ISACA Journal

Volume 5, 2016

Features

How to Audit the Human Element and Assess Your Organization's Security Risk

Tom Pendergast, Ph.D.

The *2016 Data Breach Investigations Report* (DBIR), Verizon's ninth annual report, revealed some grim news—the human threat vector is more dangerous than ever. The latest DBIR reaffirmed the fact that employees continued to play a major role in many of the breaches in the past year. Some 63 percent of confirmed breaches involved weak, default or stolen passwords. Worse, miscellaneous error—staff sending information to the wrong person—accounted for nearly 18 percent of breaches.[1] Despite a wealth of preventive measures, employees remain one of the costliest vectors in a number of data breaches and security incidents, which are increasing at an alarming rate.

Who is at fault? It is hard to say because although employees are clearly identified as a source of risk to the business, boards and executives are also increasingly being held responsible for risky cybersecurity practices. In fact, recent research shows that employees often want to place the blame for cyber shortcomings squarely on the shoulders of boards and executives. Twenty-nine percent of surveyed office workers and IT decision makers in the United Kingdom believe that the chief executive officer (CEO) should be responsible for a significant data breach, while 38 percent of office workers believe boards should be held accountable.[2]

Conversely, these boards and executives are looking to those in IT or information security and asking what they are doing to mitigate the risk posed by the "human element." Whether this examination of current practices is called an audit or something else, the push is on for a more rigorous way of accounting for organizational efforts to address this most vexing security risk: employees. Boards and executives want to know what exactly is being done to address the issues and whether or not these actions are getting the desired results. They want to see that there is a true awareness program in place, i.e., a program that targets meaningful changes in employee knowledge and behavior.

However, those who are asked to perform such an audit will find very little guidance on the subject. The normal sources that guide program evaluation—various documents provided by the US National Institute for Standards and Technology (NIST), the International Organization for Standardization (ISO), and the US Health Insurance Portability and Accountability Act (HIPAA), among others—provide only vague descriptions of awareness program standards and requirements. Fortunately, there is a lot of good work being done in this area that can help organizations evaluate whether they are on the right track in addressing the human threat. The best practices used in some of the world's most risk-aware companies

highlight some core attributes organizations should look for (or create) as they seek to make improvements in the performance of the human element.

Although these best practices take different forms and different names, the best awareness programs do some common things: They assess and analyze the real human performance within the organization; they create a plan for sustained improvement; and they introduce a series of educational interventions (e.g., training and reinforcement) targeted at changing behavior and encouraging a risk-aware culture. Organizations that take the human problem seriously know that they must examine the current state of employee knowledge, skills and attitudes toward security (and privacy, often intertwined in the eyes of employees). This requires stepping back to take a broad look at the organization's culture, assessing all the potential ways employees are (or are not) understanding and responding to security-related risk.

Some of the best ways to understand a company's human risk factors are by conducting employee surveys, both pre- and post-training. These help organizations to understand what employees know today, so appropriate enhancements can be made in the future. Even if the budget is tight, there is no shortage of free industry data, such as the previously cited DBIR, to help an organization understand its specific employee risk. Only when the risk factors are understood can the organization ensure that it works to deliver the right training to the right employees.

Additionally, data from network incident reporting tools, such as security and information event management (SIEM) systems and data loss prevention (DLP) software that may already be in place, will help in understanding the prevalence of data handling issues. The concept of user and entity behavioral analytics (UEBA or UBA) is quickly emerging as a way to parse through all the information collected by SIEM, DLP and other sources, and provide prioritized trend information to the IT professionals monitoring the network. UEBA tools provide real value in identifying patterns and signs that reveal the presence of bad actors in the IT environment.

An exciting emerging use for UEBA is tying it directly to "just-in-time-training" at the spot of the foul. UEBA might identify Jane Doe saving a company document to an unapproved cloud storage site such as Dropbox, Box or Google Drive, and deliver a system-generated pop-up that reminds her of the company's policy on storing company documents in an authorized ecosystem. If Jane does it again, the system then might provide a quick video on the reasons why it is best to avoid an unapproved cloud storage system. Months later, if Jane makes the same mistake again, she might be automatically enrolled in a 15-minute course on approved cloud storage and the appropriate way to store company documents. That is a perfect example of delivering the right training to the right person at the right time.

Separate from network monitoring tools, simulated phishing and social-engineering attacks reveal what risky actions employees are most likely to take when given the opportunity. Such simulations can employ a wide variety of clever techniques to gather passwords, obtain access to sensitive information, or gain physical access through tactics as simple as an email or a phone call, tailgating, or leaving dummy USB devices in the work environment.

A number of vendors offer phishing simulator programs as part of an awareness program package. But vendors that focus too heavily on phishing as the be-all, end-all of cyberthreats should be viewed with some caution. Such an approach targets only one vector of attack and does not do the work of helping employees see the multilayered nature of threats.

Another important step in improving employee performance and culture is understanding the risk specific to the organization's industry and unique business environment. For example, if an organization has a call center, its employees are going to face very different risk factors from those encountered by workers at a bank—it is just the nature of what the job entails. Understanding the risk factors in specific areas of the business allows the organization to deliver training that is tailored to its employees' specific lines of work, which is inherently more relatable and useful. (Training loses much of its effectiveness if it is not relevant.)

Recently, the US Securities and Exchange Commission (SEC) noted that cybersecurity is the biggest risk to the US financial system, with SEC Chair Mary Jo White saying, "What we found, as a general matter so far, is a lot of preparedness, a lot of awareness, but also their policies and procedures are not tailored to their particular risks."[3] A recent report by the SEC Office of Compliance Inspections and Examinations (OCIE) examined the securities industry and recommended the industry as a whole "focus on how training is tailored to specific job functions and how training is designed to encourage responsible employee and vendor behavior,"[4] lending further support for the need for training that is relatable and useful.

While there are many tools for analysis, the goal of them is the same: to come up with a list of five to 10 human-centered risk factors that can be the focal point of efforts to improve (there is no golden number, but the more effective programs limit the number to focus their efforts). Once these human-related risk factors are understood and described, the next step is to develop a plan for an awareness program that addresses the risk factors. Like anything in life, planning is key when it comes to developing a successful, comprehensive awareness program. As part of that plan, organizations should ask themselves if they have set out to implement both formal and informal educational programs. Conventional wisdom would say formal training, often web-based, is the way to go. This is largely due to the ease with which employees can be held accountable for taking training, but the education program cannot stop there if the organization really wants to reach its employees and create that ever-important change in behavior. The best programs do not rely solely on formal training; instead they rely on a variety of educational measures to communicate desired knowledge and behavior to employees.

Once an organization has a solid plan, it needs to quickly inventory whether or not it has the capacity to deliver a program and make good on its plan. For example, does the organization have the capacity to deliver educational reinforcement in the form of games, videos and posters? Are executives on board and willing to champion messages in their daily communication with employees? Are all the right people in place to support and help carry out the program? Organizational capacity to successfully deploy a program is critical to carrying out the plan and will determine whether or not it can go "all in" with an adaptive campaign of phishing, training, posters, games, animations and the like over the course of the year.

In more progressive organizations where the goal is a mind-set change, messages about information protection become part of the daily culture. This may include catchy and memorable posters on the walls, animated videos playing on lobby TV screens, or even a game that gets people competing against one another and allows employees to show what they know about security and privacy. These types of examples are what make the difference when paired with more formal, ongoing training.

One example often cited is Microsoft because it does a great job of this. Anyone who has walked around one of its many campuses should be accustomed to seeing constantly changing messaging about security and privacy. An auditor or executive in any company should see these types of awareness-

raising devices when they walk around. If they do, that is an indication of a company that has made tremendous strides in protecting company information and empowering employees to do the same.

Additionally, a good program delivers training that is role-based or role-specific; employees in different roles, such as human resources (HR) and IT, should receive training tailored to their specialties. Why does this matter? IT employees do not need to know about safeguarding conversations with potential hires, but do need to be well versed in preventing unauthorized data access and use. Conversely, the HR staff need not be as concerned with education on data transmission practices, while protecting sensitive employee information is exactly in their wheelhouse.

Another way to focus education on those who need it is to deploy a means of assessing competence prior to training delivery. How? Rather than giving everyone training on a whole slew of topics—the most expensive and most time-consuming option—individuals can be trained on what they might be lacking, on a case-by-case basis. For instance, Jane Doe has received five simulated phishing attempts over the past year and has forwarded each of them to IT without clicking the link, whereas John Doe has bitten on three of those five phishing campaigns. Based on that information, one can conclude that Jane probably does not need phishing training, but John definitely does. Identifying risk factors at the individual level saves time and money, as the organization likely does not need to train John and Jane equally. As the saying goes, "time is money," and when employees are spending time being trained on things they do not need to know, they are potentially missing out on more important, job-related tasks (and coming to the conclusion that information security does not matter to them!).

Even the organization that has identified its specific risk factors, developed a plan, and is going to implement formal and informal training can do more if it wishes by assessing whether it has a culture of security. This is hard to measure, but not impossible. Information gathering at this level calls for rigorous employee knowledge assessment. A Security Culture Diagnostic Survey has been designed to identify and compare security cultures in organizations and can be found in *People-Centric Security: Transforming Your Enterprise Security Culture*.[5]

Alternatively, organizations can start by looking at what messages managers and executives are (or are not) communicating relative to security. Moreover, are the security-reinforcing systems (e.g., incident reporting, systemic security reviews) valued and utilized? Do any business units outside of information security attempt to meaningfully engage with security issues? If the answer to any of these is "no" or "do not know," the organization may not have reached the point where it has an established culture of security, which should be part of its plan to improve its awareness posture.

A truly mature organization, one that adheres to the principles of tier 3 and tier 4 in NIST's Cybersecurity Framework (CSF),[6] approaches information security as a self-reinforcing program of continuous improvement, not simply an annual event, like the required training model of old. The CSF makes it clear that there are levels to cybersecurity maturity and, in a similar way, awareness maturity. These levels of maturity are conveniently broken out into tiers:

- **Partial (tier 1)**—Risk management is ad hoc with limited awareness of risk and no collaboration with others.
- **Risk informed (tier 2)**—Risk management processes and programs are in place, but are not integrated enterprisewide; collaboration is understood, but the organization lacks formal capabilities.

- **Repeatable (tier 3)**—Formal policies for risk-management processes and programs are in place enterprisewide, with partial external collaboration.
- **Adaptive (tier 4)**—Risk management processes and programs are based on lessons learned and embedded in culture, with proactive collaboration.

Organizations that approach training as simply an annual event likely find themselves in tier 1 or tier 2, whereas organizations that continuously improve are more likely to be found in tier 3 or tier 4.

Whatever tier or maturity level an organization is or aspires to be, the path to understanding and improving starts with stepping back and examining existing practices. The best organizations analyze their human risk factors using a variety of different tools; they develop a plan to change behavior related to those risk factors; they align their resources to execute on that plan; and then they deliver adaptive, flexible education to the right people, when and where they need it. Threats are not slowing down and the best efforts of employees are not keeping up. Employee security awareness education must continually adapt to new and emerging threats. The best way toward this goal is through a robust, risk-aligned and adaptive awareness program.

Author's Note

The author wishes to disclose that Microsoft has done work with MediaPro in the past.

Endnotes

[1] Verizon, *2016 Data Breach Investigations Report*, www.verizonenterprise.com/verizon-insights-lab/dbir/2016/
[2] VMare, "The Cyber Chasm: How the Disconnect Between the C-suite and Security Endangers the Enterprise," The Economist Intelligence Unit, 2016, www.vmware.com/radius/wp-content/uploads/2015/08/EIU-VMware-Data-Security-Briefing.pdf
[3] Lambert, L.; "SEC Says Cyber Security Biggest Risk to Financial System," Reuters, 18 May 2016, www.reuters.com/article/us-finance-summit-sec-idUSKCN0Y82K4
[4] Securities and Exchange Commission, "OCIE's 2015 Cybersecurity Examination Initiative," National Exam Program Risk Alert, vol. 4, iss. 8, USA, 15 September 2015, https://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf
[5] Hayden, L.; *People-Centric Security: Transforming Your Enterprise Security Culture*, McGraw-Hill, USA, September 2015
[6] National Institute of Standards and Technology, Cybersecurity Framework, USA, 2013, www.nist.gov/cyberframework/

Tom Pendergast, Ph.D.
Is the chief architect of MediaPro's Adaptive Awareness Framework, a vision of how to analyze, plan, train and reinforce to build a comprehensive awareness program, with the goal of building a risk-aware culture. He is the author or editor of 26 books and reference collections. Pendergast has devoted his entire career to content and curriculum design, first in print as the founder of Full Circle Editorial, then in learning solutions with MediaPro.