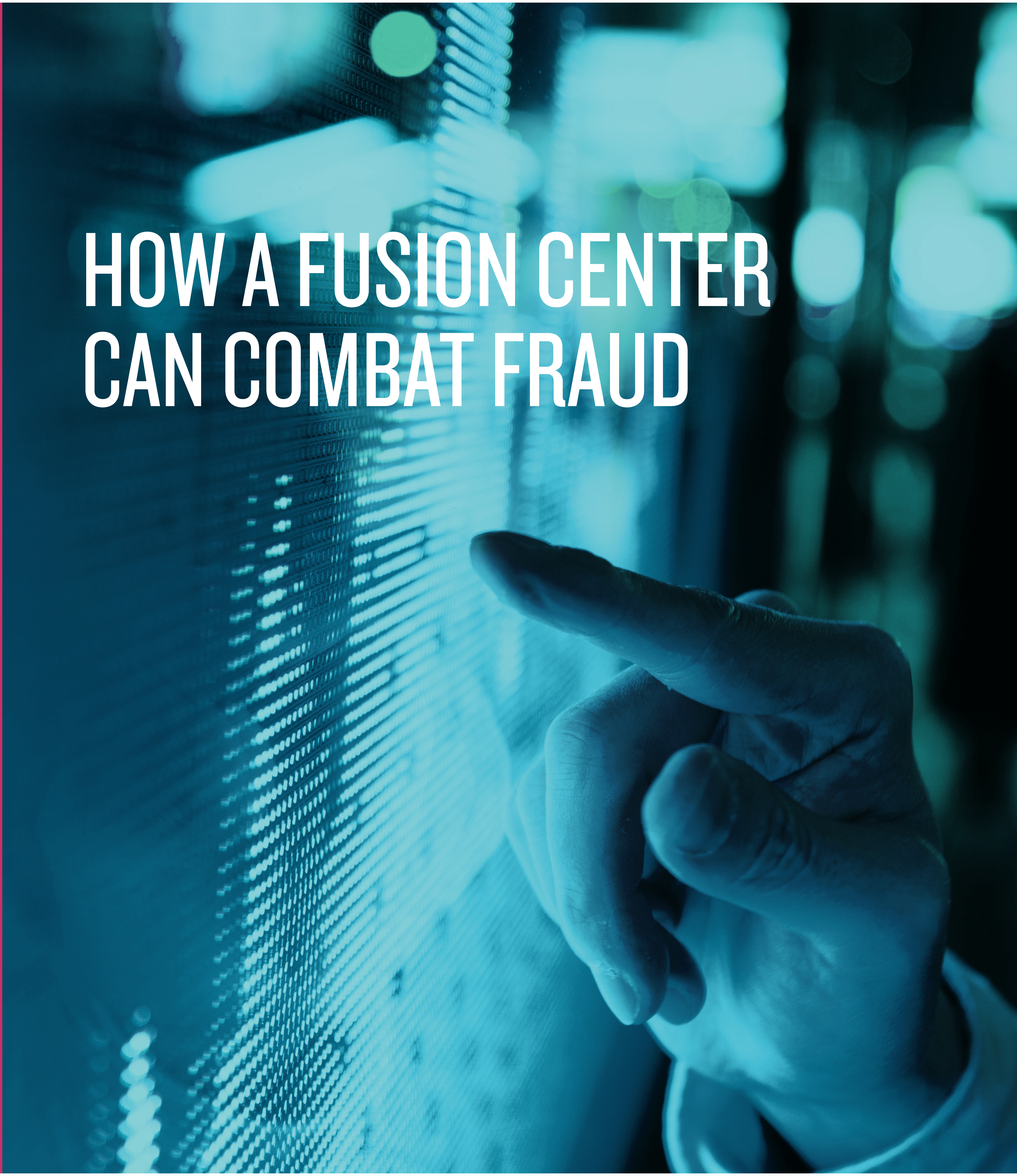
Booz | Allen | Hamilton



HOW A FUSION CENTER CAN COMBAT FRAUD

CONSULTING | ANALYTICS | DIGITAL SOLUTIONS | ENGINEERING | CYBER

SECURE PAYMENT
CLICK

FRAUD: A GROWING PROBLEM

It's no secret that fraud is one of the biggest threats to the financial services ecosystem. Account takeovers increased 45% in the second quarter of 2017, costing $3.3 billion in losses to financial institutions, and that's just one type of fraud in a three-month period[1]. Although companies are dedicating more resources to addressing fraud, losses continue to increase: a 2017 report shows that every $1 lost to fraud costs companies between $2.48 and $2.82[2].

Today's fraudsters are sophisticated and have the upper hand. They operate as organized businesses, complete with data-sharing and research and development efforts. As a result, these "bad actors" have access to vast stores of intelligence, which they exploit through cyber techniques. Social engineering and business email compromise, which continue to gain traction, allow fraudsters to obtain and use legitimate credentials to access accounts, making them nearly impossible to detect by traditional means.

CURRENT SOLUTIONS ARE INEFFECTIVE

Contemporary fraud prevention and detection methods are ill-equipped to handle the tactics, techniques, and procedures being used by today's threat actors. Specifically, fraud and cybersecurity teams at most organizations do not typically collaborate and their tools and protocol are not synced to enable proactive detection. They speak different languages, have different workflows, and generally stick to their own spaces. When cyber teams notice something suspicious, they don't always share their intelligence with the fraud team, and vice versa. Eric Reddel, a Principal at Booz Allen, shares his insight: "Because fraud now cuts across the responsibilities of cyber and fraud teams, lack of communication can lead to security teams addressing a single threat actor from two different approaches."

Another issue with traditional fraud solutions is that they are reactionary by nature. Action is taken ***after*** fraud occurs, leaving less time to track and escalate a fraud incident before losses are incurred. Many times, organizations have already suffered a loss and the only recourse is a post-mortem assessment. By the time new controls are implemented for that particular tactic, adversaries have moved on to a new technique.

Bridging cybersecurity and fraud prevention is critical to maintaining the integrity of your organization's overall security posture, as well as matching the dangers posed by the convergence of cyber and fraud from a threat actor perspective. This is where the Fraud Fusion Center can create an environment for cyber and fraud professionals to work together to create an effective detection, prevention, and response program.

THE FRAUD FUSION APPROACH

A Fraud Fusion Center is a next-generation security operations center that brings cyber threat intelligence (CTI) and cyber defenders together with fraud specialists to create a continuous loop of information exchange. This "fused" team hunts for threats across domains, shares data and surveillance technologies, and case management tools. It leverages advanced analytics, repeatable processes, and workflow automation/orchestration tools to accelerate manual actions.

Amy Boawn, a Senior Associate with Booz Allen and a leader of the firm's fraud practice, explains the benefits of a fraud fusion system. "It not only leverages traditional cyber fusion and fraud operations, but taps into threat intel, analytics, monitoring, and response," she says. "It also facilitates the sharing of monitoring operations." When an anomaly or fraudulent activity is detected, the time to respond can be aided with the fraud fusion concept. "If cyber teams see something, they can readily alert fraud analysts, and the fraud team can respond," Ms. Boawn adds. "This is much faster and more effective than waiting for coordinated responses from individual tools."

WHEN FRAUD ALERTS SHOULD TRIGGER

Your organization should be monitoring the behavioral patterns of your customers to proactively detect anomalies and trigger the proper alerts.

EXAMPLE BEHAVIORAL ANOMALIES TO TRACK:

- Unusual IP addresses
- Changing email addresses
- Unusual patterns of activity
  - Changing personal information
  - Moving funds
- Time of transactions

Consider an online banking customer based in New York, who typically logs in to her account between standard workday hours. One day, she logs in in the middle of the night, from a Singapore-based IP address, requesting a transfer of funds. This should immediately raise an alert.

[1] Ponemon Institute's 2017 Cost of Data Breach Study: Global Overview

[2] LexisNexis® Risk Solutions 2017 True Cost of Fraud^{SM} Study, October 2017

FRAUD FUSION CENTER COMPONENTS

THREAT INTELLIGENCE

- Cyber Threat Intelligence teams and fraud strategy teams must agree upon requirements
- Leverage feeds already in existence, either from a vendor or produced organically, to enhance fraud detection and parse for efficiency

ANALYTICS

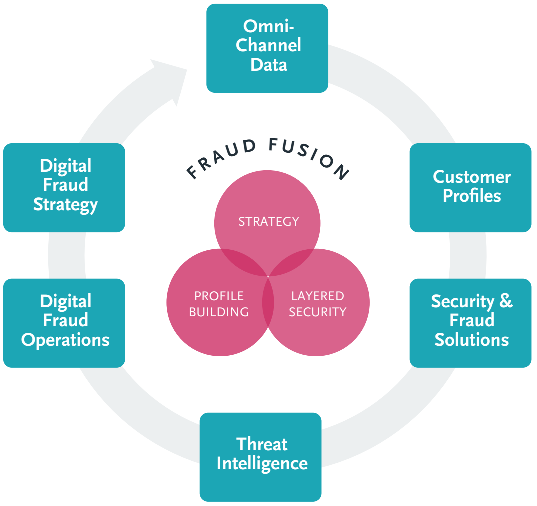
- Critical at every point in the client lifecycle
- The right data is key
- CTI, fraud and Omni-Channel teams must work together to fuse customer profile and behavior data
- Increase efficiency in operations, improve awareness, increase confidence in transations and reduce client friction

MONITORING

- Shared indicators of compromise between fraud and cyber will enhance triage and respose capabilities
- Teams will have the ability to see patterns of suspicious activity and possible fraudulent behavior across multiple channels and domains that would otherwise go undetected

RESPONSE

- Response teams have a multi-function purpose
- Fraud, security and legal teams may have a different focus, depending on the incident
- Streamlining the process allow for all teams to work together and possibly reduce response times, leading to faster containment and recovery



Enhanced leadership awareness.

Increased organizational awareness.

Faster detection and response times.

Improved client experience.

STEPS FOR SUCCESS

Building a Fraud Fusion Center requires a paradigm shift; cyber and fraud teams to speak the same language, understand (and agree upon) the different levels of compromise, and be willing to work together before they can effectively share data, people, and processes. While this transformation can take a year or even longer to achieve, there are some immediate steps organizations can take to enhance their fraud prevention programs: these can be divided into “quick wins” and “strategic actions.”

Quick Wins:

Find a champion.
Bringing fraud and cyber together requires serious change management that is best led by a senior leader or executive who can champion the program. This person must have the authority to mandate and create a Fraud Fusion Center. Without this level of sponsorship, organizations spend a lot of time and energy making very little progress.

Take stock of existing capabilities.
"Fraudsters know the weaker links in technology: organizations with softer controls are the targets because fraud rings are hitting everyone equally—every bank across the board," Ms. Boawn says. "Organizations must take inventory of what they have and benchmark their capabilities against their peers."

It is vital that organizations understand what technologies they have and who is benefitting from their outputs. Often, the fraud and cyber teams are using similar tools that would be more effective at combating fraud if both teams had access to the outputs. For example, both teams sharing the same SIEM tool and log data will improve their combined abilities to combat fraud verses having these tools separate.

Partner a fraud analyst with your CTI team (or vice versa).
By partnering together, fraud and CTI analysts can quickly coordinate efforts which brings greater insight into threat actor patterns, indicators of compromise and potential large-scale fraud campaigns.

Strategic Actions:

Define a strategy and communicate often.
When defining a strategy for a Fraud Fusion Center, begin by identifying the commonalities between the fraud and cyber teams. Build a strong foundation comprised of shared indicators of compromise that leverages response workflows, analytics, data sets, and coordinated responses for faster action. Meanwhile, leaders must communicate the strategy early and often.

Nail several use cases.
Identify a few Fusion Center use cases and pilot them successfully. You might, for example, decide to monitor ATOs in a specific channel during a defined timeframe using a specific method. Once you are able to demonstrate success and consequently gain traction and support, you can start expanding your efforts.

Fuse your data.
Fusing data too soon can create a lot of false positives and messy data lakes. It's easier to keep data separate until you understand what types of fraud you're seeing and the processes that work to address them; then, you can start fusing data a little at a time. Every organization is different, and teams should look to leverage feeds already in existence, either from a vendor or produced organically, to enhance fraud detection.

Layer technology solutions and establish a baseline.
Let the analytics platform run to establish a baseline, and then determine what success will look like for your Fraud Fusion Center. Determine what type of fraud you are detecting, what is the time to respond, and how many fraudulent attempts you are blocking. These metrics will help you demonstrate success.

Evaluate often.
Assess how the fraud and cyber teams are collaborating and where there is room for improvement. After an alert or event, make the appropriate changes to enable the Fraud Fusion Center to proactively detect that fraud in the future.

Keep it consistent.
You need repeatable processes for alerting and responding to fraud. Responding to fraud consistently and feeding information back into your data sets will reduce false positives and improve a center's ability to catch new fraud.

CONCLUSION

As fraudsters continue to adopt cyber techniques at an increasing and more complex rate, the need to adopt a holistic solution grows more urgent. A Fraud Fusion Center will help your company establish the process and tools to communicate across capabilities, transition reactive approaches to proactive ones, and help stop fraudulent activity from disrupting successful

To learn how Booz Allen Hamilton can help your business thrive, contact:

Scott Walters
Vice President
Walters_Scott@bah.com
+1-917-305-8011

Emily Helmke
Financial Services Director
Helmke_Emily@bah.com
+1-917-305-8134

Amy Boawn
Fraud Lead
Boawn_Amy@bah.com
+1-202-615-6093

Booz | Allen | Hamilton

DISCLAIMER: *We offer these recommendations for informational use only and do not make any warranties or other promises they will be effective against the threats described herein. If you would like assistance in addressing this type of threat, please feel free to contact us.*