Inside the Insider

—G. Lawrence Sanders
Professor, Department of Management Science and Systems, University at Buffalo, The State University of New York, Buffalo, NY 14260 USA

—Shambhu Upadhyaya
Professor, Department of Computer Science and Engineering, Associate Dean of Research and Graduate Education, School of Engineering and Applied Sciences Director, Center of Excellence in Information Systems Assurance Research and Education, University at Buffalo, The State University of New York, Buffalo, NY 14260 USA

—Xunyi Wang
Ph.D. Student,
Department of Management Science and Systems, University at Buffalo, The State University of New York, Buffalo, NY 14260 USA

(Corresponding author: G. Lawrence Sanders.)

IEEE DOI 10.1109/EMR.2019.2917656

***Abstract*—*We present an overview of two major research projects on the role of monetary incentives and psychological traits in attracting individuals to hacking behavior. In the first study, scenarios were developed for five situations to determine if monetary incentives could be used to influence subjects to obtain healthcare information and to release that information. Approximately 35% to 46% of the 523 survey participants indicated that there is a price, ranging from $1,000 to over $10 million, acceptable for violating HIPAA laws. In the second study, 439 subjects completed a survey that identified the psychological traits that contribute to an individual's propensity to participate in White Hat, Grey Hat, or Black Hat hacking. Preliminary results suggest that individuals that are White Hat, Grey Hat and Black Hat hackers score high on the Machiavellian and Psychopathy scales. We also found evidence that Gray Hatters oppose authority, Black Hatters score high on the thrill-seeking dimension, and White Hatters, the good guys, tend to be Narcissists. Our focus on both studies is malicious insider attacks because insiders have the ability to do substantial monetary and reputational damage to the organization. Several suggestions have been made on addressing insider threats.*

I. Introduction

IT is estimated that 2.5 quintillion bytes of data are generated each day.[1] There is a constant chronicling of peoples' actions, desires, interests, and even intentions. The dark side of this batholith of organization and personal information is that it can and will be compromised by the shadowy world of hackers, but also by trusted insiders. Insiders can pose a considerable threat to organizations as they can bypass many of the security measures using their knowledge and access to the systems.[2] The Privacy Rights Clearinghouse keeps a running tab on the number of data breaches. It is now approaching 11.6 billion records.[3] The eighteenth largest breaches in 2018 involved more than 10.3 million individuals.[4] That was a banner year for healthcare data breaches where 2,545 breaches were reported, and they affected over 194 million records.

In some instances, breaches occur because of negligence. For example, some people do not know that they are not supposed to maintain social security numbers in a temporary file or they email a medical diagnosis to another doctor without obtaining permission. The motives behind malicious attacks are diverse, including seeking revenge and retribution, thrills, anarchy, and curiosity. Financial motives, however, are the undercurrent of many attacks (see Figure 1).

Organizations use customer buying patterns to target and fine-tune their product offerings. Pharmaceuticals and health-care companies use personal data to identify potential customers for their products and

[1] https://www.forbes.com/sites/bernard-marr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/#5a4aaa5260ba Last accessed April 30, 2019

[2] https://www.sei.cmu.edu/research-capabilities/all-work/display.cfm?customel_datapageid_4050=21232 Last accessed April 30, 2019

[3] https://www.privacyrights.org/data-breaches Last accessed April 30, 2019

[4] https://www.hipaajournal.com/largest-healthcare-data-breaches-of-2018/ Last accessed April 30, 2019

services. Social networks sell their treasure trove of information on interests and beliefs to companies and organizations. They use the data to profile and target individual consumers and groups, and occasionally to manipulate political activity.

Privacy is about the control of sharing [1]. Privacy has been discussed in the legal literature in terms of the autonomy and control of the intimacies of personal identity [2].

Even though there is not a constitutional amendment for the right to privacy, it has been indirectly supported by several amendments. This is nevertheless a controversial subject [3, 4]. The fact is that individuals, organizations and government agencies want to control those who have access to data, information and transactions about them (see Table 1). However, all privacy stakeholders want access to everyone else's information, but not their own.

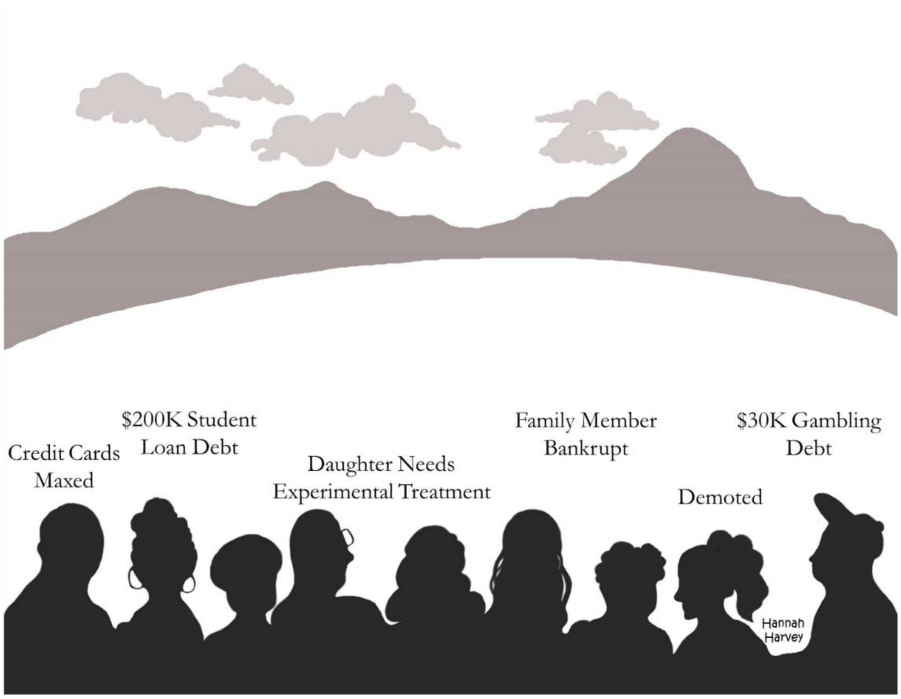

Figure 1. What prompts insiders attacks.

Table 1. The Gold Standard for Protecting Privacy is Complete Control.

- **Financial privacy**: Our resources are transferable, viewable, and available only to those individuals and organizations that we choose.
- **Mental privacy:** Our personality profile and thoughts are transferable, viewable, and available only to those individuals and organizations that we choose.
- **Biologic privacy:** Our biological and organic metrics are transferable, viewable, and available only to those individuals and organizations that we choose.
- **Location privacy:** Our past, present, and future locations are transferable, viewable, and available only to those individuals and organizations that we choose.
- **Social privacy:** Our past, present and future social networks connections and interactions are transferable, viewable, and available only to those individuals and organizations that we choose.
- **Intellectual Data Privacy:** Our inventions, literary work, designs, symbols, and business processes are transferable, viewable, and available only to those individuals and organizations that we choose.
- **Organizational Data privacy:** Organizational data, including intellectual property from all of the above, are storable, transferable, viewable, and available only to those individuals and organizations that we choose.

II. Background: Insider Attacks

Our current research focus is on insider attacks because they account for a substantial portion of privacy violations including funds embezzlement, pilfering of trade secrets, theft of customer information and competitive information, and a variety of illegal, fraudulent activities [5] and they can also result in significant losses [2]. Malicious insiders have the ability to do more damage to the organization than the traditional hackers [17].

The average cost of an insider attack is $8 million per year.[5] But the fallout from a breach can lead to long-term loss of customers, lawsuits and damaged reputations. In certain situations, insider attacks have the potential to be truly catastrophic. For example, in the case of nuclear plant breaches, the attacker intends to cause a nuclear incident. This is such an alarming issue that researchers are investigating the use of wearable Electroencephalogram (EEG) monitoring devices to identify high-risk insiders inside nuclear plants [6].

Insiders can be current and former employees, contractors and business partners that have access to an organization's network, system, or data. Insiders can engage in malicious or unintentional activity that negatively affects the confidentiality, integrity, and availability of an organizations information system [7].

The following sections discuss two major studies we are conducting on the propensity of individuals to engage in violating privacy laws and engaging in both legal and illegal hacking behavior. Our research shows that employees that are about to enter the workforce, even in the

[5] https://www.darkreading.com/the-6-worst-insider-attacks-of-2018—so-far/d/d-id/1332183 Last accessed April 30, 2019

face of strong laws, can be incentivized in certain situations to engage in illegal behavior. This effect can be amplified when individuals have psychological traits that are conducive to engaging in legal and illegal hacking activity.

III. Study 1: Where's the Money?

The objective of the first study was to identify the role that monetary incentives play in violating HIPAA regulations and privacy laws in the next generation of employees [8]. The research model was developed using the economics of crime and rational choice theory frameworks to identify situations where employees might engage in illegal breach behavior.

A pilot study was first conducted using sixty-four medical residents and thirty-two executive MBA candidates to test the constructs. The main survey data involved 523 students with an average age of 21 that are on the cusp of entering the workforce.

Scenarios were developed for five situations to determine if monetary incentives could be used to influence subjects to obtain health care information and to release that information. As an example, one situation assumes that the subjects were nurse's aides earning $30,000 per year, and a friend asked them to get information on a patient. The subjects were asked the amount of money they would require. They were also asked about their perceived probability of getting caught for violating HIPAA laws. Many of the subjects believed there was a high probability of being caught. More than 50% of them indicated that the probability of getting caught was more than 75%. Nevertheless, many of them could still be incentivized to violate HIPAA laws.

Approximately 46% of the survey participants indicated that there is a price, ranging from $1,000 to over $10 million, acceptable for violating HIPAA laws. A key finding that also has previous empirical support is that individuals perceiving a high probability of being caught are less likely to release private information.

However, the bad news is that there is a small chance of being caught and there is an even smaller chance of being convicted. One security expert estimates that only 1 in 10,000 people that commit internet crimes are caught and that only 1 in 100 people are prosecuted and received fines or jail time [9]. We also did a search at The United States Department of Justice (DOJ) (https://search.justice.gov/) using *HIPAA* as a keyword and put together a summary of the cases that DOJ has obtained fines and jail time. There were only 11 cases. Many of the subjects in our study thought that there is a high probability of being caught for violating HIPAA laws. For example, in the nurse scenario noted earlier, 30% of the subjects indicated that there was at least a 93% chance of being caught. However, the true probability of getting caught and punished is very, very low.

IV. Study 2: What Are You Thinking?

This purpose of the second study was to understand the psychological profile of individuals that will soon enter the workforce and their propensity to engage in both legal and illegal hacking behavior [10]. This survey was distributed to 439 sophomores and juniors. The goal of the study was to identify the psychological profile of an individual's propensity to participate in White Hat, Grey Hat or Black Hat hacking.

White Hat hackers, sometimes referred to ethical hackers, assist system owners in detecting and fixing security systems vulnerabilities. Gray Hats can have ideological motivations that translate to hacking attacks against an adversarial political position, a company policy that they do not agree with or even a nation-state. They are often referred to as hacktivists. Black Hat hackers, sometimes called crackers, are typically motivated by the personal gain to illegally breach computer systems, though they might also be mischief-makers that are in it for the thrill of the attack, for revenge or to seek notoriety.

Among other psychological personality variables, the Dark Triad personality variables are our main focus in this study. The Dark Triad refers to a group of three generally, socially undesirable personality traits, including Machiavellianism (manipulative, deceitful and exploitive) Narcissism (self-centered and attention seeking) and Psychopathy (lack of remorse, cynical and insensitive) [11–13].

Depending on the question, 14% to 25% of the subjects would participate in ethical White Hat hacking, 10% to 29% would participate in illegal Black Hat hacking, and 10% to 27% would engage in Gray Hat or so-called hacktivist hacking.

Preliminary results suggest that individuals that have the potential to be White Hat, Grey Hat and Black Hat hackers score high on the Machiavellian and Psychopathy scales. That is, they have personality traits that are manipulative, deceitful, exploitive, lacking remorse, cynical and insensitive. The implication is that even though White Hats may be Machiavellian and Psychopathic, we need them to address nefarious hacking activity. Moreover, we found evidence that Gray Hatters oppose authority, Black Hatters score high on the thrill-seeking dimension and White Hatters, the good guys, tend to be Narcissists. Interestingly enough, the relationship between Narcissism and the Gray Hatters and Black Hatters was not significant.

The major takeaway from the two studies is that many people have a price. It may be a significant amount of money, or it may be a situation where a family member or a friend needs critical medical assistance. Spurred on by their psychological traits, some individuals may succumb to monetary incentives.

V. Implications: Protecting the Organization

There are many organizations that provide information on how to develop security procedures to counter insider threats, such as Office of the Director of National Intelligence,[6] National Insider Threat Task Force,[7] and the Software Engineering Institute of Carnegie Mellon University [7]. The Software Engineering Institute of Carnegie Mellon University produces very detailed procedures, and they are presented in Table 2 [7]. One area that they do not cover in depth, related to our empirical findings, is the behavioral motivations and the psychological profiles of potential hackers.

Table 2. Best Practices for Countering Insider Threats From Carnegie Software Engineering Institute.

Practices
Know and protect your critical assets.
Develop a formalized insider threat program.
Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior.
Anticipate and manage negative issues in the work environment.
Consider threats from insiders and business partners in enterprise-wide risk assessments.
Be especially vigilant regarding social media.
Structure management and tasks to minimize insider stress and mistakes.
Incorporate malicious and unintentional insider threat awareness into periodic security training for all employees
Implement strict password and account management policies and practices.
Institute stringent access controls and monitoring policies for privileged users.
Deploy solutions for monitoring employee actions and correlating information from multiple data sources.
Monitor and control remote access from all endpoints, including mobile devices.
Establish a baseline of normal behavior for both networks and employees.
Enforce separation of duties and least privilege.
Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities.
Institutionalize system change controls.
Implement secure backup and recovery processes.
Close the doors to unauthorized data exfiltration (copying of data).
Develop a comprehensive employee termination procedure
Adopt positive incentives to align the workforce with the organization.

A. The CMO Framework The **Capability**, **Motive**, and **Opportunity** (CMO) framework is frequently used to understand why insider cyber-attacks occur. In the CMO model, the potential perpetrator needs to have the Capability to commit the attack, the Motive for attacking, and the Opportunity to carry out the breach [14].

Capability is in abundance today. Many Generation Z individuals (born after 1995) and Millennials (born after 1981) have a good foundation in technical skills. Even insiders with weak technology skills can find ways to compromise systems because they understand the nuances of organizational systems, they can turn to the internet to develop hacking skills, they probably have friends with hacking skills, and they can even turn to the Darknet[8] and the Deep web[9] to purchase hacking expertise.

Motives are also in abundance today. We have already looked at some of the *motives* for insider attacks, and they are usually related to financial difficulties. Student loans, credit card debt, health debt and being upset with an employer for being passed over for a raise can prompt breaches.

Opportunities are also in abundance. Over time, employees will gain insight into the inner-workings of organizational systems. Private data is pervasive, and systems that use that data are also pervasive. The net effect is that the procedures used to validate access and protect private data are always trying to catch-up and counter the numerous opportunities that are available for hacking organizational systems.

Organizations can use both preventative and deterrent controls to reduce the probability of minor and major security events [15]. Preventive controls impede criminal behavior by forcing the perpetrator to deplete resources [16]. Preventives controls include sophisticated monitoring technologies, constant attention to authentication protocols to prevent unauthorized access to buildings, software, and databases. For example, an unobtrusive insider security system can be used to control and validate access to all critical encrypted documents and to identify malicious insiders [17]. Organizations usually focus on preventives, because preventives can be implemented and they are under the control of the organization.

This is in contrast to deterrent strategies that focus on the apprehension and punishment of perpetrators as well as on education, legal campaigns and fear appeals. The alarming state of affairs is that it is very difficult to detect intruders and that punishment is the exception rather than the rule. Developing a viable security education, training, and awareness (SETA) program is the

[6] https://www.dni.gov/ Last accessed April 30, 2019

[7] https://www.dni.gov/files/NCSC/documents/nittf/20181024_NITTF_MaturityFramework_web.pdf Last accessed April 30, 2019

[8] https://en.wikipedia.org/wiki/Darknet Last accessed April 30, 2019

[9] https://en.wikipedia.org/wiki/Deep_web Last accessed April 30, 2019

most important activity. A constant focus on security awareness is necessary [18]. It is not enough to have employees complete an online or even an in-person security training class.

Employees need to be immersed in security training, receive feedback and have social interaction with other employees on security issues if the training is to be successful [19]. Some organizations are taking very aggressive steps to counter insider threats from malicious employees, negligent users, and infiltrators. They install software that tracks users' logons, they monitor file and database usage locally and in the cloud, and they record web activity and regularly monitor email activity. These systems, in addition to recording activity, can also be used to send out alerts involving unusual behavior by insiders.

B. Behavioral Preventives As noted many malicious insider attacks are prompted by monetary difficulties and greed. Monitoring credit reports is a very invasive and controversial practice, but some companies are turning to credit monitoring to counter breaches prompted by financial gain, even though several states have taken steps to ban or limit employer's access to credit reports.

Psychological profiling of hackers has been of significant interest for many years, and this interest has dramatically increased because of the significant impact of insider threats [2, 20–23]. Indeed, hacking knowledge is a two-edged sword that can be used for mischief as well as to counter illegal attacks against individuals, organizations, and society. It has been suggested that profiling using the Dark Triad personality traits as a way to evaluate new employees as security threats, similar to the use of the Myers-Briggs Type Indicator (MBTI) in screening employees.

Personality data gathered from employees is usually biased and unreliable. Social desirability bias is a problem in studies involving abilities, personality, and illegal activities. This issue occurs when subjects are less prone to answer questions truthfully that could diminish their social prestige. Individuals will tend to over-report "good behavior" and under-report "bad behavior."

For example, it is unlikely that employees would be very candid in answering the Dark Triad questions. The only way you could obtain such information is to conduct a 360-degree analysis of each employee's personality. That would raise numerous legal and ethical issues and thus would not be a viable solution. We think that this strategy should be approached cautiously for ethical, legal and practical reasons.

Even though White Hat hackers may score high on the Machiavellian and Psychopathy scales, that does not mean they will become Black Hats. Indeed, they may be a strong line of defense against the Black Hats [24].

VI. Conclusion

Threats from trusted insiders are difficult to detect, embarrassing, damage the reputation of the organization, and often destructive and cause serious operational disruption [23].

Companies need to employ educational, monitoring and enforcement strategies that strike the proper balance of protecting organizational information, protecting the privacy of individuals, and also protecting individuals that are falsely accused of violations. A good information source on creating employee policies, legal issues and best practices related to criminal checks and profiling is the Equal Employment Opportunity Commission (EEOC).[10,11]

The key will be to implement organizational procedures, constantly monitor, and develop educational and training programs that will provide the appropriate frequency and intensity of deterrent information so that employees will not ignore but will embrace privacy compliance.

Acknowledgments

This research is supported in part by National Science Foundation Grant No. DGE-1754085.

[10] https://www.eeoc.gov/employers/small-business/checklists/ Last accessed April 30, 2019

[11] https://www.eeoc.gov/policy/docs/factemployment_procedures.html Last accessed April 30, 2019

References

[1] A. Acquisti, C. Taylor, and L. Wagman, "The economics of privacy," *J. Econ. Literature*, vol. 54, no. 2, pp. 442–492, Jun. 2016, doi: 10.1257/jel.54.2.442.

[2] R. E. Crossler, A. C. Johnston, P. B. Lowry, Q. Hu, M. Warkentin, and R. Baskerville, "Future directions for behavioral information security research," *Comput. Secur.*, vol. 32, pp. 90–101, Feb. 2013, doi: 10.1016/j.cose.2012.09.010.

[3] D. Gray and D. Citron, "The right to quantitative privacy," *Minnesota Law Rev.*, vol. 98, no. 1, pp. 62–144, Nov. 2013.

[4] L. J. Pittman, "The elusive constitutional right to informational privacy," *Nevada Law J.*, vol. 19, no. 1, p. 135–186, 2018.

[5] P. B. L. Robert Willison and Raymond Paternoster, "A tale of two deterrents: Considering the role of absolute and restrictive deterrence to inspire new directions in behavioral and organizational security research," *J. Assoc. Inf. Syst.*, vol. 19, no. 12, pp. 1187–1216, 2018.

[6] Y. A. Suh and M. S. Yim, "'High-risk non-initiating insider' identification based on EEG analysis for enhancing nuclear security," *Ann. Nucl. Energy*, vol. 113, pp. 308–318, Mar. 2018, doi: 10.1016/j.anucene.2017.11.030.

[7] T. Michael et al., "Common sense guide to mitigating insider threats, sixth edition," Softw. Eng. Institute, Carnegie Mellon Univ., Pittsburgh, PA, USA, Tech. Rep. CMU/SEI-2018-TR-010, 2019.

[8] J. Gaia, X. Wang, C. W. Yoo, and G. L. Sanders, "The good news and bad news about incentives to violate HIPAA: It depends on the context, and it's mostly bad news," *Working Paper*, 2019.

[9] R. A. Grimes, "Why it's so hard to prosecute cyber criminals," [Online]. Available: https://www.csoonline.com/article/3147398/data-protection/why-its-so-hard-to-prosecute-cyber-criminals.html, accessed: Jan. 2, 2019.

[10] J. Gaia, B. Ramamurthy, G. L. Sanders, S. P. Sanders, S. Upadhyaya, X. Wang, C. W Yoo, "Psychological profiling hacking potential," *Under Review, HICSS Conf.,* 2020.

[11] D. L. Paulhus and K. M. Williams, "The dark triad of personality: Narcissism, machiavellianism, and psychopathy," *J. Res. Personality*, vol. 36, no. 6, pp. 556–563, 2002, [Online]. Available: https://doi.org/10.1016/S0092-6566(02)00505-6

[12] P. K. Jonason and G. D. Webster, "The dirty dozen: A concise measure of the dark triad," *Psychol. Assess.*, vol. 22, no. 2, pp. 420–432, 2010, [Online]. Available: http://dx.doi.org/10.1037/a0019265

[13] D. N. Jones and D. L. Paulhus, "Duplicity among the dark triad: Three faces of deceit," *J. Personality Soc. Psychol.*, vol. 113, no. 2, pp. 329–342, 2017, [Online]. Available: http://dx.doi.org/10.1037/pspp0000139

[14] E. E. Schultz, "A framework for understanding and predicting insider attacks," *Comput. Secur.*, vol. 21, no. 6, pp. 526–531, 2002, [Online]. Available: https://doi.org/10.1016/S0167-4048(02)01009-X

[15] J. Webb, A. Ahmad, S. B. Maynard, and G. Shanks, "A situation awareness model for information security risk management," *Comput. Secur.*, vol. 44, pp. 1–15, 2014, [Online]. Available: https://doi.org/10.1016/j.cose.2014.04.005

[16] R. D. Gopal and G. L. Sanders, "International software piracy: Analysis of key issues and impacts," *Inf. Syst. Res.*, vol. 9, no. 4, pp. 380–397, Dec. 1998, [Online]. Available: https://doi.org/10.1287/isre.9.4.380

[17] S. Pramanik, V. Sankaranarayanan, and S. Upadhyaya, "Security policies to mitigate insider threat in the document control domain," in *Proc. 20th Ann. Comput. Secur. Appl. Conf.*, 2004, pp. 304–313.

[18] E. H. Park, J. Kim, L. L. Wiles, and E. Y. S. Park, "Factors affecting intention to disclose patients' health information," *Comput. Secur.*, to be published. https://doi.org/10.1016/j.cose.2018.05.003

[19] C. W. Yoo, G. L. Sanders, and R. P. Cerveny, "Exploring the influence of flow and psychological ownership on security education, training and awareness effectiveness and security compliance," *Decis. Support Syst.*, vol. 108, pp. 107–118, 2018, [Online]. Available: https://doi.org/10.1016/j.dss.2018.02.009
[20] N. S. Safa, C. Maple, T. Watson, and R. Von Solms, "Motivation and opportunity based model to reduce information security insider threats in organisations," *J Inf. Secur. Appl.*, vol. 40, pp. 247–257, Jun. 2018, [Online]. Available: https://doi.org/10.1016/j.jisa.2017.11.001
[21] G. Dhillon, S. Samonas, and U. Etudo, "Developing a human activity model for insider IS security breaches using action design research," *IFIP Adv. Inf. Commun. Technol.*, vol. 471, pp. 49–61, 2016, [Online]. Available: https://doi.org/10.1016/j.jisa.2017.11.001
[22] M. Kajtazi, B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Assessing sunk cost effect on employees' intentions to violate information security policies in organizations," in *Proc. 47th Hawaii Int. Conf. Syst. Sci.*, Waikoloa, HI, USA, 2014, pp. 3169–3177.
[23] K. Roy Sarkar, "Assessing insider threats to information security using technical, behavioural and organisational measures," *Inf. Secur. Techn. Rep.*, vol. 15, no. 3, pp. 112–133, 2010, [Online]. Available: https://doi.org/10.1016/j.istr.2010.11.002
[24] M. Maasberg, J. Warren, and N. L. Beebe, "The dark side of the insider: Detecting the insider threat through examination of dark triad personality traits," in *Proc. 48th Hawaii Int. Conf. Syst. Sci.*, Kauai, HI, USA, 2015, pp. 3518–3526, doi: 10.1109/Hicss.2015.423.

G. Lawrence Sanders is currently a Professor with the Department of Management Science and Systems, School of Management, State University of New York at Buffalo, Buffalo, NY, USA.
He played a leadership role in developing a new for a Bachelor of Science degree in Information Technology and Management that will start in the Fall of 2019. He is currently a co-pi on a $2.39 million grant from the National Science Foundation related to training future cybersecurity experts. He has authored or coauthored papers in a variety of outlets such as *The Journal of Business*, *MIS Quarterly*, *Information Systems Research*, the *Journal of Management Information Systems*, the *Journal of Strategic Information Systems*, and *Communications of the ACM*, the *Journal of Management Systems*, *Decision Support Systems*, and *Decision Sciences*. His research interests include the behavioral economics and psychological profiling of hacking behavior, gamification, game addiction and teaching blockchain concepts.
Dr. Sanders was a recipient of the Provost's Exceptional Scholars Sustained Achievement Award from the University of Buffalo. He is an Associate Editor for *Decision Support Systems* and Review Editor for the section "Smart Contracts" for the journal *Frontiers in Blockchain*.

Shambhu Upadhyaya (SM'01) is currently a Professor of Computer Science and Engineering with the State University of New York at Buffalo, Buffalo, NY, USA, where he also directs the Center of Excellence in Information Systems Assurance Research and Education (CEISARE), designated by the National Security Agency and the Department of Homeland Security. Prior to July 1998, he was a faculty member with the Electrical and Computer Engineering Department. He has authored or coauthored more than 285 articles in refereed journals and conferences in these areas. His research has been supported by the National Science Foundation, U.S. Air Force Research Laboratory, the U.S. Air Force Office of Scientific Research, DARPA, and National Security Agency. His research interests include broad areas of information assurance, computer security, and fault-tolerant computing.

Xunyi Wang is currently working toward the Ph.D. degree with the Department of Management Science and Systems, School of Management of State University of New York at Buffalo, Buffalo, NY, USA. His research interests include gamification, online healthcare platforms, and user-generated content. He has authored or coauthored in the Journal *of the American Medical Informatics Association*, International Conference on Information Systems, and Americas Conference on Information Systems.