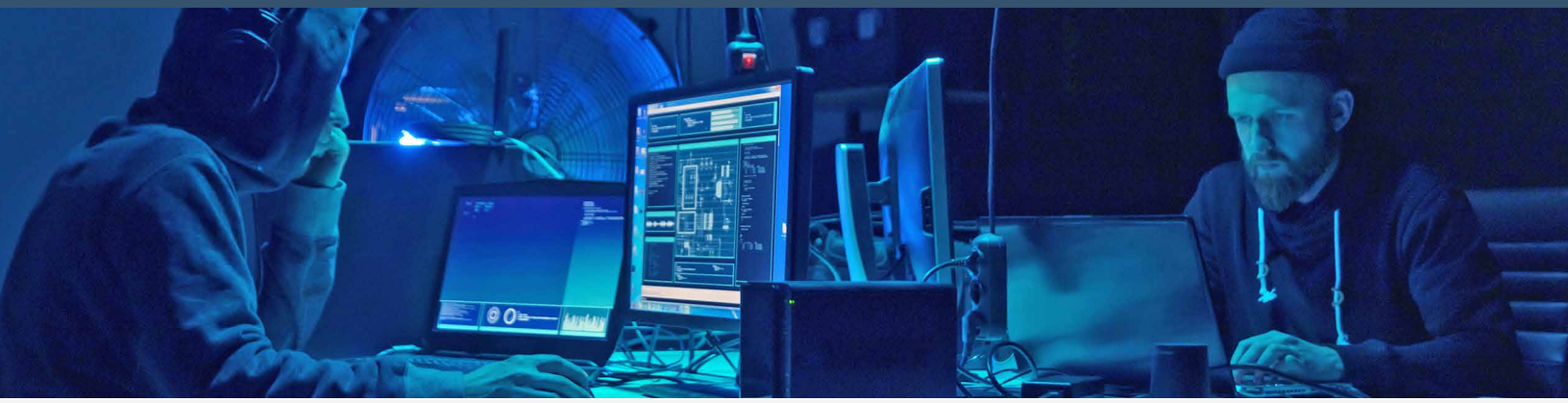
Fraud Lifecycle

Use a holistic approach

By Victor Hartman, JD, CPA, CFF, CFE



Due to fraud's potentially pervasive effect on an organization, a holistic approach is required to deal with the ecology of fraud. Understand the fraud lifecycle to take steps to understand, anticipate, prevent and detect fraud before significant damage occurs.

Consider several disparate frauds that can strike a healthcare organization. When a ransomware attack occurs, data is abruptly encrypted, patient care is put at risk, and the associated costs to mitigate damages can be astronomical.

A long-running embezzlement scheme by a senior executive can result in both significant losses and a breach of trust among a variety of stakeholders.

Lastly, a billing scheme that defrauds a federal healthcare program can require a sizeable reimbursement under the False Claims Act and may even result in the exclusion of the organization from all federal healthcare programs.

All these frauds originated in the mind of a fraudster, matured into a fraudulent act, and then left the victim organization to deal with the calamity. The maturation of fraud can be dealt with systematically by using a model that is known as the fraud lifecycle—prevention, detection, investigation, mitigation and remediation.

To understand how the fraud lifecycle model can be integrated into your organization's internal control and fraud response plan, two fundamental questions should be addressed.

- What frauds probably could occur in your organization?
- Why would a fraudster commit those frauds?

Once the *what* and *why* questions are answered, the results can be juxtaposed on the fraud lifecycle to develop a fully integrated approach for dealing with fraud in an organization.

What

Organizations face enormous challenges regarding fraud. Internal fraud risks are known as occupational frauds, and external frauds are known as non-occupational frauds. Internal frauds can be broken down into three categories: financial statement fraud, corruption and asset misappropriation.

The fraud lifecycle is prevention, detection, investigation, mitigation, and remediation.

Non-occupational frauds are quite varied but include business email compromise fraud and ransomware. Business email compromise is increasing, and annual losses are in the billions of dollars. The essence of the business email compromise fraud is that a fraudster poses as a vendor and instructs the victim to wire funds to the fraudster's account.

A common type of fraud occurs when a rogue actor in a healthcare organization intentionally submits false billings to a federal program such as Medicare. These predatory fraudsters create tremendous liability for themselves and their organizations.

Frauds vary in how they are executed, the motivation of the fraudsters, and the decision-making processes of the victims. Further, healthcare organizations face all the fraud risks of other businesses but have increased exposure to ransomware attacks and fraud involving government healthcare programs. For example, healthcare organizations may be more reluctant to patch a computer vulnerability for fear of interfering with expensive legacy medical equipment and software that is dependent on the network.

Your organization should perform a fraud risk assessment to identify the frauds that are most likely to occur and the estimated dollar loss. With data from the fraud risk assessment, a heat map can be created using frequency and loss estimates to assist in allocating resources to combat fraud.

Why

Fraud is a human act. Fraud is also an intentional act—not a mistake or accident—where a fraudster gains something of value at the expense of a victim. The psychology of why people commit fraud is complex. Although greed is often an easy answer for most frauds, a deeper dive will likely reveal different and more useful explanations.

As the various reasons of why people commit fraud in an organization are explored, the different motivations will often have a strong correlation to the different frauds identified in the fraud risk assessment. When the results from the what-and-why analysis are married up, an organization can more effectively address each component of the fraud lifecycle.

To make the *why* analysis easier, each fraud identified in the fraud risk assessment for the organization should be assessed. Occupational frauds—financial statement fraud, corruption and asset misappropriation—will be the most challenging to assess for likely motivations.

Occupational fraud

Financial statement fraud – Misstating the financial statements is the least likely to occur in an organization. However, when this fraud does occur, the result is likely the greatest loss. Putting the motivation of greed aside, causes of financial statement fraud may include ego, pride or shame by the leadership of the organization. For example, a hospital system chief financial officer who manipulates revenue by understating the allowance for doubtful accounts receivable may fear that his competency will be put into question if financial performance expectations are not met.

Corruption – The root causes of corruption can be challenging to understand. Corruption can include both public and private officials as well as both types of these officials when working together as part of a collusion scheme. An underlying motivation for corruption can lie with the phenomenon known as the social compact of reciprocity. The social construct posits that when one individual does a favor for another, the latter is likely to reciprocate in kind.

In the corporate environment, the free lunch leads to the free dinner only to be followed by a golf round or sport tickets. As the thing of value gets larger, the pressure to reciprocate increases. For example, healthcare providers may have financial ties to pharmaceutical companies or medical device manufacturers that influence their treatment decisions or research findings.

Asset misappropriation – Asset misappropriation is undoubtedly the most common type of fraud. Fortunately, the associated dollar loss is generally less than the other two types of occupational frauds. Probably the most common asset misappropriation fraud is procurement card abuse. The category can also include embezzlement and employee reimbursement schemes. Here, greed may be a more likely candidate for motivation but can also include financial need or a belief that everyone else is doing it.

Non-occupational fraud

The other category of fraud is non-occupational fraud where an outsider targets the organization. These bad actors can be thought of as predatory fraudsters, and common schemes include ransomware attacks and business email compromise.

Motivations for these frauds can include excitement or a gaming challenge among rogue internet actors where financial gain may be a secondary motivation. Other types of non-occupational frauds include bank fraud, insurance fraud and healthcare fraud whereby large institutional victims are defrauded for financial gain.

Fraud lifecycle

Every organization faces unique fraud risks. An understanding of these risks and the related motivation of fraudsters places an organization in a much better position to address all facets of the fraud lifecycle. The *what* and *why* questions should not be considered in a vacuum. An important part of this discussion involves the culture of an organization, including the importance placed on fraud prevention and detection, the willingness to be resilient, and how fraud matters are communicated to organizational stakeholders.

Prevention

Your organization's first line of defense is prevention. Fraud prevention can best be addressed through a functioning control environment. The control environment should include a combination of hard and soft controls. Both types of controls are the responsibility of management but can be tested by internal auditors.

Hard controls concepts are well known to management and internal auditors and are a function of experience and resource commitment. These controls can be described as preventive, detective and corrective. When a hard control fails, a fraud will eventually be detected, and a painful but finite loss incurred.

Soft controls can be more complex. Soft controls are intangible factors derived from an organization's culture that guide employees through their decision-making processes. Key factors involve the strength of the organization's trust, competency, integrity, training and shared values. A soft control failure can result in systemic damage to an organization—think Enron or WorldCom, or in the healthcare environment, a massive False Claims Act fraud involving a government healthcare program.

Once frauds and their associated motivations are identified, management has an opportunity to enhance the soft controls. The culture can be tweaked so that employees are motivated to do the right thing for the right reason.

Detection

Since all frauds cannot be prevented, organizational resources must also be focused on early detection. On average, fraud schemes run for about 18 months. If this timeframe can be shortened with robust detection strategies, losses will correspondingly decrease. The ability of an organization to detect fraud early is also a function of the control environment. A key question you should ask during a fraud risk assessment is: If someone sees a red flag, will they feel comfortable reporting it?

Defining fraud as a human act is axiomatic, and the manner of fraud detection should be just as obvious—by a human. Although technology should be a part of an integrated solution, the most prevalent way fraud is detected is from an employee, customer or vendor. Having a well-publicized ethics program and hotline that is communicated to internal and external stakeholders is one of the most effective ways to detect fraud.

Lastly, whistleblowers are more likely to report internally before seeking external vindication. Your organization should have a fraud policy with an escalation protocol so that all complaints are evaluated timely and appropriately. If this process fails, an aggrieved whistleblower may report externally to the Federal Bureau of Investigation, Health and Human Services Department, Securities and Exchange Commission or to a whistleblower attorney.

Investigation

Once a fraud has been detected, your organization must respond with an appropriately staffed investigation to discover the facts surrounding the fraud. The goals of the investigation will include identifying the fraudster(s), understanding internal control weaknesses, and assessing the legal elements needed for a civil or criminal action. Internal auditors are a good choice for staffing an investigative team due to their inquisitive nature and knowledge of the organization.

The most important aspect of an investigation is interviewing the fraudster. Knowing the type of fraud that was committed and the likely motivation of the fraudster is critically important to the interviewer. Understanding the motivation will shed light on how the fraudster rationalized his or her conduct. With these insights, the interviewer has the greatest chance of obtaining cooperation, a confession and voluntary restitution.

Consider how fraud matters are communicated to your organizational stakeholders.

Mitigation and remediation

Mitigation is a process of minimizing the collateral effects of fraud on the organization as well as ensuring that the fraud never occurs again. A ransomware attack is a good example. Mitigation will involve stopping the cyberattack, making the decision whether to pay the ransom, recovering network data, and beginning the process of restoring stakeholder trust.

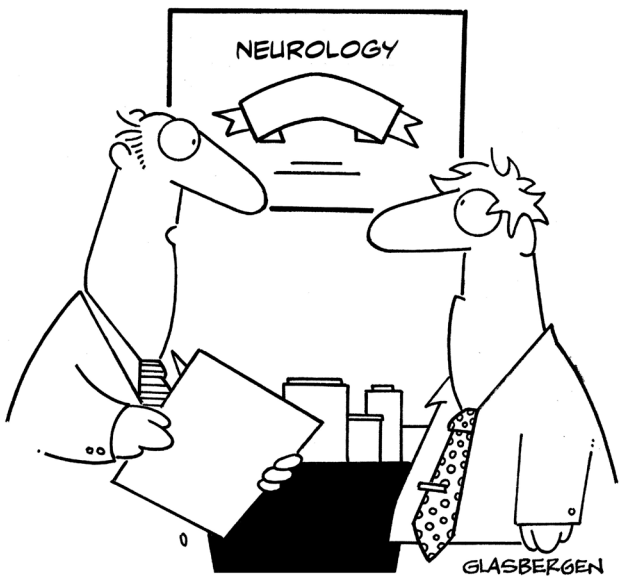
As the mitigation process begins, the organization will begin considering the longer-term goals of making itself whole through remediation. The quickest way to achieve this may be through a fidelity insurance policy or cyber insurance policy. Remediation also includes holding the responsible parties accountable through civil or criminal actions. The goal of remediation is to try to recoup losses through financial recovery.

Conclusion

Fraud is an unfortunate cost of doing business in an organization. The fraud lifecycle model holistically enables your organization to plan for a fraud event. Begin by understanding the fraud threat picture—the *what* question. Next, understand the motivation for the fraud—the *why* question. A correlation usually exists in the answers to these questions. With this information in hand, your organization will be much better equipped to deal with each phase of the fraud lifecycle—prevention, detection, investigation, mitigation and remediation. **NP**

Victor Hartman, JD, CPA, CFF, CFE, is Principal of The Hartman Firm, LLC, specializing in forensic accounting and internal investigations. He was an FBI Special Agent. He is now an Adjunct Professor at Georgia State University and serves on Georgia Southern University's Forensic Accounting Advisory Board. Vic can be reached at 404-369-0616 and Vic@HartmanFirm.com.

©Glasbergen
glasbergen.com



"I have the results of your brain scan. We found evidence of extensive PowerPoint damage."

pwc

The New Equation is where advanced tech, data and expertise come together.

Reimagine cyber, risk and regulation to build trust and drive sustained outcomes.

It all adds up to The New Equation.

Learn more at
www.pwc.com/us/hirr

© 2023 PwC. All rights reserved. PwC refers to the US member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.