Key Steps Towards Complying with SEC Accounting Controls

and how to ensure your company is protected against payments fraud

nsknox.net

nsknox

The SEC Has Affirmed: Organizations Must Act

Losses incurred by banks due to payments fraud is estimated to exceed $31 billion by 2018. (McKinsey)

In October 2018, the Securities and Exchange Commission (SEC) issued a report stating unequivocally that **companies need to consider the damaging implications of cyber threats** when designing and implementing internal accounting controls.

The report follows the SEC's investigation into the accounting controls of nine public companies that fell victim to cyber-fraud, each of which suffered a loss of at least $1 million, with one company having been defrauded in excess of $45 million.

In all cases, most of the money lost was unrecoverable.

Cyber-Fraud In Focus: Business Email Compromise

"The Federal Bureau of Investigation recently estimated that these so-called "Business Email Compromise" had caused over $5 billion in losses since 2013, with an additional $675 million in adjusted losses in 2017- **the highest estimated out-of-pocket losses from any class of cyberfacilitated crime during this period."** (SEC)

The SEC's investigation focused on a specific fraud known as **"Business Email Compromise" (BEC)**, in which fraudsters pose as company executives or vendors, using email communications to trick company personnel into transferring payments to bank accounts controlled by the perpetrators.

In some of these cases, **the fraud continued for months** and was often undetectable by incumbent processes and/or technologies.

Ramifications Beyond Financial Loss Alone

It appears that, for the time being, securities laws have not been violated, since no charges were brought against the victim companies or their personnel.

However, it should be noted that public companies subject to the internal accounting controls requirements of Section 13(b)(2)(B) of the Securities Exchange Act of 1934 **should adjust policies and procedures to adapt and respond to the emergence and growth of cyber-fraud.**

Failure to make the requisite adjustments **may in the future be deemed as a violation**, with potential implications being fines and/or the **debarment** of relevant company officers.

It is therefore anticipated that **auditors will likely be more conservative** and thorough in their scrutiny as to whether appropriately robust controls are in place. It is further contemplated that audits could even result in a refusal to sign-off on financial statements.

Challenges in Preventing Corporate Payments Fraud

Needless to say, there is a growing burden of change on companies to protect themselves against these risks. Yet, detecting and preventing corporate payments fraud presents significant challenges.

Organizations can turn to a checklist provided by the FBI, or to one of many articles authored by numerous consulting firms. However, following the guidelines outlined in these recommendations alone will not provide the requisite level of protection, as they depend on the absolute success and adherence to ever-changing requirements of employee education, training, and policy adjustments.

Conducting employee education and training, and adjusting policies – such as requiring two parties sign off on payment transfers, can only go so far.

The methods of cyber-fraudsters are extremely sophisticated, often leveraging technologies that are more advanced than those deployed to stop them. They are adept at exploiting a security framework's points of **vulnerability**, **manipulating** account information in the **master vendor data**, and sending convincing emails that **enable them to falsely** assume an executive's identity.

Policies, procedures, and education alone cannot provide a consistently dependable protective barrier. Fraudulent transaction attempts require automated, real-time detection and prevention.

Moreover, the responsibility of recognizing both clearly evident as well as hidden indicators of fraud should never be placed solely on the shoulders of even the most observant and conscientious employees.

This is an undertaking that should be performed by technologies and frameworks specifically designed to counter the complexity and sophistication of the techniques employed by cyber-fraudsters.

It is not sufficient to only attend to issues that the organization faces today. Rather, it is critical to get at the root cause of the issue and apply preventative measures at the deepest levels of technology, infrastructure, and process.

9 Key Steps & Capabilities

to Corporate Payments Fraud Prevention

The team at nsKnox have used their extensive, collective experience and domain expertise to define the key steps and capabilities that organizations should deploy when seeking to align with the SEC and to prevent corporate payments fraud.

1. **Real-time controls** should be established for **detecting threats and preventing attacks before they harm the organization** and its customers. Once an attack is underway it becomes extremely challenging to identify the source and sufficiently and satisfactorily mitigate damages.

   Real-time control is enabled, for example, by **analyzing payment data files at each step of the transaction journey**, where any change to the data (such as account or routing information) can be identified and the payment can be **blocked before the fraudulent transaction is completed.**

2. **Centralized and external controls** for all payment-related processes should be established. That is, it is critical to centralize payments controls and assessments, and to externalize and segregate this critical function from the organization's own internal network.

   Furthermore, these controls should not be dependent on the payment channel, in order to further reduce the risk of insider treats.

3. **A comprehensive list of payment corporate policies** should be defined, for example, a beneficiary or financial value of a payment request that does not comply with the company's pre-defined rules. **These payments must be automatically routed in real time to two individuals in the organization** who are authorized to make such approvals. Without both approvals, the payment should automatically be blocked.

4. **Maximum payment thresholds** for vendors should be defined, both for individual payments and for cumulative value across a given period of time. Payment requests that exceed theses thresholds, regardless of origin or source, should be automatically blocked in real time.

5. **Requests for payments from executives** must automatically be routed for verification by the executive as well as to another person in the organization as **an additional source of verification**, via means **other than a reply to the email** communicating the request.

6. **Requests for changes to vendor master file data** must be **automatically routed** for verification in real time to an authorized vendor representative. Verification should be executed through an **independent communication channel**, and not in a reply to the email request.

   Furthermore, within the paying and payee organizations, change approvals should be **provided by a minimum of two authorized individuals.**

7. **Email servers should be secured**, where **security monitoring tools and programs should be configured** to aid in the detection of suspicious activity, such as the receipt of emails or other communications coming in from unfamiliar addresses or from countries wherein cybercriminals are known to operate.

8. **Account verification** should be executed in systems/databases outside of the organization's network and limited to a small number of authorized employees, so as to reduce the risk of insider threats.

9. **Execute an independent KYC process** during supplier onboarding.

Detecting & Preventing Payments Fraud In Real Time: How nsKnox Can Help

nsKnox can assist companies to ensure alignment with the SEC guidelines and compliance with the Securities Exchange Act, protecting businesses against risks and financial losses by detecting and preventing payment fraud in real time.

With TxAuthority™, we ensure that every payment reaches the intended beneficiary, by securing the transaction with the approved supplier and account.

The solution analyzes every piece of data in the payment files, from initiation through fulfilment in the transaction journey, enabling the detection, alerting, and blocking of fraudulent payment attempts in real time.

Moreover, our unique approach of establishing external controls with a distributed framework, ensures that there is no single point-of-failure, delivering tamper-free protection.

To get started today with the only solution for real-time detection and prevention of corporate payments fraud, we invite you to reach out to us at **contact@nsknox.net.**