also be blocked.
- Implement strong password requirements for all systems and devices, including those supplied by employees if they are going to be connected to the organization's network (including email connectivity).
- Implement virtual private network (VPN) technology across the mobile laptop environment to increase network security.
- Implement two-factor authentication (2FA) technology for all high-risk access points, including VPN and remote access to email.
- Mandate all employees receive security awareness training at least annually.
  - Offer targeted training on specific types of threats to a specific population (e.g., training for those who have the authority to release wires related to phishing attacks).
- Conduct periodic penetration assessments to test both the IT security infrastructure and social engineering prevention.
- Adopt a generally accepted cybersecurity framework, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework.
- Develop, maintain and regularly test a cybersecurity incident response plan.
  - Establish procedures to confirm whether cyberincidents have occurred and whether they were evaluated and disclosed in accordance with relevant laws.
- Engage a third-party professional services provider to evaluate cybersecurity and privacy compared with industry benchmarks and to obtain a listing of gaps for future remediation.

Fraudulent disbursement prevention measures
To ensure the organization is mitigating risk around fraudulent disbursements, we recommend a focus on three key areas: centralized payment processing, online banking, and vendor creation or updates.

Centralized payment processing: Well-defined internal controls including a centralized payment processing function are a leading practice given the increased transparency it provides regarding flow of funds out of the organization. In a cyberscam scenario, when processes are not followed properly, funds are released without the recipient being properly vetted and without knowledge by the necessary parties.

The following list contains a few examples of enhanced payment controls:

- Evaluate and document segregation of duties within the procure-to-pay cycle with a particular focus on manual wires and cash transfers.
- Develop monitoring and auditing plans which include historical dashboarding and a look back at high-risk disbursement activity. Develop a transactional testing program to evaluate compliance.
- Ensure someone from corporate is involved in the approval or release of an electronic payment. A threshold could be established so that corporate approval is required for wires over a certain dollar amount. Approval by finance should be obtained through direct phone discussion with senior executives.
- Restrict employee ability to open or close bank accounts.
- Restrict administrative access to online banking systems.
- Implement a global treasury management tool.

Online banking: As is true with central payment processing, online banking is tied directly to an organization's cash. Therefore, rigorous controls should exist to ensure that payments being released are going to the correct and appropriate parties.

The following list contains a few examples of enhanced online banking controls:

- Limit unauthorized changes to online banking user access by requiring dual authorization of changes by independent administrative users (control within the online banking application).
- Restrict changes to vendor banking information stored in wire templates by requiring dual authorization of changes (control within the online banking application).
- Require all outgoing wire transfers to be initiated and approved or released by separate users.
  - Additional approval thresholds should be established for wire transfers and automated clearing house (ACH) batches that exceed a certain dollar amount.
- Implement multifactor authentication (e.g., call backs for wire transfers over a certain dollar amount, key code sent to cell phone, etc.).
- Ensure ACH batch files are secured so that data output from the enterprise resource planning (ERP) system cannot be modified prior to upload into the online banking system.
- Restrict release of wire transfers from investment accounts to only internal bank accounts (e.g., the organization's main operating account) and not external vendors.
- Require periodic review (at least semiannually) of user access and authorized signers for all bank and investment accounts to confirm:
  - Access for terminated employees has been removed.
  - Access is appropriate based on the individual's current job responsibilities.

Vendor creation or updates: We have seen that many fraud schemes are executed through phony vendor accounts. Because of this, it is vital that organizations ensure their controls around vendor creation and updates are sound.

The following list contains a few examples of enhanced vendor controls:

- Restrict the creation of new vendors or processing of changes to existing vendors until an authorized signature is obtained, certifying standard operating procedures and checklist are completed to ensure all appropriate documentation has been received to validate the request.
- Require that all requests for changes to key vendor information (e.g., banking or routing numbers, address) are confirmed with the requestor either in person or via phone call.
  - A reply to an email received or using contact information contained within an email is not recommended.
  - This confirmation should be performed even if the request is coming from an internal email address.
- Perform an annual review of the vendor master file to remove duplicates, confirm that there are no employees listed as vendors (unless required for expense reimbursement), and identify and remove vendors that the organization no longer has a relationship with.

Fraudulent payroll prevention measures
Just as it is important to ensure the funds flowing out of an organization to vendors and third parties are validated appropriately, so too should the funds distributed to employees be validated.

The following list contains a few examples of enhanced payroll controls:

- Restrict access to employee direct deposit information through employee self-service portals, which require employee access via unique username and password. (Note: If employee banking information must be changed by payroll personnel, a discussion either in person or on the phone with the employee is required in order to validate the request.)
- Establish the segregation of duties so that employee payroll changes are reviewed and approved (agreed to source documentation) by individuals who do not have the authority to process changes in the payroll system.
- Require periodic reconciliation of active employees with payroll records.

Although these BEC attacks begin with computer skills and social engineering techniques, having the proper internal controls in place can limit the financial damage and reputational concerns that a company exposed to a cyberattack may face. By staying aware of emerging fraud techniques—and their impact on the company—you can better prepare yourself to avoid such issues in the future.

+1 800 274 3978
rsmus.com

tl-nt-ras-all-0119

RSM