Perspectives | POINT | COUNTERPOINT

Ensuring the Secure Enterprise

By Marc Sokol

The challenge of enterprise security, at first glance, seems one of having the right technology, a more consistent process, and avoiding others with bad intentions. Then again, perhaps you have come across the Pogo cartoon phrase, "We have met the enemy and he is us." The author of our lead perspective, as well as the other thought leaders providing commentary, tell us that in the end we are responsible for what happens. It comes down to awareness of our own human nature, our habits, and the unintended consequences of structures we create in pursuit of specific objectives. It also comes down to enabling choice and the capacity to act in the face of difficult decisions. Building this into your organizational culture and preparing teams to think together—before, during, and after a crisis—this is the real opportunity for HR professionals.

Mary Gentile, author of the book and program, *Giving Voice to Values*, is a global authority on why people choose not to speak up, and what we can do to foster speaking up when it matters most. In her lead perspective, Gentile shares a view on the human factor in enterprise security, along with research that tells us it's more than building a better mousetrap.

The commentaries that follow each build upon the initial perspective.

Malcolm Harkins, a deeply experienced chief information security officer, provides concrete example of how people are both the cause and cure for information security issues.

Ron Sanders, former chief HR officer for the U.S. Intelligence Community, the IRS, and the Defense Department's civilian workforce, shares his observation of habit and response as the critical human factors that impact enterprise security. Ron also sees effective response coming from human resources, and how we can access the levers of organizational DNA to enhance enterprise security.

Judy Docter, the chief human resources officer for a financial institution, provides a final commentary, showing how we put intention into action, and how an HR team comes together to build that culture of risk management called for by other thought leaders. Culture, in this case, isn't just a lofty concept; it's a set of tangible tactics that give voice to individuals and teams across the organization.

If you believe effective enterprise security and risk management requires intentional action before, during, and after critical events, then this issue of Perspectives is for you. After reading the lead perspective and commentaries that follow, you can contact any of the authors or me directly. Let us know what your company is doing to ensure a secure enterprise.

Marc Sokol is executive editor of *People + Strategy*. He can be reached at Marc.Sokol@SageHRD.com.

POINT

The Human Factor in Enterprise Security

By Mary C. Gentile

At its heart, enterprise risk and enterprise security come down to the human factor. This includes tangible and critical arenas for HR risk management, such as working with risks potentially associated with engaging third-party service providers, protection of company data, outright fraud, issues of physical safety, and numerous but less tangible risks to good organizational decision-making that arise from false or incomplete information. In all of these cases, ensuring enterprise security requires more than systems of data flow, approval processes, and monitoring systems.

The most logical and well-communicated control system is useless if it is not observed, and employees can find ways to circumvent the most complete monitoring process, whether they are driven by nefarious intent or merely acting upon a desire to simplify their workload. In the end it comes down to a human factor, how conscious we are of the choices we face, whether we choose to act on this awareness, and the ability to act effectively.

Even within institutions where we assume heightened attention to security and risk, this can be an issue. A recent study by professors at the Army War College illustrates this point. Professors Leonard Wong and Stephen J. Gerras found that lying and untruthfulness are not only very common in the military, but that the proliferation of requirements and systemic assurances demanded of personnel have actually contributed to this phenomenon (*Washington Post*, 2/18/2015, “Lying in the Military is Common, Army War College Study Says” by Dan Lamothe). Individuals feel pulled in seemingly conflicting directions—speed and productivity on the one hand, and compliance with checks and regulations, on the other—and this too often results in a “let’s-not-and-say-we-did” type of response to comply with risk management protocols.

Building “Moral Muscle Memory”

The point here is not to say that the careful design, clear communication and consistent monitoring of risk management protocols is unnecessary or useless, but rather that it is not sufficient by itself. What becomes critically important is an organizational culture and leadership development training that builds the capability, the confidence and the “moral muscle memory’ needed to really act on these protocols.

The most effective way to build this muscle memory is through pre-scripting, rehearsal, and peer coaching. Yes, there are those employees who intentionally flaunt rules and regulations, but this is not the largest group. More often, we see individuals who feel caught in the type of conflict mentioned above (time pressure vs. compliance) or who feel pressured by colleagues or managers similarly caught in what looks like a no-win dynamic. To resist this sort of very real, intense pressure, organizations are beginning to see the value of going beyond communicating the guidelines to actually creating opportunities for employees to practice how they can respond to these pressures, and in a manner that is likely to be effective.

Responding to Pushback

The elaborate speeches that we might craft in our heads are often difficult to deliver and not often effective. What is proven to be more effective is for people to think through the tactics and arguments that will enable more of their colleagues to see the value in compliance. This typically means identifying what is at risk or at stake for all parties in an effort to find ways to mitigate those risks. It also means anticipating the sorts of pushback—the “reasons and rationalizations”—that one is likely to hear when trying to adhere to risk management protocols.

> At its heart, enterprise risk and enterprise security come down to the human factor.

These arguments are actually predictable and therefore, vulnerable to rehearsal for effective response. Rather than engaging in the “preach and pretend” model of compliance training, it is more effective to invite employees to rehearse and peer coach each other, to harness their own creativity in coming up with convincing ways to address challenges, and to hear themselves voice these very responses in front of their colleagues and with their help in enhancing the scripts.

Beyond planning and leading control systems, a key role for HR leaders in enterprise security is building the capacity for effective voice and action in the face of risk. We need to make a conscious choice to build such capacity throughout the enterprise and act on that choice.

Mary C. Gentile, Ph.D., is the creator and director of Giving Voice to Values curriculum and author of *Giving Voice To Values: How to Speak Your Mind When You Know What’s Right.* She can be reached at mgentile3@babson.edu or http://www.marygentile.com.

COUNTERPOINT

The Cause Is Also the Cure

By Malcolm Harkins

Consider the following statistics:

- Seventy-five percent of mobile apps will fail security tests.
- Eighty-four percent of organizations who suffered a breach were out of compliance with application security controls.
- Eighty percent of CISOs believed at the beginning of 2014 that their security framework was strong enough to prevent/manage potential breaches.
- Malware used in the Sony attack would have gotten past 90 percent of cyber defenses.
- Seventy-five percent of corporate boards have no part in reviewing security or privacy risks.
- Seventy percent of employees frequently ignore IT policies.
- Fifty-six percent of employees reuse passwords between personal and corporate accounts.
- Twenty percent of employees share passwords with other employees.
- Fourteen percent of employees say they would sell their passwords to a third party.

The common thread across these data points isn’t just information security, it’s people. People created the web apps that fail security. People manage the systems and applications within their organization. People are the employees who ignore policies including sharing passwords. People are responsible for corporate governance on the boards of directors who have not stepped up to be accountable for corporate oversight. People are the CISO’s who mistakenly believed their existing security solutions were strong enough to prevent potential breaches. People are the creators of the malicious code being spread around daily, taking foothold on our systems driving the cycle of information risk we experience.

People are the cause of the information security issues we face, but they are also the cure. Even as computing shifts to mobile and social technology, and as we see an explosion of applications and device types, it remains that people dynamics determine an organization's ability to manage information risk in the following ways:

Structure drives behavior. If you have the wrong security and a privacy structure that lacks independence from the technology creators or managers, you may not have sufficient tension in the system to effectively deal with information risk. Structures can drive an organizational bias that is siloed and can leave blind spots.

> The common thread across these data points isn't just information security, it's people.

You get what you measure. If your IT organization is managed primarily on cost and the fast deployment of new tools, you will not have adequate information security and privacy in your infrastructure. If your technology product/services team are primarily measured on time to market and margin, then you will likely not have sufficient security development lifecycle and privacy by design to limit vulnerabilities in the technology your organization will release to its customers. If you get the measurements correct you will get movement in improving security.

Culture is the strongest form of control. The top sets the tone for the importance of security. This includes role modeling a "see something say something" approach where we all hold one another accountable for following processes meant to sense, interpret, and act upon risks. This includes the tendency to run toward risky things the organization may want to do to get there early, rather than shape the path of the risk, and be there late or even say no. If the security team isn't working on enabling the business and its employees they will go around the controls meant to manage risk.

The rule of law needs to be applied in the cyber domain. Governments need to cooperate internationally to enhance and protect our digital future. This includes prosecution for those responsible for attacking consumers and corporations.

People may be the cause, but in the end they are also the cure.

Malcolm Harkins is global chief information security officer at Cylance and former chief security and privacy officer, Intel Corporation. He is the author of *Managing Risk and Information Security: Protect to Enable*. He can be reached at mharkins@cylance.com.

Embedding Cybersecurity into Your Company's DNA

By Ronald Sanders

Today's organizations, both private and public, face a daunting variety of threats to cybersecurity, not just from criminals and hacktivists, but also from state and non-state actors who are after their intellectual property. A cyberattack can threaten the very existence of an organization (not to mention the jobs of some of its C-suite officers), but the response doesn't rest solely on a building a better technical solution.

It's all about the people, and that means it's HR's business. It is not just about assuring the skill and trustworthiness of an organization's cyber talent, or mitigating any impact a cyberattack may have on the organization's workforce. Those are relatively obvious. HR also has a strategic role to assure the cyber-efficacy of the organization's culture and its leaders; that role is just as crucial to preventing, detecting, and responding to an attack as your network operations center.

Creating a Cyber-Secure Culture

Ironically, many cyber breaches are the result of nothing more than poor "cyber hygiene"—that is, an insider who unwittingly responds to a spear phishing attack, lets slip a confidential passphrase, or plugs an infected device into the network. These individual behaviors, many of them almost second nature to today's digital natives, can put an entire organization at risk. While this most common attack vector can be slammed shut with nothing more than good, commonsense cybersecurity practices, when it comes to organizational behavior, that's always easier said than done.

Cyber insecurity comes down to an organization's culture…something squarely in the chief HR officer's job jar. The CTO or CISO shares that responsibility, but at the end of the day, good cyber hygiene comes down to ensuring individual employees understand, internalize, and behave according to a set of commonsense cybersecurity standards—just as we would expect them to comply with standards of conduct, ethics, non-discrimination, and the like.

> HR has a strategic role to assure the cyber-efficacy of the organization's culture and its leaders; that role is just as crucial to preventing, detecting, and responding to an attack as your network operations center.

Good cyber hygiene is more than just providing mandatory annual online training. Like other core values, it must be embedded in an organization's DNA, and since HR holds sway over most of the levers that shape that DNA, we have to be as much a part of an organization's cybersecurity strategy as the CTO.

Preparing Senior Leaders for the Worst

While shaping a cyber-secure culture is important, HR's most critical contribution is helping leaders prepare for that almost-inevitable worst case. That too is a shared responsibility with the chief risk officer, the COO, or whoever is responsible for an organization's emergency management protocols. Since no contingency plan survives contact with reality, it cannot stop there; effective cyber response requires leadership practice. Just as the military uses war games and exercises to practice for war, so too must any organization in someone's cyber crosshairs…and that's just about everyone!

My firm is in the business of helping organizations prepare for and respond to cyberattacks (just as my agency was when I served in the Intelligence Community). We've found that war games can be one of the most powerful ways to prepare for the worst, and have conducted dozens of them for commercial and government clients. They can be especially valuable for senior leaders who have not lived through the intensity of a cyberattack, when they must act quickly and collaboratively for the survival of the enterprise. Experiencing that intensity as a leadership team, in the relative safety of a mock attack, can be invaluable when it comes to the crucible of the real thing.

When we take C-suite leaders through these exercises, they often find that placing their organization's technical experts in charge of managing the crisis can be risky. A firm's technical response to an attack is only one piece of the crisis puzzle, and often a relatively small one compared to the risks inherent in dealing with the media, shareholders, suppliers, bankers, customers, regulators, and boards of directors. To successfully navigate through such a crisis, an organization requires C-suite leaders who understand the *strategic business implications* of a cyberattack, and who, like a championship athletic team, have trained to collaborate and connect *all* of the dots—not just the technical ones—in the simulated heat of that crisis.

Think of it as leadership teambuilding on steroids, and that's HR responsibility too.

Ronald Sanders, Ph.D., is a vice president and fellow at Booz Allen Hamilton where he is a leader in the firm's human capital, war gaming, and organizational transformation practice areas. He was the former chief human capital officer for the U.S. Intelligence Community, the chief human resources officer for the Internal Revenue Service, and the director of civilian personnel for the Department of Defense. sanders_ron@bah.com.

Build a Culture of Risk Management

By Judy Docter

As an HR department, do you consider yourself in the risk management business? If not, it may be time to rethink that position. The 2014 "Report to the Nations on Occupational Fraud and Abuse" by the Association of Certified Fraud Examiners, which bills itself as the world's largest anti-fraud organization, shows that employee fraud is on the rise. The report estimates the typical organization loses five percent of its revenue each year to fraud. That works out to a global impact of $3.7 trillion, according to the report. With this type of revenue drain as a result of employee behavior, we must determine appropriate actions.

Tangible Tactics to Give Voice

As Mary C. Gentile says, "What has proven effective is for people to think through the tactics that will enable more colleagues to see the value in compliance and build capacity for effective voice." She is right on with this thinking. As we know, what gets measured gets managed. There are several approaches to developing risk management tactics, particularly for human resources departments.

Give voice to those close to the action. Give voice to those who are actually responsible for managing risk—colleagues on the front line of HR. Imbed a risk management officer into HR's organizational chart, someone that gets up every morning and thinks about identifying, measuring, and managing people risk.

When awareness is coupled with proactive detection measure at the front line, it builds a powerful defense against those who may consider fraudulent actions.

Sponsor the collaboration of HR professionals from across the organization. Next, create a larger HR Risk Committee to broaden the responsibility both within and outside the department. Ensure representation from all areas of HR. The talent acquisition group will likely see risk from a different perspective than the benefits design team. Getting all voices to the table is an important part of the exercise.

Define levels of risk and what that looks like. Have the Risk Committee create a definition for different levels of risk. We know that the risk of an employee violating the dress code (assuming you still have one), or not protecting customer data is not the same. Some risks are greater than others. Build language that defines the difference.

Measure, report, and widely communicate risk levels to drive ongoing risk mitigation. Provide the Risk Committee with the responsibility and accountability to identify and rate the risks within HR, and importantly, determine actions for mitigation. Then, broadly communicate the action plan.

This approach helps to build a culture of risk awareness. When awareness is coupled with proactive detection measures at the front line, it builds a powerful defense against those who may consider fraudulent actions.

Judy Docter is chief human resources officer at Associated Bank. She can be reached at judy.docter@associatedbank.com.