SPOTLIGHT

Sponsored by: PwC

This Spotlight explores how and when the concept of a combined cyber fraud/security operations center starts to make operational and financial sense for an organization.

Cyber and Fraud Fusion Comes of Age

April 2023

Written by: Craig Robinson, Research Vice President, Security Services

Introduction

Silos not only limit information sharing but also can produce negative outcomes. Some of the lessons learned from the terrorist actions of 9/11 revolved around the lack of data sharing between different law enforcement agencies. Relevant pieces of information were available prior to the events of that horrendous day, but they were cloistered in their respective organizational silos. Looking back at how things unfolded, the different agencies recognized that better information sharing between similarly focused teams could have been helpful. The lack of a holistic view of the available information could certainly be considered a contributing factor to the events of the day.

AT A GLANCE

KEY TAKEAWAYS

Fraud prevention teams and cybersecurity practitioners have a common goal of preventing damage or loss to an organization. The time has come for their siloed domains to be brought together in a cyber fraud fusion center to eliminate duplication of data while providing rich, contextual information to their respective teams to fulfill their departmental objectives.

The lessons of 9/11 can help and should inform how different teams tasked with protecting intellectual and financial assets can help shape their operations. In today's digital-first world, there is often a need to protect the assets of an organization as well as those of its customers. This requirement is typically concurrent with the need for cybersecurity teams to put a blanket of protection around the systems and data that they are charged with protecting.

Unfortunately, a virtual wall has existed for far too long between the teams designed to help reduce financial fraud and the cybersecurity teams focused on preventing or detecting malicious activity that could result in business disruption or loss of data. Some of these barriers are the result of prior technological shortcomings. An overabundance of data is available to decipher bad intent on the part of financial crime groups; however, it is typically siloed in the fraud and security operations teams, which can make correlating these disparate data sets difficult.

A Partial Solution Exists, But It Is Fragmented

The existence of the cloud certainly can help in providing the needed surge capacity to correlate the immense numbers of data points that humans and machine systems can create. Prior to the dawn of the cloud computing era, the ability of systems to ingest vast amounts of data was circumscribed. Today, the infrastructure and computing limitations of a purely on-premises infrastructure have been overcome due to the elastic demand capabilities of modern cloud computing environments.

The user behavior analytics (UBA) that are utilized to help detect patterns of normal behavior are of particular benefit. The machine learning algorithms that they employ are often able to have a digital feast with the avalanche of data that is possible to be ingested. Actual patterns of behavior can be tracked, and some anomalies can be flagged for additional controls. For example, a UBA system can help detect when financial transactions are attempted that fall outside of the normal behavioral patterns of a customer. Let's say that a customer normally stays in a static geographic area and then breaks that pattern by making a large purchase from a distant location.

A UBA system can be a key technology piece to filling in the jigsaw puzzle that can help reveal the picture of a fraud operation or provide additional context to a cybersecurity investigation. Yet, despite the availability of great tools such as UBA, or other technology such as the use of data analytics or fraud prevention software, financial losses continue to persist. The question is, Why?

A Holistic View Is Needed

The digital footprint detectable by the fraud operations team isn't likely to provide a holistic view if the only data sources utilized are those that live within the fraud team. For example, if the data from a physical badging system were combined with fraud data, additional insight could be created to help prevent insider fraud. The fact that an employee was swiped in at a physical work location might provide the missing link that would stop a fraudulent purchase two hours later at a location 2,000 miles away.

Here's another way to picture this scenario. Fraud operations teams are traditionally focused on watching the "front door" of a financial institution. Security operations teams are traditionally focused on the digital infrastructure. If a bad actor is probing a company's perimeter, and is simultaneously attempting fraudulent account actions, it would be ideal to correlate the two events with one another to help achieve a holistic view.

The traditional three-tier architecture of computing systems can serve as an appropriate way of understanding what changes are required to help fuse cybersecurity and fraud capabilities together.

Start with the data layer: The good news is that the data required to close the loop may not be that far away. It might just be in a different silo that is walled off from other functional uses. What is needed is a centralized data platform to help collect the data necessary to detect and prevent cyberattacks and/or fraud. Fortunately, the foundation for such an effort already exists in many security information and event management (SIEM) solutions and/or the data lakes that chief information security officers (CISOs) have at their disposal.

The second tier, the application layer, is arguably one of the hardest parts to engineer. The extra feeds that can be added to the data lakes that cybersecurity teams utilize can provide more context to help close the loop on fraud. However, it isn't typically easy to do. For example, if a bank tried to put all the varying data feeds together on its own, the engineering that goes into the machine learning algorithms and artificial intelligence needed to authorize transactions in microseconds can be quite a complex operation.

There is also a need to make sure that additional friction is not introduced during the process. The information security (InfoSec) teams will likely require that the data analytics and other engineering that occur in the application layer do not raise additional false positives. The fraud teams will often require that the tuning and normalization of data allow for speed without letting fraudulent transactions occur.

The presentation layer requires some work as well. The views certain personas get in either the InfoSec or fraud teams should be built with the appropriate data governance. The additional context the combined data lake holds can be very insightful when doing fraud investigations or piecing together forensic data as part of a cybersecurity threat hunt, but care should be taken to make sure that protected data is presented only in a "need to know" situation.

While not necessarily a part of the three-tier model, there are additional considerations to take into account. Now that the data is living in harmony together and creating meaningful insights across the financial enterprise, the question becomes: How do these teams work together? Operational and structural integration is often the place where fusion centers can fall short. A shared data set exists with each event that fires and the corresponding alert and case it creates. Those items go into a ticket that is tracked, investigated, and remediated by their respective teams.

Industry-leading practice dictates the integration of alert and case management systems to allow the teams to collaborate on investigations and ultimately achieve the goal of helping prevent fraud from occurring through real-time information sharing. Additionally, the ability to help reduce detection and investigation times by making cyber/fraud data available as opposed to just siloed data is now a reality. Precious time can be saved, and time typically equals money.

Definitions

Cyber fraud fusion centers are the integration of disparate functional teams. This can be achieved by thoughtfully combining technical and operational systems and procedures. The fusion layer is the middle layer between the security and fraud layers and helps address the gaps that exist because of the siloed legacy framework. The outcome facilitates more efficient and effective communication and collaboration between cybersecurity and fraud prevention teams as well as reduced financial losses.

What Are the Benefits of a Fusion Center?

The concept of a combined cyber fraud/security operations center makes operational and financial sense for several reasons:

- It can be mined for insights before a fraudulent transaction is finalized. Higher-fidelity alerts, events, and corresponding cases can be raised to allow for a more effective investigation of the questionable activity.
- The additional data sets from SIEM systems and/or data lakes can help provide extra fidelity and context around potential attacks. This fidelity is of particular concern given the prevalence of a hybrid/remote workforce. The expanded attack surfaces that come with hybrid work can require additional data to help identify and protect against cyberthreats and insider fraud.
- Financial losses among customers or financial institutions can be lowered by identifying actual fraud sooner. Funds that were previously held in loss reserves can be reduced.
- Friction can be reduced for legitimate customers that get caught up in fraud controls that are meant to protect them, but too often, due to legacy siloed data, can cause extra steps and delays for these customers.
- Demonstrable compliance can be shown to regulatory bodies and management teams that have an interest in seeing enhanced risk reduction as exhibited by the fusion center.
- Consider the performance gains that fraud detection teams can achieve by shrinking the time needed to determine whether a suspicious activity report (SAR) should be filed. The decision on whether or not a SAR needs to be filed can be subjective. The decision can require numerous data points that need to be correlated to make the filing decision. The additional context provided by the fusion center capabilities may help justify the appropriate decision as well as provide the insights when filing the SAR in an expedited time frame.
- Better metrics on common cybersecurity measurements such as mean time to detection (MTTD) can equate to higher cybersecurity maturity levels and lower cyberinsurance premiums.

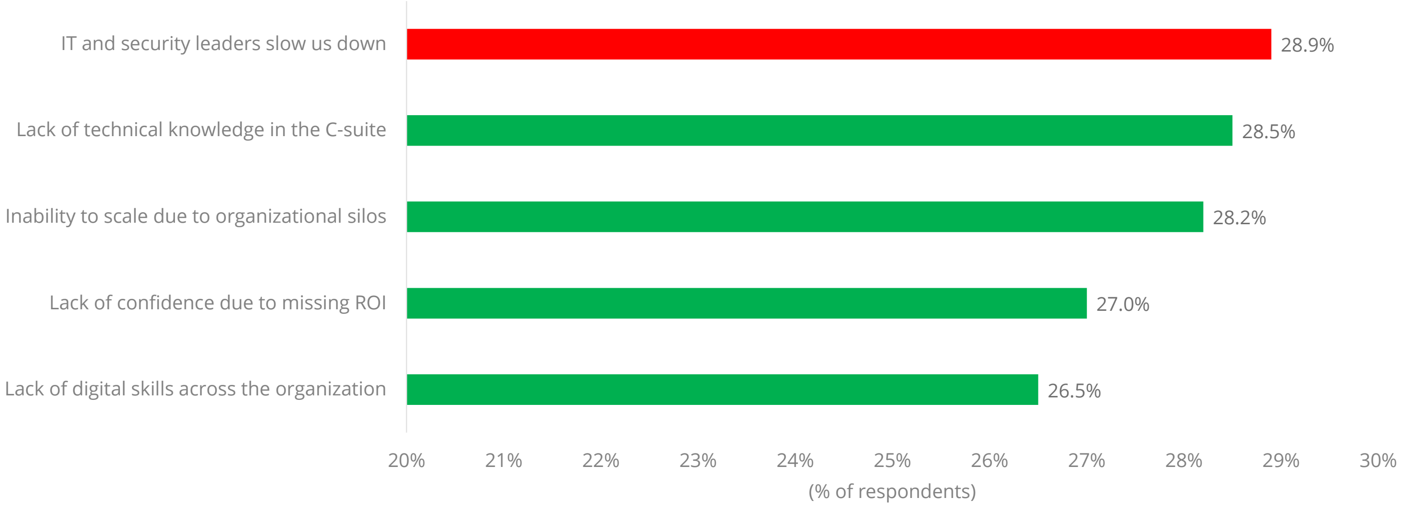
Recent Trends Around Removing Silos

Organizational silos have declined over the past decade. Today, the modern CIO has broken out of the technology silo to become a partner with the business and an enabler of digital transformation. At the same time, CISOs are stepping out of the shadow of the CIO. With that change comes the expectation that CISOs will likely be more responsive and proactive in putting together the systems a digital company needs as a result of COVID-19.

However, security and IT leaders are still perceived as being a hurdle when it comes to completing digital initiatives (see Figure 1). The inability of organizations to scale due to silos is also seen as an obstacle.

FIGURE 1: ***Worldwide Top 5 C-Suite Hurdles to Digital Initiatives***

Q *What are the most serious hurdles to completing digital initiatives in your organization?*



n = 858

Source: IDC's Worldwide C-Suite Survey, August 2022

While the trend of IT and security leaders moving closer to the business is a welcome sign of organizational cohesion, there is more work to be done to change how these teams are viewed by the business.

Considering PwC

Making use of its services and technologies focused on clients' first-line fraud controls, PwC has created a cyber fraud fusion center built on AWS that leverages its services for extensive compute, storage, and transformation capabilities. The platform leverages the Open Cybersecurity Schema Framework (OCSF) for log normalization and streamlined analysis provided by AWS Security Lake. Traditional AWS services used include CloudTrail, Security Hub, VPC Flow Logs, Route 53, S3, Glacier, Lake Formation, EMR Serverless, Glue, Athena, DynamoDB, SageMaker, and Lambda. The model system is also architected to be multitenant, and it can leverage multiregion zones afforded by the AWS footprint. The result can be ultra-low latency and high availability in real time.

PwC services in conjunction with its one-click deployment model are designed to help build a solution typically within one minute, according to the company. This model system also includes proprietary collectors to help ingest and securely transfer data from on-premises systems to the cloud for integration and action.

The result can be easier deployment and cost-effective fusion solutions for the financial services industry.

Challenges

There will likely be the challenge of overcoming the territorial nature displayed by many department leaders. Trust needs to be built between the cybersecurity and fraud teams before a fusion center can become a reality. PwC should recognize that while it may hold the blueprint for successfully building a fusion center, each new implementation will likely require a unity of purpose between teams that historically have existed in siloed environments.

Conclusion

The ingredients for building a fusion center exist. The elastic capabilities of the cloud can provide the technology and the speed. The existing data feeds that go into the separate fraud- and cybersecurity-focused data lakes are already identified.

The prospect of fusing cybersecurity and fraud information into a cohesive platform that results in reduced fraud- and cybersecurity-related losses is compelling. However, it will take working with a trusted collaborator to help bring this vision to fruition.

The prospect of fusing cybersecurity and fraud information into a cohesive platform that results in reduced fraud- and cybersecurity-related losses is compelling.

About the Analyst

Craig Robinson, *Research Vice President, Security Services*

Craig Robinson leads IDC's Security Services research practice. Topics of coverage include managed detection and response services, incident readiness and response services, cyber-resilience, and the intersection of the C-suite, the board, and cybersecurity.

MESSAGE FROM THE SPONSOR

More About PwC

PwC can help clients reduce risk initiatives by identifying and addressing security, privacy, and regulatory barriers. PwC's AWS cloud deployments are augmented by deep business and technical experience, proven methodologies, and a strategy through execution approach. To learn more, click here:

https://www.pwc.com/us/en/services/alliances/amazon-web-services/aws-cybersecurity.html

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.