DECEMBER
2022

INSIDER THREAT FRAUD

JOB AID

CDSE Center for Development of Security Excellence

INTRODUCTION

This job aid will provide information about risks associated with fraud and guidance for organizations to prevent, detect, deter, and mitigate threats posed by insiders who may use trusted access to commit fraud. This job aid includes insider threat fraud data from the Association of Certified Fraud Examiners (ACFE), Report to the Nations. The Center for Development of Security Excellence (CDSE) has established an insider threat fraud tab on the insider threat toolkit on the CDSE website to provide additional training and awareness resources related to insider threat fraud which can be accessed via the following URL: https://www.cdse.edu/Training/Toolkits/Insider-Threat-Toolkit/

WHAT IS FRAUD AND HOW DOES IT RELATE TO INSIDER THREAT?

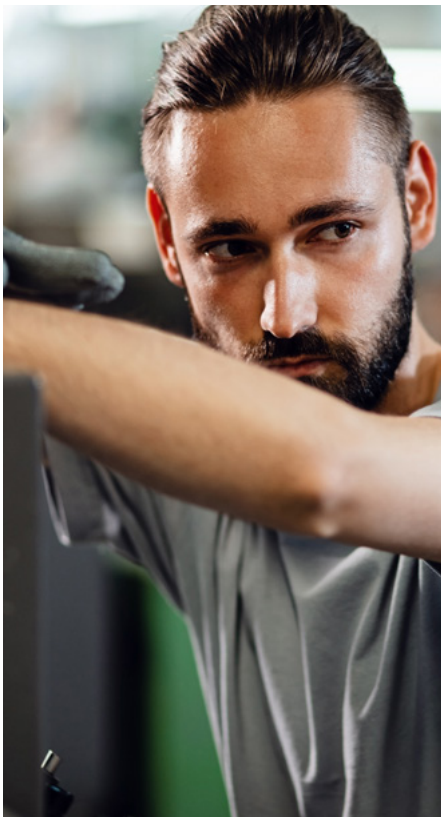
Fraud is "any activity that relies on deception in order to achieve a gain". Fraud becomes a crime when it is a "knowing misrepresentation of the truth or concealment of a material fact to induce another to act to his or her detriment" (Black's Law Dictionary). In other words, if you lie in order to deprive a person or organization of their money or property, you're committing fraud. Trusted employees with access to systems, data, information or other assets can potentiallyuse that access to commit fraud.

WHO ARE THE PERPETRATORS OF FRAUD?

- Owners/Executives (Avergage of $337,000 of losses caused by fraud) - Owners and Executives only committed 23% of the fraud but they caused the highest losses.
- Manager (Average of $100,000 of losses caused by fraud.)
- Employee (Average of $50,000 of losses caused by fraud.

High-ranking managers and employees with trusted access to internal documents, data, and assets and control over processes such as ethics, oversight, processes, and policies have more opportunity and ability to commit fraud.

85% of fraudsters displayed behavioral redflags of fraud, and only 6% had a prior fraud conviction.



WHY DO PEOPLE COMMIT FRAUD?

The most widely accepted explanation for why some people commit fraud is knows as the Fraud Triangle, which is illustrated below. The Fraud Triangle was developed by Dr. Donald Cressey, a criminologist whose research on embezzlers produced the term "trust violators."

The Fraud Triangle hypothesizes that if all three components are present - unshareable financial need, perceived opportunity and rationalization - a person is highly likely to pursue fraudulent activities. As Dr. Cressey explains in the *Fraud Examiners Manual:*

> When the trust violators were asked to explain why they refrained from violation of other positions of trust they might have held at previous times, or why they had not violated the subject position at an earlier time, those who had an opinion expressed the equivalent of one or more of the following quotations: (a) 'There was no need for it like there was this time'. (b) 'The idea never entered my head.' (c) 'I thought it was dishonest then, but this time it did not seem dishonest at first.'

Just as in the Critical Path model commonly utilized by counter-insider threat professionals, the fraud triangle has pressure, and while financial pressure is the number one reason insiders may commit fraud, other pressures coupled with opportunity and rationalization may contribute to the overall risk picture. Just as in the Fraud Triangle, deterrence can prevent opportunities to commit indiser threat acts to include fraud. Insiders may use rationalization to justify their actionssuch as not getting a salary increase, promotion, or that their actions really are acceptable and accepted within the organizational culture.

CATEGORIES OF FRAUD

Unfortunately, fraud is so common that it can be categorized in countless ways. But fundamentally, every type of fraud is either organizational or individual. Let's look at some key characteristics of each.

AGAINST INDIVIDUALS

This is when a single person is targeted by a fraudster - including identity theft, phishing scams and "advance-fee" schemes. Perhaps one of the most noteworth and devastating individual frauds is the Ponzi scheme.

INTERNAL ORGANIZATIONAL FRAUD

Sometimes called "occupational fraud," this is when an employee, manager or executive of an organization deceived the organization itself. Think embezzlement, cheating on taxes, and lying to investors and shareholders.

EXTERNAL ORGANIZATIONAL FRAUD

This includes fraud committed against an organization from the outside, such as vendors who lie about the work they did, demand bribes from employees and rig costs. But customers sometimes defraud organizations, such as when they submit bad checks or try to return knock-off or stolen products. And, increasingly, technology threatens organizations with theft of intellectual property or customer information.

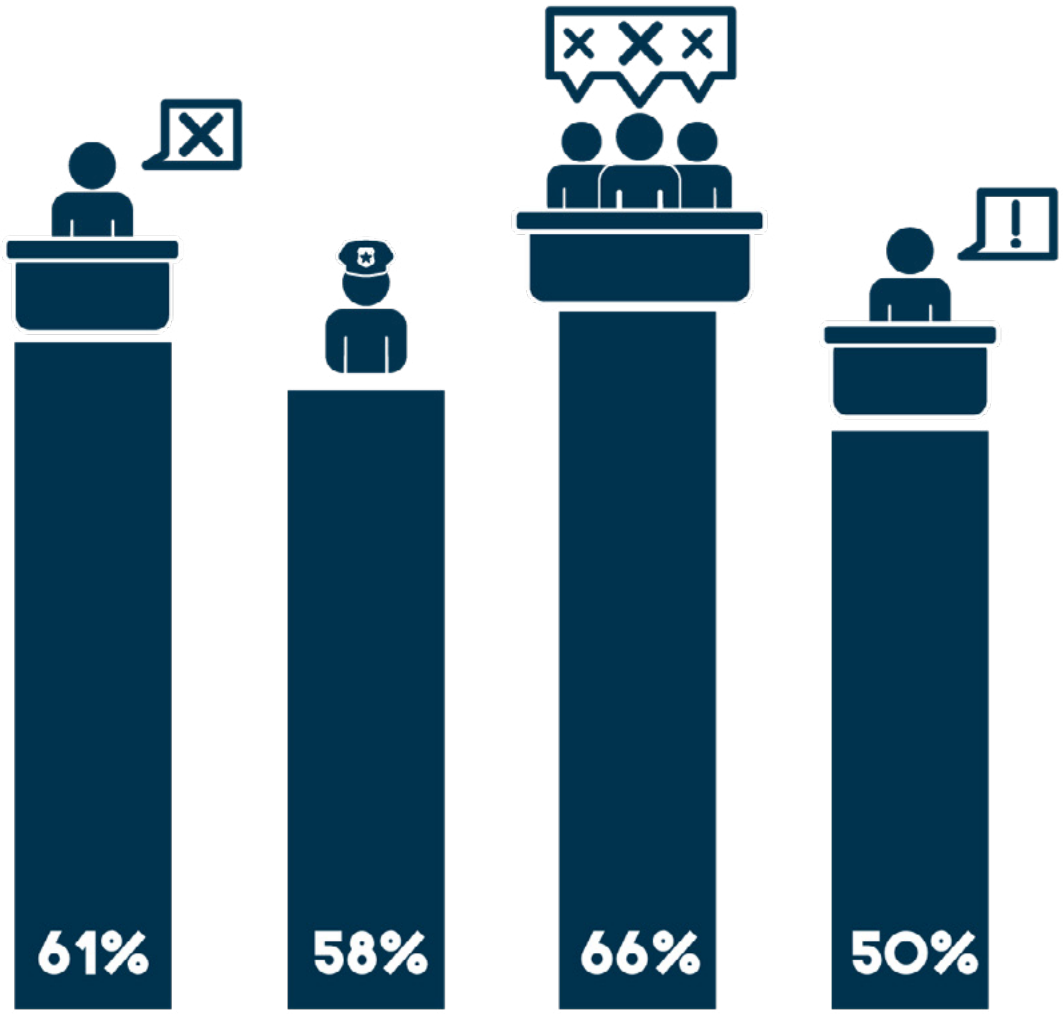
THE COST IMPACT OF FRAUD

- The global cost of fraud is estimated to be $4.7 trillion dollars based on a global economy of almost $95 trillion.
- Reported fraud is 2,110 cases from 133 countries accounted for $3.6 billion of total losses.
- Organizations lose an estimated 5% of revenue each year or $1,783,000 loss per case.
- A typical fraud case lasts 12 months before detection and causes a median loss of $117,000.
  - 15% in Operations
  - 12% in Accounting
  - 10% in Executive Level
  - 10% in Sales
- Corruption was the most common fraud scheme in every global region.
- 8% of fraud involved use of cryptocurrency and 48% involved bribery and kickbacks.
- Organizations with the fewest employees had the most median loss ($500,000).

FRAUD DETECTION AND REPORTING

- 42% of fraud was detected by tips which is three times more than the next most common method, and a half of those were reported by employees.
- Email (40%) and web-based (33%) reporting surpassed telephone reporting (27%).
- Organizations with hotlines detect fraud more quickly (12 months and $100,000) and had lower costs than organizations without hotlines (18 months and $200,000).
- Nearly half of fraud cases occurred due to lack of internal controls (29%) or override of existing controls (20%).
- 81% of organizations modified their anti-fraud controls following a fraud incident with 75% increasing their management review procedures and 64% increasing the use of data monitoring analysis.

ACTIONS TAKEN AGAINST FRAUDSTERS



61% of fraudsters were terminated by their employer.

58% were referred to law enforcement.

66% of cases referred to law enforcement resulted in a conviction.

50% of organizations that didn't refer their cases to law enforcement cited internal discipline as the reason.

QUESTIONS FOR ORGANIZATIONS REGARDING INSIDER THREAT FRAUD

1. Does your fraud awareness training incorporate insider threat fraud training and awareness in its training? Is it included as part of the counter-insider threat program or risk mitigation program? Does it include relevant case studies?
2. Did your organization have any incidents of fraud? If so, to what extent and what was done to prevent future fraud?
3. What impacts would fraud have on your organization? Monetary? Branding? Impact to employees?
4. What processes are in place to prevent, detect and investigate fraud?
5. What policies are in place to report and investigate fraud?
6. Which employees are the most likely to commit fraud in your organization? What controls are in place to watch those with control or "watch the watchers?"
7. Does your organization have a tip hotline for reporting fraud? Is it anonymous and does it provide follow up so employees know action is being taken?

WHAT ARE SOME MEASURES YOUR ORGANIZATION CAN TAKE AGAINST THE RISK OF FRAUD?

- Conduct fraud training relevant to your organization.
- Establish processes and policies to deter, detect, report, investigate, and take action when fraud does take place.
- Establish an anti-fraud culture at all levels - all employees from the top down should know the organization is serious about fraud.
- Work with anti-fraud partners to leverage resources that are not inherent to your organization.
- Have a counter-insider threat or risk mitigation section that includes fraud as one of its priorities.
- Establish an employee fraud tip line that is monitored and acted upon, and follow up as applicable.

ADDITIONAL RESOURCES

Insider Threat Fraud Tab - https://www.cdse.edu/Training/Toolkits/Insider-Threat-Toolkit/

Association of Certified Fraud Examiner's Website - https://www.acfe.com

Potential Risk Indicators: Insider Threat (Job Aid) - https://www.cdse.edu/Portals/124/Documents/jobaids/insider/INTJ0181-insider-threat-indicators-job-aid.pdf

Department of Justice - Report Fraud - https://www.justice.gov/criminal-fraud/report-fraud

Department of Treasury - Report Fraud - https://home.treasury.gov/services/report-fraud-waste-and-abuse

Department of Defense Whistleblower and Fraud Hotline - https://www.defense.gov/Help-Center/Article/Article/2763108/dod-inspector-general-hotline-and-whistle-blower-protection/