The Impending Fusion of Computer and Behavioral Forensics

Apply the principles of psychology to your investigative approach

By Vic Hartman, JD, CPA, CFF, CFE, and Dr. Sri Ramamoorti, ACA, CPA/CITP/CFF/CGMA, CIA, CFE, CFSA, CGAP, CGFM, CRMA, CRP, MAFF

The rise in ransomware incidents at hospitals is a disturbing confluence of dark human behavior and the unavoidable dependence on technology. Nevertheless, the nightmare of ransomware[1] is only the tip of the iceberg. In healthcare, we are frequently talking about life and death situations and a massively regulated industry, so the vulnerability of patients/victims is only too obvious to those who would perpetrate fraud in healthcare.

The National Healthcare Anti-Fraud Association lists the most common types of fraud committed by dishonest providers as follows:

1. *Services not rendered* – Billing for services that were never rendered, either by using genuine patient information, or information obtained through identity theft, to fabricate claims with charges for procedures or services that did not take place.

2. *Upcoding* – Billing for more expensive services or procedures than were actually provided or performed.

3. *Unnecessary services* – Performing medically unnecessary services for the purpose of generating insurance payments—often seen in nerve-conduction and other diagnostic-testing schemes.

4. *Misrepresenting services* – Billing non-covered treatments as medically necessary, covered treatments for purposes of obtaining insurance payments—widely seen in cosmetic-surgery schemes, in which non-covered cosmetic procedures such as rhinoplasties are billed to patients' insurers as deviated-septum repairs.

5. *False diagnoses* – Falsifying a patient's diagnosis to justify tests, surgeries or other procedures that aren't medically necessary.

6. *Unbundling* – Billing each step of a procedure as if it were a separate procedure.

7. *Overcharging copays* – Billing a patient more than the co-pay amount for services that were prepaid or paid in full by the benefit plan under the terms of a managed care contract.

8. *Kickbacks* – Accepting kickbacks for patient referrals.

9. *Undercharging copays, overcharging insurance* – Waiving patient copays or deductibles for medical or dental care and over-billing the insurance carrier or benefit plan (insurers often set the policy with regard to the waiver of copays through its provider contracting process, while under Medicare, copays may only be waived due to financial hardship).

Almost every one of the above scenarios can be enabled by the use of technology. Indeed, technology can be a most dangerous tool in the hands of white collar criminals.

Increasingly, hospitals and clinics pushing the boundaries of automation and patient medical records, medical

[1] Hartman, V.E. & Ramamoorti, S. (2017). Ransomware: A Primer. What it is, how it happens, and what do about it. *New Perspectives in Healthcare Risk Management, Control, and Governance 36*(1), 7–11.

procedures—and most importantly, patient billings—are being created and maintained in digital form. As technology-fueled global communication advances, and technology-driven healthcare fraud becomes a reality, computer forensics will become indispensable. Already, forensic investigations of white collar crime in the 21st century, especially in financial services, find computer forensics critically important.

We must understand that computers and technology by themselves are mere instruments. They require human beings to use them as powerful weapons and tools to aid in the perpetration of fraud. Of course, the better the technology capabilities of a fraudster, the better they can use it for committing fraud and also concealing the audit trail. Auditors and fraud examiners need to pay keen attention to the manner in which technology-driven healthcare fraud is proliferating as well as evolving.

Technology may be the toolkit, but motivated people can use these tools for crime as well as productivity.

It was not until the publication of the book *A.B.C.'s of Behavioral Forensics* that the behavioral sciences, especially psychology and psychiatry, were seriously explored to understand why people commit fraud. Dorrell and Gadawski define forensic accounting as "the art and science of investigating people and money."[2]

What is forensics?

Computer forensics utilizes advanced technology capabilities such as key word searches, computer and data imaging, electronic evidence, link and network analysis, data mining and predictive analytics, etc., to identify incidents of fraud.

Behavioral forensics parallels computer forensics by leveraging insights from the behavioral sciences to understand the fraudster's motivations. It also looks at the psychology of the victims, as well as the fraud investigators themselves.

To the extent that fraud involves intent to deceive, the ecology of fraud necessarily is infused with behavioral implications throughout. However, to truly understand these behavioral elements, an important aspect of the contemporary investigative approach also involves electronic evidence gathering, because most complex white collar crimes involve technology. After all, cybercriminals are human beings first, so the general principles of psychology apply to them.

As surely as the future will bring new forms of technology, it will bring new forms of crime.

–Cynthia Manson & Charles Ardai (eds.) (1992), Future Crime: An Anthology of the Shape of Crime to Come. New York: Donald I. Fine, p. ix.

We predict that in the next few years, fusing the behavioral forensics and computer forensics approaches to address healthcare fraud will become inevitable. The blending will consider how they feed into each other and how they can inform each other, and will demonstrate an understanding of the synergistic power of an integrated perspective.

People and internal controls

Computers and software are, in themselves, tools of massive utility for communication and productivity. But technology can be a great enabler to perpetrate fraud. Internal controls are typically viewed as systems and processes devoid of the human element. We need to put the people back into internal controls so there can be superior assessments of behavior/integrity risks, conflicts of interest, ethical lapses, etc.

Technology is unlikely to catch fraud predicated on these types of "integrity failures." There needs to be a deeper understanding of soft measures and associated soft controls.

It is important for the computer forensic examiner to be knowledgeable about not only the technical operations of a computer, but also human behavior.

Today's personal devices, such as smartphones, play a significant role in connecting people's digital lives. The exponential growth of mobile devices that put incredible power at one's fingertips makes these devices extremely connected to the human using them. People manage their entire lives based on what is on their mobile devices. The amount of personal information stored on these devices is massive and unfathomable.

[2] Dorrell, D. D. & Gadawski, G. A. (2012). *Financial Forensics: Body of Knowledge*. Hoboken, NJ: Wiley.

Traditionally, computer experts and technology specialists have had a tendency to treat behavioral approaches as unnecessary, and to their detriment, have thereby ignored available insights.

Conclusion

We pay a heavy price for not bringing insights from the behavioral sciences to understand and respond effectively to the fraud problem when cybercriminals are motivated to use technology in the planning, execution and concealment of white collar crime. Technology may be the toolkit, but motivated people can use these tools for crime as well as productivity.

We wish to thank David Sems for his thoughts and ideas that have benefitted this column. **NP**

Victor Hartman, JD, CPA, CFF, CFE, is is Principal of The Hartman Firm, LLC, specializing in forensic accounting and internal investigations. He was an FBI Special Agent serving as a Street Agent, Supervisory Special Agent and Chief Division Counsel. Victor is an Adjunct Professor at Georgia State University and serves on Georgia Southern University's Forensic Accounting Advisory Board. You can reach Victor at (404) 369-0616 and Vic@HartmanFirm.com.

Sridhar Ramamoorti ACA, CPA/CITP/CFF/CGMA, CIA, CFE, CFSA, CGAP, CGFM, CRMA, CRP, MAFF, is an Associate Professor in the Department of Accounting of the University of Dayton. Dr. Ramamoorti has a unique blended academic-practitioner background with over 30 years of experience in academia, auditing and consulting. He is co-author of over 40 articles in respected journals, and 15 books and monographs. You can reach Sridhar at (630) 347-9172 and Sri.Ramamoorti@gmail.com.

AHIA NEWS

The CPA Journal, published by the New York State Society of CPAs, has announced Sridhar Ramamoorti, and Barry J. Epstein, PhD, CPA, CFF, a principal with Epstein + Nach LLC, as winners of its Max Block Distinguished Article Awards. They were recognized in one of three categories for the most outstanding and thought-provoking articles published in 2016. Their achievement was for *Outstanding Article in the Area of News & Views/Opinion,* titled: When Reckless Executives Become Dangerous Fraudsters: Reward Structures and Auditing Procedures Need to Be Reformed to Deter `Dark Triad' Personalities, published in the November 2016 issue.