SearchSecurity.com **E-Book**

Online Fraud: Mitigation and Detection to Reduce the Threat of Online Crime

As our economy struggles to regain its footing, online fraud is more prevalent than ever. In this E-Book, experts reveal a model for common fraud and present tips on easing fraud pains. Also, find out how financial fraud affects consumer bank behavior.

Sponsored By:

SearchSecurity.com **E-Book**

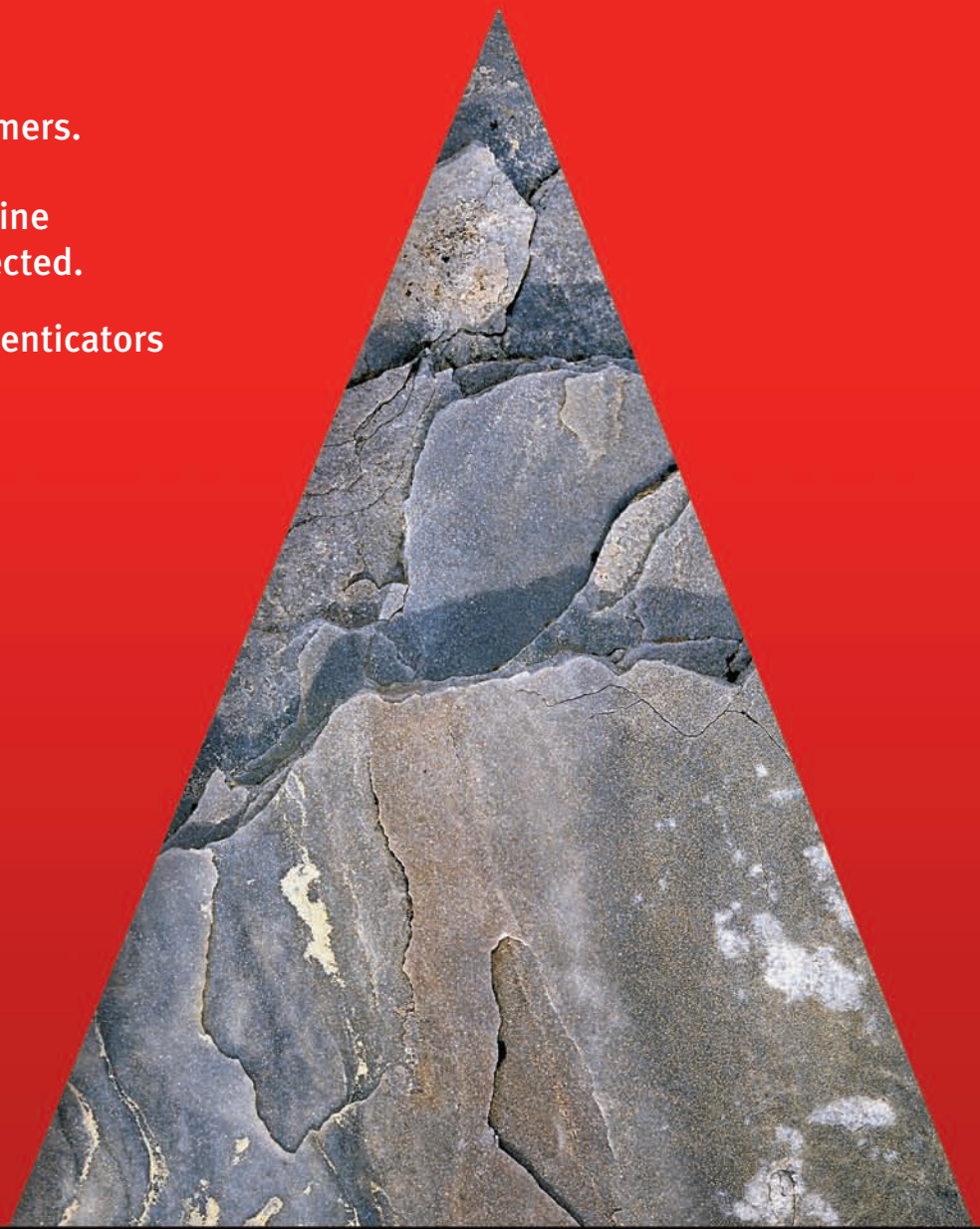
Online Fraud:
Mitigation and Detection to Reduce the Threat of Online Crime

Table of Contents:

34,000+ customers.

200 million online identities protected.

40 million authenticators deployed.



For an authentication solution that is truly strong,

Find security in RSA.

RSA®

The Security Division of EMC

www.rsa.com

Security Information and Event Management | Data Loss Prevention | Identity & Access Management

Insider threat mitigation and detection: A model for committing fraud

by Ron Woerner

On almost any given day you can find a news story about an employee who has gone bad and committed fraud or damaged an organization. Insider threat is a timeless problem. It's always been there and it always will be there. Why? Because companies need to trust their employees in order to stay in business.

The most widely accepted model for explaining why people commit fraud is the fraud triangle created by noted criminologist and sociologist Dr. Donald Cressey in the early 1950s. According to Cressey, three factors must be present at the same time in order for someone to commit a security breach: pressure or motivation, rationalization and opportunity.

Today's electronic society has changed this model. In Cressey's time the incentive was mostly financial, but now there are many other reasons why a person may bypass security or commit fraud. In the early days of IT, hackers wanted fame or were just curious to see if they could pull off an exploit. These days the motive may be revenge against the company or an employee, which is not financially related. Pressure to get the job done no matter what may also cause someone to skirt security.

Therefore, I postulate that there is a new fraud model to consider. To commit fraud, or any other improper action, a person needs the following three elements: access, knowledge/ability and intent.

Access: Physical or logical ability to enter, touch or reach a resource. In computers, this is often controlled by network rules, access control lists (ACLs) and a user ID and password.

Knowledge/Ability: Familiarity or experience with an object or resource. This means knowing what to do after accessing the resource.

Intent: The purpose or an anticipated outcome that guides a person's planned actions; knowingly causing damage to the resource.

Here's an example of how these elements fit together. Suppose I have a logon ID and password to our mainframe computer, therefore I have access. Not only that, but I am given full administrator rights to it. The problem is I'm a neophyte on the mainframe-I barely know how to log on. Plus, I like my organization and don't want to cause it harm. Therefore, I'm missing two of the three requirements for fraud: knowledge and intent. Even though I have access, there is little risk of my causing intentional harm.

Access and knowledge are the elements most under our control (it's impossible to audit intent). If you can reduce a user's access/authority or increase the controls (which requires the attacker have more knowledge), then you reduce the risk. You must also ascertain what is required for the exploit. Many vulnerabilities require uber-hacker abilities to exploit them, like freezing the memory chips to bypass disk encryption. However, while only a minute percentage of people can normally exploit such vulnerabilities, there are increasingly more script kiddie tools available to reduce the knowledge level required.

Insider threat mitigation: Fraud detection model

Keeping the new fraud model in mind, an organization can prevent fraud by having the following processes in place:

* Separation of duties
* Background checks, including a financial records check
* Job rotation/cross-training
* Protecting and limiting access to administrator accounts
* Role-based access control (RBAC)

By considering the access, knowledge and intent required to compromise a system, you can make more intelligent risk decisions. Furthermore, using these concepts promotes the proper balance of security within an organization, thereby reducing costs while improving security.

You can't identify an insider threat you can't see.

EnCase® Cybersecurity allows you to investigate suspected misconduct from a central location with no disruption to business. Find out why more than half of the *Fortune* 100 rely on EnCase® software to investigate and expose fraud.

Visit www.guidancesoftware.com for more information

EnCase® Cybersecurity

Guidance® SOFTWARE
The World Leader in Digital Investigations™

Investigation management tools ease fraud pains

Michael Rasmussen, Contributor

Financial service organizations are often in disarray when it comes to having consistent processes and technologies for managing fraud investigations and loss. The disarray is a result of:

> "In today's complex and distributed financial services environment, an organization ... needs a 360-degree view of enterprise fraud investigations."

Fragmentation. Financial service organizations often lack a common platform for managing enterprise-wide investigations, fraud, incidents, issues, events, complaints and/or loss. Instead, different business groups within the organization manage corporate investigations in their own silos.

Inconsistency. These fragmented investigation processes are poorly defined and do not provide an enterprise visibility into incidents and loss. As a result, the organization has a variety of methodologies ranging from the ad hoc to the mature.

Misuse of technology. Financial service organizations tend to have an abundance of homegrown spreadsheets, custom-built databases, and perhaps an occasional commercial product thrown into the mix. There is limited adoption of enterprise technology to manage fraud investigations processes.

This is cause for concern. In today's complex and distributed financial services environment, an organization, from both a compliance and operational risk perspective, needs a 360-degree view of enterprise fraud investigations and loss. Corporate governance, strategic decision-making and the protecting stakeholder value require understanding where the greatest incidents and losses have been.

Further, the over reliance on spreadsheets and homegrown databases to manage investigations should raise issues with legal and corporate compliance departments. These systems lack the robust audit trail found in commercial applications. Spreadsheets in particular should be avoided for managing investigations as they fail to demonstrate the integrity of the information and who entered it (what is referred to as non-repudiation).

Consistency is key

The first step in overhauling a financial organization's fraud investigation management approach is to think 'enterprise.' A common process for managing enterprise investigations provides for collaboration, consistency, efficiency, accountability, and transparency.

Collaboration on fraud investigations requires that the organization implement an enterprise platform for managing fraud investigations. Enterprise investigation platforms provide a common and consistent

approach to reporting incidents (e.g., hotlines), handling escalation, managing the investigation process, and analyzing loss. The platform enables an organization to evaluate the criticality of incidents, assign investigation/response team members, monitor business impact and regulatory requirements, manage the investigation process and report on loss/impact.

An enterprise approach provides incident data across business units, processes, and relationships. It allows the organization to maintain detailed investigation history and audit trails, manage the lifecycle of investigations, link incidents to remediation procedures, and identify trends to monitor similarities and relationships in investigations. This in turn allows the organization to understand all of its mitigation and prevention requirements.

Financial organizations considering an enterprise fraud investigation platform should consider the following in their selection process:

- **Investigations process management.** The platform should have a lifecycle approach with robust process management capabilities. Process management capabilities provide the ability to prioritize, assign, and track incidents from identification to resolution. Within each incident, the organization should have the ability to assign a lead investigator and support staff as well as the capability to notify personnel when incidents enter their case management queues. Look for visual workflow modeling, process flowcharts, and task management features. This includes project management capabilities to assign and manage the calendars and resources assigned to investigations.

- **Investigations content management.** A strong investigations management tool also provides a breadth of content management functionality, including content repository, version control, access management, and records and retention management for investigations.

- **Enterprise loss analysis.** The platform should have robust capabilities to categorize, measure, allocate, record, import (external loss data) and report on fraud and losses across the organization. This includes analytic capabilities to model and report on loss trends, such as root cause and trend analysis, ability to report on loss/event data to the control environment, as well as functionality to provide for loss distributions and calculations).

- **Remediation management.** Related to the process and project features, a platform should have the ability to track and manage the remediation process. Specifically, organizations should look for the ability to track and monitor the status of remediation, such as recognized control gaps, audit findings, and regulatory interactions/reporting.

- **Hotline.** Another important feature to look for is the ability to integrate with the organization's anonymous hotline/whistleblower system for reporting incidents and events.

• **Security architecture.** Investigations management platforms are effective only if the financial organization can tightly control access to sensitive information. Data security is a critical element to consider in an investigations platform -- and an inherent weakness in spreadsheets and personal databases. Features should include elements such as: role based administration of privileges, integration with directory services, secure access incident data down to the individual field level, protection of the identity of the individuals involved, and ensuring the integrity of your organization's confidential
information.

• **Reporting and dashboarding.** A full-bodied investigations management platform provides an easy-to-use interface for reporting and managing investigations. Specific features to consider include the ability to monitor investigation status, produce reports that measure and report on impact, and other reports to track incidents by type, date, person, location, financial impact, and other attributes. Dashboards are also essential and should provide management with real-time access to current incidents, their resolution status, key metrics, and the relationship of incidents/events. That will enable the organization to identify trends and relationships.

• **Configuration flexibility & usability.** The strongest tools support flexible configuration without customization of code. The entity can manage structures, rules, workflow, and user-interface characteristics without customization. Investigation personnel should be able to use the system without being technically savvy. Select a platform that has an intuitive look and feel with navigation and an information presentation that minimizes the need for user training.

About the author:

Michael Rasmussen (mrasmussen@corp-integrity.com) is with Corporate Integrity, LLC. Michael is the authority in understanding governance, risk and compliance (GRC). He is a sought-after keynote speaker, author and collaborator on GRC issues around the world and is noted for being the first analyst to define and model the GRC market for technology and professional services. Corporate Integrity, LLC is a strategy & research advisory firm providing education, research and analysis on enterprise governance, risk management and compliance.

>IMAGE GENERATED USING VISIBLE, UNENCRYPTED EMAIL TRAFFIC

>THESE ARE UNENCRYPTED EMAILS
>THEY ARE VISIBLE TO THE WHOLE WORLD
>WE ENCRYPT EMAILS SO NO ONE ELSE CAN SEE THEM
>UNWELCOME EYES REMAIN UNWELCOMED

>VISIT MESSAGELABS.COM

MessageLabs | Now part of Symantec

Financial fraud affects consumer bank behavior, Gartner finds

By Marcia Savage, Features Editor, Information Security magazine

A new report released by Gartner Inc. Wednesday shows the impact of data breaches and financial fraud on consumers' behavior, including their banking activity.

About 7.5% of U.S. adults lost money due to some type of financial fraud, mostly due to data breaches, according to a survey of 5,000 Americans conducted by the research firm last September.

Of the respondents, 14% said they were victims of credit card fraud and 7% said a thief used their debit or ATM card to make purchases or withdraw cash. Six percent said they were victims of new account fraud, where a thief opened an account in their name, while 5 % said a criminal stole money out of their existing checking or savings account and 4 % said a thief forged checks on their account.

Compared to the average consumer, nearly twice as many people who lost money to fraud changed their shopping, payment and e-commerce behavior, according to Avivah Litan, vice president and distinguished analyst at Gartner.

"We all read about the data breaches. This survey certainly proves they're having an impact in terms of spooking customers," Litan said.

Victims of electronic checking and/or savings account transfer fraud were almost five times more likely to change banks due to security concerns, compared to the average consumer, according to the report.

"From a bank point of view, this is really causing customer churn," she said. "It's costing them customers."

Consumer security concerns have a big impact on online banking, she said, with 20% of survey respondents worried about security, saying they stopped or won't start transferring money between accounts. The percentage doubled among fraud victims.

While only 6% of the consumers surveyed said they changed banks due to security concerns, the number jumps to 28% among checking/savings account transfer fraud victims, according to the report.

Thirty-five percent of survey participants said security was an important factor in their decision to bank online or do more business with their bank online, but security isn't as important to consumers as bank fees and customer service, the Gartner survey showed. Security, however, becomes much more important for consumers who have been victims of a financial account takeover, according to the report.

Litan advised financial institutions that have implemented strong security to publicize that fact to their customers to gain their confidence. They should also engage customers to participate in security; an example would be to sign up for a service that alerts them to suspect transactions, she said.

"There's a lot of value in advertising your security," Litan said. Right now, banks aren't using security as a customer retention tool, she added.

One company that's benefitting from consumers who change their online payment behaviors due to security concerns, particularly those who are fraud victims, is PayPal Inc., she said. Survey participants said they switched to PayPal because of concerns about online payment safety while using other payment systems. PayPal has promoted its security, which has really helped the company, Litan said.

Sponsor Resources

RSA®
The Security Division of EMC

- 2009 Fraud Trends whitepaper
- 2009 Fraud Trends webcast
- Register to receive the RSA monthly online fraud report

Guidance® SOFTWARE
The World Leader in Digital Investigations™

- Corporate Website
- Cybersecurity
- Data Protection

MessageLabs® | Now part of Symantec

- Everything you need to know about email and web security
- Email Continuity: You don't know what you've got until it's gone
- Web use and Risk to Business