Intelligent Forensic Accounting

A Whitepaper

BGESH
Incorporated

CONTENTS

INTELLIGENT FORENSIC ACCOUNTING

INTRODUCTION

Fraud, Waste, and Abuse (FWA) in Government and Commercial systems have a common adversary in persons who intend to commit fraud for financial gain at the cost of billions of dollars annually to the taxpayer and general consumer. The scope and abilities of criminals and criminal enterprises has become more complex with the advent of crypto banking (bitcoin), virtualization that makes adversary attribution extremely difficult, and a growing network of individuals who may wittingly or unwittingly become parties to fraudulent scams.

As commercial banking dives deeper into the digital currency markets, they are inadvertently enabling criminals to tap into resources of anonymity and additional means to launder. As retailers opt for network-connected ATMs, eCommerce plugins, and seemingly secure Point-of-Sale terminals, criminals are finding new ground for exploiting commercial consumer accounts through new means of credit card skimming and laundering for personal or organizational enrichment.

The Magecart group has exploited eCommerce retailers through the Magento eCommerce platform by utilizing SQLInjections and Git Repositories to inject malicious code with the intent to scrape unhashed consumer debit and credit card details. The Carbanak Cyber Group exploited weaknesses within a bank to steal and launder over $1 billion through online banking, e-Payment systems, inflating account balances, and controlling ATMs. Roman Seleznev, referred to as "The Carder," stole over 1.7 million credit card numbers from U.S. businesses and sold them to dark web brokers at a cost of over $170 million to credit card companies.

In 2015, the National Background Investigation System (NBIS) was hacked in a pair of breaches by the group, Deep Panda, who were able to exfiltrate the security clearance and personal data of over 21 million federal employees, contractors, and dependents. The IRS has been a target of fraud and money laundering seemingly since its creation and has become the victim of exploitation through Knowledge-Based Authentication (KBA) hacking. The KBA hacks, in turn, enable criminals to gain access to tax filer information and submit returns on behalf of the taxpayer, but divert the returns to criminal accounts. Larger organizations such as the Department of Health & Human Services (DHHS), which administers Medicare, Medicaid, and HUD, and other social welfare programs are exploited daily by individual criminals, fraudulent businesses, hostile state actors, and even medical professionals who commit fraud. These government organizations are especially vulnerable to exploitation because the government process, government systems, and, budgets that account for over half of U.S. Federal Government spending make it an easy mark for exploitation.

There exists significant research and material regarding how the government can reconcile its Information Technology infrastructure to make it more secure, collaborative, productive, and counter-FWA. Unfortunately, the research and scholarly articles do not consider the complex, cumbersome, and segregated government procurement process. It is a highly political realm that requires deep consideration when setting out to solve the problems of government and commercial FWA. Politically, one has to consider that civilian oversight provided by career employees and congressional members weighs heavily on whether or not an application can be developed to replace a legacy system. In the case of the Defense Health Agency's (DHA) Armed Forces Health Longitudinal Technology Application (AHLTA) Electronic Medical Record (EMR) system, the application has undergone multiple significant iterative deployments and implementations within the Army, Navy, and Air Force and has been a mainstay application since 2003. Beginning about 2017, the application, which heavily shares attributes of an undistributed ledger based on Microsoft Access Databases, received approval for a successor called MHS Genesis.

At a cost of over $70 million, the application was to be fully implemented by 2019 to assist the Department of Defense reduce fraud, waste, and abuse within the military health system. Unfortunately, a complex system that must share data across all services and the Veterans Administration (VA), cannot be feasibly developed and implemented service-wide without sacrificing functionality and security. This has proven to be the case with many other Government and Commercial Off-the-Shelf (GOTS/COTS) Applications. There also exists the political reality that defense contractors are fully aware of the principle that "He who controls the data, controls the power – or the contract."

With evolving criminal enterprises, channels of exploitation, and the unreliability of procurement processes to secure government applications and networks, the focus of forensic accounting should, therefore, turn to enabling and enhancing defensive FWA operations using a robust and knowledgeable Forensic Accountant Network.

THE FUTURE OF FORENSIC ACCOUNTING

Data protection has increasingly become a matter of national security as the examples show that even our security clearance and tax records are vulnerable to exploitation. The data within those files are enough to fully exploit an individual by controlling their identity, thus their lives. The implications of this are significant as the gate keepers of the nation's combat forces, financial records, and state secrets become vulnerable to exploitation as a result. Amplify the government breaches by cases such as the Equifax breach, and an entire nation can be held hostage.

The U.S. Treasury Department's Financial Crimes Enforcement Network (FinCEN) is one organization that supports safeguarding the financial system from illicit use, combatting money laundering, and promoting national security through the strategic use of financial authorities and the collection, analysis, and dissemination of financial intelligence. FinCEN also works with other federal agencies to achieve this mission. However, FinCEN's mission and the Treasury Department's Strategic Plan have placed a focus on denying revenue sources to hostile state actors and terrorist organizations rather than the small cell or individual operating for personal financial enrichment. In many cases, the strength of the Federal Government must be put to the most appropriate use to defend our national security and interests, but the experience of Bgesh consultants is that even small cell operators can have a tremendous impact to national security. If the events of the 2008 Financial Crisis are any indication, cases such as Bernard Madoff's fraudulent investment schemes have created enough of an impact to bankrupt financial institutions and destroy the lives of thousands of unsuspecting clients – that was just one man.

Bgesh would put forth the idea of a national directive to create a Forensic Accounting Agency that is robust, well-funded, coordinates with Federal and State Financial investigatory agencies, and is supported by the National Security Agency (NSA) and the Central Intelligence Agency (CIA). Ideally, the agency's operational aspects would consist of teams known as Forensic Accounting Response Teams that are comprised of the following:

- Forensic Accountant
- Legal Attaché
- Operations Team Lead
- Cyber Security Engineer
- Cyber Security Analyst

These teams would ideally be focused on utilizing the systems currently in place, have a robust knowledge of emerging trends in fraudulent activities, remain up-to-date on trending vulnerabilities in systems (e.g. XSS, SQL Injection, etc.), and serve to function similar to Offensive and Defensive Cyber Operations Teams with the intent to immediately disrupt illicit activities as they emerge rather than focus on reimbursement and prosecution after the fact. Prevention can be real-time.

Where FinCEN is focused primarily on "big game" and issues of national and international presence, this new component would work with federal, state, and local governments, as well as representatives of the commercial sector that can be considered parties to critical infrastructure or hosts of Personally Identifiable Information (PII) (e.g. manufacturing, banking, insurance, utilities, etc.).

This division would be a very large component of the federal government that is funded and operated similar in principle to the Michigan Cyber Civilian Corps (MiC3) that offers a mutually beneficial relationship between the state government and business organizations for the purpose of rapid response to critical cyber incidents. As financial crimes are more often being conducted through cyberspace, the functions of Forensic Accounting and the denial of hostile actors should be conducted with the same level of vigor and immediate response.

AN ELASTIC INFORMATION FRAMEWORK

The Forensic Accounting Response Team would function as a preventative and responsive entity that utilizes the data sources available to create an analytics framework that would be designed to assist them in detecting FWA. In Security Information and Event Management (SIEM), many organizations employ the use of the Elastic Stack analytics framework.

The Elastic Stack is a complete end-to-end log analysis solution which helps in deep searching, analyzing, and visualizing the log generated from difference machines or data sources. It accomplishes this by using multiple applications that function together within the Stack to Collect & Transform, Search & Analyze, then Visualize & Manage the data.

Essentially what this would enable the Forensic Accounting Response Teams to do is to create connections to multiple data sources (e.g. Medicare, State Farm, UnitedHealth, and J.P. Morgan Chase) and create signatures, rules, and functions related to Artificial Intelligence and Machine Learning that are hybridizations of Cyber Security SIEM and Forensic Accounting techniques. As agencies tend to rely on a narrow set of rules and basic analysis to detect fraud, the Elastic framework would be enabled to learn from the operators, history, and anomalies detected to enhance the effectiveness of the system. As criminals evolve their complex schemes or repurpose old schemes, it is imperative the government resolve to integrate the segregated systems preventing a holistic view of FWA activities impacting U.S. business and government operations.

Many would argue that a general Enterprise Approach to detecting and resolving fraudulent activities is the most effective means of achieving this goal. Most Enterprise Approaches involving reconfiguring individual government programs to fit the mold of a standard fraud prevention system are effective. However, the reality is the feasibility of rewriting programs and operating procedures for government functions that vary greatly between the various levels of government (e.g. Federal, State, and Local), and even the individual service components (e.g. HHS, DoD, FinCEN, etc.) currently in use is not as practical as providing a detachment branch agency with connections to the various systems, databases, and programs. This plugin approach may be best suited to answer the question of how government resources can best be utilized to prevent FWA and respond to incidents of FWA.

The implementation of the Elastic Stack as an analytics framework would be useful in providing such a connection to a detached agency and develop new systems and processes to respond and counter criminal acts. The detached agency would then coordinate with agency investigation units (e.g. Office of the Inspector General, FinCEN, Secret Service, etc.) to provide notification, data, and evidence of malfeasance. The agency would also work with operators within the government agencies as liaisons to close connections and remediate vulnerabilities in terms of channels of financial exploitation and cybersecurity vulnerabilities. In basic terms, it would be the marrying of FinCEN to Computer Emergency Response Teams (CERT).

The difference is the components of financial investigators, or Forensic Accountants, would be teamed permanently with penetration testers and government-approved white hats to serve the mission.

BARRIERS TO ADOPTING THE FORENSIC ACCOUNTING RESPONSE TEAM APPROACH

The difficulties in obtaining cooperation between government agencies at any level can be daunting. However, as an agency dedicated as a resource specifically to target all cases of FWA at all levels of government and even supporting commercial enterprises, the pressures of organizational cultural differences are side-stepped through implementing the detached agency approach. It takes the pressure off the individual government program agency to focus just on fraud prevention and affords them the ability to provide services as is their primary function and mission. Allocating a resource of support rather than of oversight can be a valuable commodity to agencies that are limited by budgets, regulations, operational constraints, and performance indicators.

The most obvious barrier to creating this detached agency of Forensic Accountants and White Hat Hackers is the provision of legislature and funding for such an endeavor. As a matter of national security, however, this component of intelligence and action could become a division within the National Security Agency (NSA) with a joint relationship with the Central Intelligence Agency (CIA).

The scope of funding, operations, and procurement processes to establish such a program would be determined by the latitude afforded the various intelligence agencies in establishing these functions and programs.

CONCLUSION

The prospect of Forensic Accountants taking a more active role in national security matters as they pertain to identifying, tracking, and eliminating cases of Fraud, Waste, and Abuse in government and commercial sectors is a promising endeavor that can enhance the security of the nation and its financial vulnerabilities. By adjoining Forensic Accountants with Cyber Security Engineers and Analysts in Offensive and Defensive Teams, the American taxpayer, the consumer, and the federal government could enjoy a significantly reduced risk of targeting by criminals seeking financial enrichment and leading the way for criminal enterprises to be denied access to services and revenue. Establishing a framework based upon the Elastic Stack that utilizes Artificial Intelligence and Machine Learning to enhance attribution and provide an early warning system for detecting cases of FWA can enhance the job of the Forensic Accountant and prosecutors. Government Agencies and Commercial Enterprises would enjoy a level of supportive security that enables them to focus on the fundamentals of their business operations while maintaining the standards of cybersecurity. Bridging the gap between cyberspace and finances is a necessary evolution towards enhancing our nation's security through the prevention of financial crimes.

ABOUT BGESH, INCORPORATED

Our team is dedicated to reducing risk for our clients and to deliver exceptional service with integrity, diligence, and fruitful communication. We consider excellent service to be of utmost importance. Not only will clients be pleased with our work product, but we also live by the golden rule of "treat others as you wish to be treated." We can assure our clients that we will be promptly responsive, that every interaction will be pleasant, and that our team will be dedicated to meeting the clients' needs, while offering the quality solutions to the problems presented.

Find out more at www.bgesh.com or by calling us at 888-313-8116.

Bgesh, Incorporated is an SBA 8(a) Certified, Native American Woman-owned Business.