Ponemon INSTITUTE

THE RISK OF INSIDER FRAUD

SECOND ANNUAL STUDY

Executive Summary

SPONSORED BY Attachmate

Independently conducted by Ponemon Institute LLC

Publication date: February 2013

Part 1. Introduction

Ponemon Institute and Attachmate are pleased to present the results of the *Risk of Insider Fraud: Second Annual Study*. The first study was published in October 2011. The findings from this year's study show that the insider threat has become more of a challenge for IT professionals.

The number of employee-related incidents of fraud continues to remain high. However, only 44 percent say their organization views the prevention of insider fraud as a top security priority and this perception has declined since 2011. Contributing to the insider risk is BYOD, employee access of enterprise systems from remote locations and lack of security protocols over edge devices.

In our study, we defined insider fraud as the malicious or criminal attacks perpetrated upon business or governmental organizations by employees, temporary employees and contractors. Typically, the objective of such attacks is the theft of financial or information assets — which include customer data, trade secrets and intellectual properties. Sometimes the most dangerous insiders are those who possess strong IT skills or have access to your organization's critical applications and data. Other risks with potentially severe consequences are the intentional misuse of data or policy violation.

Some of the most salient findings from this study are the following:

- On average, organizations have had approximately 55 employee-related incidents of fraud in the past 12 months.
- More than one-third say that employees' use of personally owned, mobile devices has resulted in malware and virus infections that infiltrated their corporate networks and enterprise systems and another 26 percent it is very likely to occur.
- Sixty-one percent rate the threat of insider fraud within their organization as very high or high.

On average, organizations have had approximately fifty-five employee-related incidents of fraud in the past 12 months

- Twenty-three percent say insider fraud incidents existed six months or longer before being discovered and nine percent could not determine when they occurred.
- Fifty-five percent of organizations say their organization does not have the ability/intelligence to determine if the off-site employee's non-compliance is due to negligence or fraud.

Using survey methods, we implemented an objective study about how highly experienced individuals in IT, security, compliance and other business fields deal with the risk of fraud perpetrated by malicious insiders. Our study attempts to ascertain what these individuals perceive to be the most serious vulnerabilities in their organizations and how they can improve IT, governance and control practices that reduce fraud and ensure compliance with regulations.

Our sample consists of 743 individuals (respondents). On average, respondents have more than 10 years of experience and the majority is positioned at or above the supervisor level. Seventy-eight percent of respondents report to the CIO or CISO. While all respondents are located in the United States, many of their organizations are multinational or with operations in other countries.

Part 2. Key Findings

Insider fraud is a common occurrence. On average, organizations have had approximately 55 employee-related incidents of fraud in the past 12 months. This translates to slightly more than one fraud event perpetrated by a malicious insider per week and is virtually unchanged from last year's study that reported an average of 53 incidents of fraud in a 12-month period.

In this year's study, there was an increase from 76 percent to 79 percent of respondents who say that in their organization a privileged user has or is very likely to alter application controls to access or change sensitive information and then resets the controls or it is very likely to happen.

According to 74 percent of respondents, an employee's malfeasance has caused financial loss and possibly brand damage. Seventy-seven percent of respondents say their organizations already have experienced or will likely experience someone accessing private customer data with above-average frequency—signaling a possible data breach. Seventy-nine percent say they already had an employee use someone else's credentials to gain elevated rights or to bypass separation-of-duty controls or it is likely to happen.

Sixty-one percent of respondents say that the insider risk in their organizations is either very high or high but a smaller percentage of respondents (44 percent) believe that their organization considers the prevention of insider fraud as a top

security priority. Evidence that it is not considered a priority is respondents' agreement that technologies and governance practices are not adequate to stop insider fraud.

Moreover, the problem is getting worse since the first study. In the past 12 to 24 months, 33 percent say the risk has worsened (versus 23 percent in last year's study) and 51 percent say it has stayed the same (versus 62 percent in last year's study).

In this year's study there is a decline in the belief that organizations consider prevention of insider fraud a top security priority.[1] Sixty-six percent strongly agrees or agrees that their organization has adequate policies to prevent or curtail insider fraud, including employees' unauthorized access or misuse of IT resources. However, less than half say the organization has technology, resources and governance controls and procedures to address the risk.

New insider fraud risks are a challenge to manage. Almost half (48 percent) of respondents say that BYOD has resulted in a significant increase in fraud risk and 77 percent of respondents say the lack of security protocols over edge devices presents a significant security challenge and risk.

Twenty-nine percent say it has already happened that a lack of security controls over edge devices provided a pathway for insiders to inappropriately access, misuse or attack mission critical systems. Thirty-two percent anticipate that such access is very likely to occur. Thirty-four percent of respondents say that employees' use of personally owned, mobile devices (such as a smart phone or tablet computer) in the workplace has already resulted in malware and virus infections that infiltrate corporate networks and enterprise systems. Another 26 percent say such infections are very likely to occur.

Mobility, edge devices and BYOD increase the insider fraud risk. The majority of IT practitioners surveyed in this study say these factors have increased the insider fraud threat. Seventy-seven percent say the lack of security protocols over edge devices presents a significant security challenge and risk. This is followed by 75 percent who say BYOD has significantly increased security risks.

With more employees and contractors working outside the office, it is not surprising that 72 percent of respondents say the risk of insider fraud has increased because of remote access of the enterprise systems from home offices, hotel rooms, public transportation, restaurants and conferences. Further, 70 percent say the use of mobile devices complicates their organization's ability to secure and track access to data.

[1]We measure respondents' perceptions using a five-point scale from strongly agree to strongly disagree to each attribution or statement. A favorable rating is defined as a strongly agree and agree response more than 50 percent (or a strongly disagree, disagree and unsure combined response at or below 50 percent.

The time it takes to investigate insider fraud makes these incidents difficult to resolve.

Ability to work in off-site locations creates opportunities for fraud. Due to increased worker mobility**,** policies and technologies need to improve in order to reduce insider fraud risk. The risk is not only the tendency of employees not to comply with policies but for most organizations there is the inability to determine if such non-compliance is occurring. Moreover, the majority of organizations admit to not being able to differentiate between non-compliance that has occurred as a result of negligence or fraud.

Edge devices and BYOD make it difficult to identify insider fraud. Fifty-eight percent agree that BYOD makes it more difficult for the security or compliance department to have complete visibility of employees' access and computing activities. The majority of respondents (78 percent) **do not agree** that employees' access and possible misuse of edge devices is completely visible to the security or compliance department.

The time it takes to investigate insider fraud makes these incidents difficult to resolve. On average, it takes 87 days to first recognize that insider fraud has occurred and more than three months (105 days) to get at the root cause of the insider fraud incident and to determine the consequences to the organization.

On average about one-third (34 percent) of these investigations result in actionable evidence against the perpetrators, which means the majority of these incidents go unpunished making organizations vulnerable to more such incidents. This is unchanged since last year's study.

More organizations are using forensic specialists to investigate insider fraud. As discussed above, insider fraud is getting worse and the time it takes to resolve longer. The primary method of investigation is to have anti-fraud or forensic specialists conduct independent investigations followed by an investigation by the internal auditors.

Organizations face multiple challenges in their efforts to reduce insider fraud risks. These challenges are: employee awareness, executive-level priority, resources and available technologies. The threat vectors most difficult to secure are mobile devices, outsourced relationships (including cloud) and applications.

A lack of visibility into employees' access and computing activities is a deterrent to reducing insider fraud.[2] Only 26 percent of respondents agree that when they are logged into the organization's systems, employees' access and computing activities are completely visible to the IT department. This is similar for security and the business unit (24 and 32 percent, respectively). These findings also indicate that the lack of visibility has not improved.

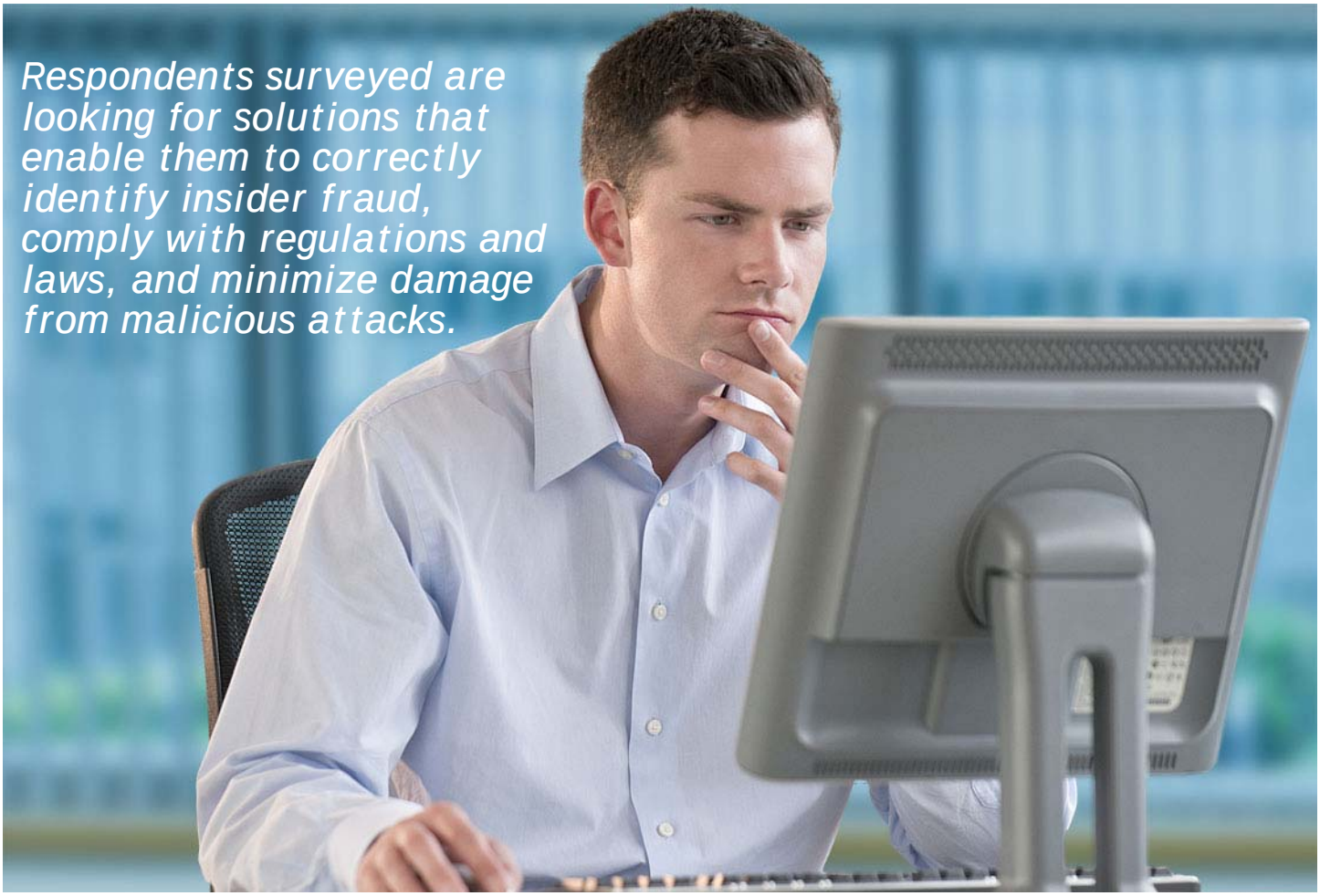
[2]Ibid, Footnote 2

The main drivers for deploying an enterprise fraud management (EFM) solution focus on detection, compliance and damage control. Respondents surveyed are looking for solutions that enable them to correctly identify insider fraud, comply with regulations and laws, and minimize damage from malicious attacks.

The majority of respondents (70 percent) believe log files for raising the level of visibility into what employees do when logged onto the organization's network or enterprise system is either very important or important. However, 79 percent respond that it is very difficult and difficult to use log files. This belief is due to the difficulty in observing employee fraud, misuse or policy violations when logged onto the organization's network or enterprise system.

As a strategy to combat insider fraud, respondents say their organizations have implemented enabling security technologies and governance and control practices. When asked what technologies their organizations believe are important to address the risk of insider fraud. The perceptions about technologies have not changed significantly since 2011. These are network intelligence, mobile device management data loss prevention, identity & access management and enterprise fraud management.

More organizations are deploying EFM solutions. There has been an increase in organizations that have fully or partially deployed an EFM solution and more are expected to deploy it within the next 12 to 24 months. Among those organizations that have fully or partially deployed such a solution, 60 percent say the return on investment (ROI) in terms of mitigation or minimizing insider fraud is either very significant or significant.



Conclusion

The findings suggest that the majority of organizations are not assigning the appropriate priority to the risk of insider fraud. As a result, the risk seems to be getting worse as is evidenced by the length of time it takes to detect and resolve these incidents.

Some recommendations to address these risks include making training and awareness an important component of a security initiative. Employee education and policies need to be supported by EFM solutions, DLP and other monitoring technologies. Finally, access privileges need to be monitored. They also need to be appropriate for the employee's role and responsibility.

Ponemon INSTITUTE

ADVANCING RESPONSIBLE INFORMATION MANAGEMENT

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

As a member of the Council of American Survey Research Organizations (CASRO), we uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.