Cybersecurity and Forensic Accounting Join Forces to Combat Criminals

JANUARY 2022

By Eric Hines & Nathan Fisher

Eric Hines
Partner, StoneTurn
ehines@stoneturn.com
+1 617 570 3755

Nathan Fisher
Managing Director, StoneTurn
nfisher@stoneturn.com
+1 415 848 7613

Not a day goes by without breaking news of a sophisticated white collar crime scheme perpetrated against a corporation, government entity or individual. In the era of digital transformation, big data and the ever-increasing adoption of technology solutions in business, it's no surprise that threat actors have taken to exploiting cybersecurity weaknesses to steal sensitive information, extort funds or otherwise create havoc in the corporate landscape. Such complex matters often demand equally complex solutions, which are perhaps best guided by multifaceted teams adept at bridging the gap between technology and finance functions within an organization.

Cybersecurity experts are an invaluable asset in preventing, detecting and responding to data breaches, cyber intrusions and other technology-related vulnerabilities. Similarly, forensic accountants are specially trained and adept at ferreting out business misconduct, unusual trends, financial anomalies, misappropriation of assets, and remediating related control weaknesses. Cybersecurity and forensic accounting experts working in close collaboration with each other can deliver a powerful one-two punch in the face of corporate crime. Here we discuss how the skill sets intertwine and how to use them collaboratively when cybersecurity issues come to light.

Cybersecurity risk centers around the protection and safeguarding of entity systems and the data sources they contain, which are collectively corporate

assets in their own right. Seasoned cybersecurity professionals can be instrumental in helping organizations assess data security risk and then designing and implementing processes, systems and controls based on industry standards (e.g.,NIST) to mitigate risk as much as possible. Investigating potential data security breaches, when they do happen, is a high-stakes endeavor and moves at lightning pace. Cyber-incident response teams must also be skilled investigators who can employ a variety of techniques that are both traditional and cutting edge, including interviewing technical witnesses, performing data analytics on relevant system data, and using technology tools to identify digital breadcrumbs. Part of the secret sauce of a skilled cybersecurity professional is practical experience, be it with commonly exploited weaknesses, tactics of threat actors or deep awareness of the traits that allow for attribution to likely attackers.

At their core, the competencies of cybersecurity professionals resemble those of forensic accountants. A skilled forensic accounting professional brings to bear deep understanding of business processes and internal controls, testing of internal controls, how entities store and use data in business processes, and experience with many forms of corporate fraud, including how corporate information can be misused from within or by third parties. Forensic accountants often employ investigative techniques that go beyond those of traditional audit steps, including collecting and searching electronic media, such as email, using analytics and visualization software to spot trends or outliers in large transactional data sets, conducting informational or confrontational witness interviews, and reviewing key business records to identify potential evidence of misconduct.

Cybersecurity and forensic accounting specialists share similar DNA, with the primary evolutionary difference being that the former focuses on safeguarding technology systems and data broadly, whereas the latter focuses on the safeguarding of financial information and assets. However, these two focus areas are often inextricably intertwined, creating a natural synergy for cybersecurity and forensic accounting professionals to serve as the right and left hands, respectively, on the same matter.

How the two can work together

Whether a matter is focused on pre-incident processes and controls, an active investigation or post-incident remediation of a cybersecurity issue, organizations can benefit from having multidisciplinary skills. Cyber-related work to identify the who, what, where and how of a breach is critical. Forensic accountants can supplement those findings by identifying how a cyber-incident may have impacted the business's controls, calculating potential losses, assessing disclosure or accounting requirements as a financial reporting matter, or assisting with collection of evidence for potential insurance claims.

The concept of cybersecurity and forensic accounting collaboration can perhaps best be articulated with some hypothetical, but real-world examples. Let's assume a publicly traded corporation has digital transformation on its list of key priorities. It begins that journey by implementing a new contract management system to digitize, store and manage vendor contracts and related attributes. That contract management system was set up to exchange information directly with the company's purchasing system to create efficiencies in ordering and paying for goods and services. Due to an unknown system weakness, a malicious threat actor successfully

hacks into the company's network through the new contract management system, thereby obtaining access to the data, which ultimately feeds into a separate purchasing system. The threat actor could then theoretically change vendor payment details to reroute payments to bank accounts controlled by the threat actor, resulting in misappropriation of vendor payments. Situations such as these often go undetected until a human being raises a red flag, such as a vendor complaining that it has not received payment for past due invoices.

While this is only one simplified example, it highlights how digital transformation exercises can lead to new system vulnerabilities that can be exploited by savvy fraudsters. A competent cybersecurity team working alongside forensic accountants would bring the ability to understand not only the systems and technological vulnerabilities in play, but also the people-driven business procedures, processes and internal controls that were not designed adequately to prevent or detect the misappropriation before losses were incurred. Working with this collective knowledge, the combined teams can more rapidly help the organization close technology and internal control gaps, implement new safeguards, and quantify the impact to the organization.

It goes without saying that no two cyber-intrusions are the same, but increasingly they are financially motivated. Criminals are continuously looking for new ways to abscond with funds through keystrokes, as opposed to hold-ups. In the fight against profit-seeking cyber attacks, cybersecurity and forensic accounting experts working side by side present a strong front line of defense.

About the Authors

Eric Hines, a Partner with StoneTurn, brings almost two decades of experience in forensic accounting, controls / compliance and dispute consulting engagements. He serves as a consultant to attorneys and corporations in matters involving complex financial and accounting issues.

Nathan Fisher, a Managing Director with StoneTurn, brings over a decade of experience investigating national security threats to the U.S. government. As a Special Agent with the Federal Bureau of Investigation (FBI), Nathan conducted a vast array of complex intelligence, counterintelligence, and cyber-focused investigations and operations.

This article originally appeared in
Accounting Today, January 2022