Some Security-Related Reminders

As a discipline, information security has come a long way. Security practices have become more sophisticated over time, and the traditionally emphasized domains, such as physical security, appear to be well under control or perhaps their importance has declined due to the virtualization of today's information systems. Fifty years ago, information systems had recognizable boundaries and it was easy to determine if the moats were filled with water and the bridges were pulled up to secure the castle. Not so anymore.

> "THE FOREMOST PRESSURE ON SECURITY SOLUTIONS IS IN KEEPING THE COSTS OF SECURITY LOW WHILE NOT JEOPARDIZING SYSTEM AVAILABILITY AND FUNCTIONALITY."

Information security over the past few decades has struggled on shifting ground. Personal computers, networks, the Internet, big data and artificial intelligence (AI) are some of the progressive developments that have kept information security tiptoeing around numerous unprecedented challenges. Demands from new generations of users, as in the uses of smartphones, and a shift toward greater efficiency—as in cloud sourcing—have pushed systems to do more and with quicker turnarounds. Society is moving toward paperless communication. Documents such as checks, bank statements, annual reports and proxy statements are no longer physically visible; instead, most documents are delivered through the web. Like it or not, the new mode of work and life is taking hold. Of the three information systems objectives—functionality, availability and security—availability has gained considerable ground. In the past, if a system was not available for some time, only a few users might be affected. Now, in the connected world, most systems are expected to be accessible almost all the time.

The new generation of networked and wireless systems means greater risk, whether users are aware of it or not. But security solutions for new scenarios are not easy. They require creativity and innovation backed by research in security technology to meet challenges of new known vulnerabilities and unidentified blind spots. And yet, the foremost pressure on security solutions is in keeping the costs of security low while not jeopardizing system availability and functionality. Whereas every security solution requires deep insights and granular work, we need to remind ourselves that there are several constants—I call them propositions—in the practice of information security. Only a reminder may be warranted, for these have existed for as long as information systems have been around.

Proposition 1: Accountability for Security Solutions Cannot Be Outsourced

Time and again, we have been told that the ultimate responsibility for security rests with the entity that owns or controls the system. Third parties are essential in the life of an entity, but the choice of engaging them comes with the obligation of managing risk and vulnerabilities that third parties knowingly or otherwise bring to the entity.[1] Whether it is electricity purchased from a local utility or cloud services from a global leader in cloud solutions, the issue remains the same. Is your enterprise safe? The answer is best determined by you only; for others see only part of the puzzle, the missing or vulnerable

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

https://bit.ly/2mqH1UG

Vasant Raval, DBA, CISA, ACMA
Is emeritus professor of accountancy at Creighton University (Omaha, Nebraska, USA). The coauthor of two books on information systems and security, his areas of teaching and research interest include financial fraud, information security and corporate governance. He can be reached at vraval@creighton.edu.

Enjoying this article?

- Read *State of Cybersecurity 2019, Part 2: Current Trends in Attacks, Awareness and Governance. https://www.isaca.org/info/state-of-cybersecurity-2019*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

pieces are your concern. Whether it is a customer or a vendor who provides services or supplies, their association with the entity is bonded in what data they share and how they share and what access rights are granted to them. In the healthcare industry, for example, patient data are accessible to patients, medical insurance providers, physicians and hospital administrators. These include data generated throughout the entire process, from making an appointment with a physician to sharing results of tests to diagnosis and treatment of the disease. Managing relationships intertwined with virtual access to all involved in providing healthcare—including those who work in patient billing—is important, and security questions should be addressed among other aspirations regarding the interconnected system.

The security obligation cannot be fulfilled by merely outsourcing security services. Outsourcing a security service does not mean that the entity can transfer the responsibility of being secure to anyone else; that responsibility still remains with the entity. In structuring such outsourcing arrangements, it is extremely important to address all aspects of security, without compromise, to lower the chances of a breach. One can be blindsided by the comfort with and assurance from service providers, many of whom are formidable enterprises with solid reputations for helping their customers stay secure. However, a misstep on the customer's part may be as simple as not properly configuring the firewall that guards their data residing with the provider. No matter where the data and the information processes go, the enterprise that owns them must take charge of providing satisfactory security of such resources.

It is quite likely that the organization depends on others to deliver some security solutions, as in the case of a cloud service provider (CSP) that assists with protecting the customer's data. Farming out security solutions is not the same thing as delivering the overarching responsibility of risk management. An in-depth understanding of what it is, how it is structured and whether it mitigates the entity's full risk spectrum—these are important questions that only the organization that is responsible can address.

Proposition 2: Most Security Solutions Are Not Guaranteed to Be Foolproof

> "FARMING OUT SECURITY SOLUTIONS IS NOT THE SAME THING AS DELIVERING THE OVERARCHING RESPONSIBILITY OF RISK MANAGEMENT."

In a recent interview, Kevin Mitnick, a formidable hacker turned white hat, said that he has never encountered a system he could not infiltrate.[2] While security measures may seem formidable, as designed, not all of them are infallible. In arriving at a reasonable security solution, developers may have had to balance system functionality and availability against system security, and this could result in a less than foolproof solution. The omission of more rigorous security measures, or just not having thought of a risk and, therefore, its mitigation, would result in gaps. Generally, it is hard to claim that any piece of software with diverse users is safe from vulnerabilities. Besides, mere length and complexity of software could be a factor in knowing confidently how well the ground is covered. Windows Operating System, for example, has approximately 50 million lines of code (LOC). Although LOC is not a comprehensive measure of software complexity, when combined with the nature of software structure, the size of the software engineering team and the turnover among team members, it would provide some understanding of risk scenarios involved. It is, therefore, wise to follow defense-in-depth practices, with layered controls to avoid a single point of failure.

The recent data theft from Capital One Financial provides an example. A veteran of the US federal government, the current chief information security officer (CISO) joined the organization in 2017. An

impression that he was unsuited to the private sector prevailed among those who worked with him. His direct reports departed and some of the replacements left, too. Even routine cybersecurity measures, such as installing an acquired software that would help detect hacks, received little attention.[3] Collectively, it is the human side that fell apart.

A clear sign of the understanding that a software may not be bulletproof comes from the renewed interest in inviting external parties (i.e., researchers, hackers, engineers) to locate vulnerabilities in the organization's code.[4] The organization provides access to the code and offers incentives wherein the size of the reward is aligned with the severity of the vulnerability identified. Inviting outsiders to unearth your software's vulnerabilities is a risk, but the payoff could also be significant. The organization may not have either the right skill set, knowledge of the hackers' motives or tools, or sufficient resources to pursue such moves; only an outsider can do it. And the cost is proportionate to risk identified, so the tactic is cost-effective. Ultimately, the value of this initiative lies in how quickly the organization acts on the vulnerabilities disclosed.

Proposition 3: Humans Are the Dominant Source of Security Compromises

No matter how strong the security measures, compromises invariably happen. Technology only facilitates, it is the humans who do the damage. Despite all the laws, regulations, codes of conduct, enforcement actions and punishments, wrongdoing has been around and will continue to persist. If anything, wrongdoing has been recognized as a norm rather than an exception.[5]

Human tendencies are like etchings on a coin; people cannot change their character easily, at least in the short run. According to one fraud model, a person's disposition—tendencies, propensities, habits—reflects the person's virtues and, depending on the disposition, the person may be self-regarding or other-regarding in nature. Influential managers of self-regarding nature are more vulnerable to the temptation of compromising their moral resolve. As a result, a self-regarding disposition can be considered a red flag in detecting or preventing a crime.[6]

Even organizations with unlimited resources for security are still at the mercy of the weakest link in their chain—the human element.[7] The latest in the exhibition of human frailty is the case of Capital One Financial. Paige Thompson, a former employee of Amazon Web Services, allegedly broke into a Capital One firewall to access data the bank had stored on the Amazon cloud service. The data breach affected 106 million records of card customers and applicants.[8] In 2013, Edward Snowden leaked classified information from the US National Security Agency (NSA). While these are extreme cases of failure in human conduct, many others likely happen daily and are committed by ordinary people who are technology savvy and serve in sensitive areas of information systems. Instead of abusing a vulnerability known to her, Paige Thompson could have helped the bank correct the configuration of the firewall that worked as part of the data protection measure for the cloud.

In an elaborate design of computer security, the one moving target is the human being. It would be easy to dismiss the cases noted as aberrations on the grounds that the actors in such cases are sociopaths. If accepted as a valid generalization, this would also result in a refusal to recognize that at the center of such breaches, there are one or more humans who helped stage the crime. Regardless of categorization, the fact remains that humans are the primary trigger in the collapse. Knowing their character deep down is probably the only remedy.

Conclusion

Answers to human frailty remain obscure, and often the search for solutions is considered fruitless. How do you measure the disposition of key employees? How do you assess the identified dispositional characteristics? Do you promote known managers from within to trusted and critical roles, or do you recruit from outside? The answers are difficult and demand more research. However, in the long run, putting more weight on the human side of wrongdoing will help detect or prevent security breaches. Proposition 1 identifies accountability—the buck stops here—and Proposition 2 suggests that security solutions are incomplete. As a result, much more emphasis must be placed on:

- Knowing the individual who inherits responsibility for security risk
- Understanding how well the individual will cope when it is time to deliver

> "IN THE LONG RUN, PUTTING MORE WEIGHT ON THE HUMAN SIDE OF WRONGDOING WILL HELP DETECT OR PREVENT SECURITY BREACHES."

It would be easy to suggest that existing controls should be strengthened and new ones built. However, there never really is any certainty that security objectives will be fully achieved. It would also be easy to say that human nature is unfathomable and, even if it was not, the tools and techniques to put such knowledge to use do not exist. Therefore, the reliance should be on enforcement. Sadly, the enforcement is often a *post hoc* reaction to what happens and, thus, not a proactive solution. Besides, negative reinforcement through punishment and fines may not be effective. In a field study of daycare centers, when a fine was introduced for late arrival to pick up their child, the incidence of late arrival increased. The parents presumably perceived the penalty as an extra fee for services.[9]

The reality is that due to challenges in deciphering human nature, the progress on knowing how the human link breaks down has been slow. More recently, however, there has been a greater degree of interest in uncovering ways to address why people indulge in a wrongdoing and what can be done to minimize the impact of such tendencies.

Endnotes

1 Raval, V.; S. Shah; "Third-Party Risk Management," *ISACA® Journal*, vol. 2, 2017, *http://www.isaca.org/archives*

2 Maniloff, R.; "An 'Old-School Hacker' Fights Cybercrime," *The Wall Street Journal*, 16 August 2019, *https://www.wsj.com/articles/an-old-school-hacker-fights-cybercrime-11565994214*

3 Andriotis, A.; R. L. Ensign; "Capital One Cyber Unit Flagged Staffing Woes," *The Wall Street Journal*, 16 August 2019, *https://www.wsj.com/articles/capital-one-cyber-staff-raised-concerns-before-hack-11565906781?mod=rsswn*

4 Rundle, J.; "Hackers Go Pro, Seeking Bounties for Bugs," *The Wall Street Journal*, 12 August 2019, *https://www.wsj.com/articles/hackers-go-pro-seeking-bounties-for-bugs-11565602203*

5 Palmer, D. A.; "The New Perspective on Organizational Wrongdoing," *California Management Review*, vol. 56, iss. 1, p. 5-23, 2013

6 Raval, V.; "A Disposition-Based Fraud Model: Theoretical Integration and Research Agenda," *Journal of Business Ethics*, vol. 150, iss. 3, 2018, p. 741-763

7 *Op cit* Maniloff

8 Rudegeair, P.; A. Andriotis; D. Benoit; "Capital One Hack Hits the Reputation of a Tech-Savvy Bank," *The Wall Street Journal*, 31 July 2019, *https://www.wsj.com/articles/capital-one-hack-hits-the-reputation-of-a-tech-savvy-bank-11564565402?mod=searchresults&page=1&pos=13*

9 Gneezy, U.; A. Rustichini; "A Fine Is a Price," *The Journal of Legal Studies*, vol.29, iss. 1, p. 1-17, 2000