Elementary Steps To Protecting The Bank

by Steve Brown

There is nothing like a good mystery story to get your mind buzzing, as you ponder who did the dastardly deed. Whether you are a fan of Sherlock Holmes, Nero Wolfe, Mike Hammer, Sam Space, Philip Marlowe, Nancy Drew or The Hardy Boys, everyone enjoys a good whodunit now and again. Characters such as these will analyze crime scenes with a keen eye, apply logic to what they see and use progressive police methods to ultimately solve the mystery at hand. The same can be said when thinking about efforts focused on stopping fraud at banks.

Consider the results of a recent Association of Certified Fraud Examiners Report on occupational fraud and abuse. It found that the most effective anti-fraud control is "proactive data monitoring and analysis." Organizations that used such an approach reduced median fraud losses by about 60% and it shortened the median amount of time from when frauds begin until they were detected by 50% in the cases studied.

This is important because the typical organization loses about 5% of revenues each year to fraud, which is a whopping $3.7T worldwide. In addition, using sophisticated analytics and human review processes are very important, as the report also points out that the median amount of time from when frauds begin until they are detected is 18 months, with almost 9% of cases running 61 months or more, so early detection is critical.

When it comes to fraud detection, it is important for risk managers and companies to start at the top of the food chain. This is because the report found that while owners or executives only accounted for 19% of all cases, they caused a median loss of $500,000. This compares to managers who committed 36% of frauds (median loss of $130,000) and employees who committed 42% (but only caused a median loss of $75,000). Targeted reviews of activity are important, because as the report also points out, fraud examiners found about 22% of cases involved losses of $1mm or more.

Another key to stopping fraud is to take a closer look at specific departments. Here, fraud examiners found about 77% of the frauds in their study were committed by people working in one of seven departments. These were: accounting, operations, sales, executive or upper management, customer service, purchasing and finance.

Perhaps the worst thing the report points out is that many organizations never get their money back once it is stolen. In fact, the study found that 58% of victim organizations had not recovered any of their losses, while only 14% had been able to make a full recovery. Prevention is important because once it is gone it is very difficult to get back.

Tips are also important ways for organizations to find out about fraud. Here, the report points out the best sources are from employees (49%), customers (22%), anonymous (15%), vendors (10%), other (7%), shareholders or owners (4%) and even from competitors (2%). Having a hotline for tips can help and is a good idea for bankers to consider.

Finally, the report also looked at the median loss and median time until fraud is detected by method. What is interesting here is that once you get to 30 months or longer, the most common ways organizations find out about a fraudulent issue is to be notified by law enforcement, external audit or by accident.

As can be seen from the data here, systems that learn, scan and continuously look for anomalies are important to banks when trying to surface fraud and protect against it. Add to that the smarts of a good internal team of human Sherlock Holmes and you are well on your way to having a more secure bank. After all, it is Elementary my dear Watson.

BANK NEWS

Employee Reviews

Studies find only about 17% of employees say performance appraisals are meaningful.

Mobile Payments

An Experian survey finds 24% of IT security professionals believe the greatest security risk to their company's payments ecosystem is in mobile. Meanwhile, 54% said NFC technology increased the risk of a security breach at their company.

Crisis Simulation

Research by Deloitte of executives, managers, analysts and crisis professionals from companies worldwide finds people said their organization last conducted a crisis event simulation as follows: unaware of any simulation or testing (53%), I don't know what a simulation is (15%), table top exercise in the last 6 to 12 months (15%), detailed simulation in the last 6 months (10%), and detailed simulation during my tenure (8%).

Technology Discussion

A PwC survey of corporate directors finds the average percentage of total annual board or committee hours spent discussing oversight of IT risks and opportunities is 5% or less (39%), 6 to 10% (37%), and 11 to 20% (14%). Meanwhile, 2% did not talk about it at all and 4% did so for 21% or more of total hours.

Cyber Worry

A survey by Travelers finds American consumers say their biggest cyber concern is that their bank account gets hacked (62%); followed by malware infections of computers and phones (60%); online identity theft (59%); offline ID theft (59%); retailer hacks exposing their personal information (58%); and breaches of their medical records (43%).

Activist Timing

A PwC survey of corporate directors finds 84% of activists will exit their investments within 2Ys.