TOPICS COVERED
// Risk and Strategy

MEGAN BELCHER ON ENDURING CULTURE

Bringing Impact and Imagination to Your Privacy and Cybersecurity Culture

Written by Megan Belcher

There is no compliance topic that has more firmly shifted itself to center stage in the C-suite and for ethics and compliance professionals than cybersecurity. Concurrently, there is no compliance topic that is evolving as quickly or demands as much agility from ethics and compliance officers as protecting their company's information security. As companies look to their compliance professionals for leadership, support, and protection in those spaces, those compliance leaders should continue to look to the long held adage of "Culture eats strategy for breakfast." for inspiration.

In 2015, Ari Kaplan Advisors and the technology company Nuix published a survey entitled, "Defending Data: Turning Cybersecurity Inside Out With Corporate Leadership Perspectives on Reshaping Our Information Protection Practices." That survey revealed that it was not complex and unpredictable technology failings that gave most businesses the greatest concern when it came to cybersecurity threats. It was employee behavior.

It is no surprise to those who work to ensure their organizations' information security that human behavior remains the largest obstacle to information security. In the Kaplan/Nuix survey, 93% of respondents claimed human behavior was the biggest threat to their organizations' security, up from 88% the year prior. Combine that data with the increased prevalence of practices that rely heavily on individual human decisions to ensure security protocols are followed, like BYOD policies and cloud usage, and you quickly recognize the importance of driving a culture of compliance and integrity around cybersecurity and information governance practices.

What does that mean to you as you seek to drive a robust culture of cybersecurity in your organization? Your employees and their behavior are the first line of defense. To that end, you must not only enable them with the knowledge they need to protect the integrity of your systems, but also drive the desire and discipline to implement that knowledge. In short, you must create the culture that will support your strategy. How do you do that? This author shares key steps and food for thought below.

Move beyond the concept of an insider threat

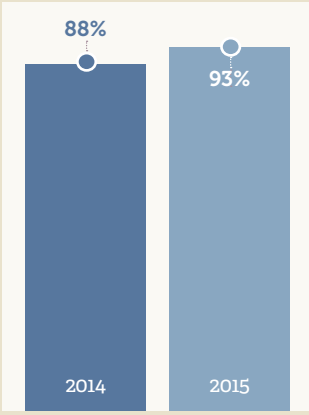
When you start thinking about shifting your culture to support your cybersecurity compliance program, it is important to move beyond just thinking about insider threats. An insider threat is someone who is within your organization and is actively working with mal intent to expose your confidential information or the integrity of your systems. However, while very damaging, those are the rarer threats with a discrete solution, namely locating and cauterizing the threat.

However, when undertaking truly impactful culture change, you need to look at the broad behavior of your employee population that is neither intentionally malicious nor part of a master plan. When you think about strengthening your culture, you need to think about the behaviors your employees exhibit as part of their muscle memory. What are the casual technology behaviors in which they engage in their day to day work? What outcomes are the product of mere sloppiness? What are the business behaviors that are driving the failures in your best practices? In short, think more broadly about your negligent neighbor, not your sinister nemesis.

Understand your base

You also need to understand the population of people you are trying to co-opt into your culture shift. Are they all your employees? Do you have a significant contractor or vendor population that you are trying to also influence? Do you have other third parties accessing your systems or interacting with your employees through your systems? By determining who your audience is, you can begin to be thoughtful about how you will influence their behavior.

Facts & Figures



*In 2014, **88%** of respondents claimed human behavior was the biggest threat to their organizations' security vs **93%** in 2015. Source: Nuix and Ari Kaplan Advisors Study, "Defending Data: Turning Cybersecurity Inside Out With Corporate Leadership Perspectives on Reshaping Our Information Protection Practices."*

By taking the time to thoughtfully understand your culture, your priorities, and your desired future state, while bringing the right dose of imagination to your process, you will be on the path to driving the culture and behaviors you aspire to build.

Separately, you need to understand how your population performs their work and interacts with your technology. Are they primarily white collar workers that are incredibly mobile and leverage VPN access? Do you have a heavy manufacturing workforce that is using computers to run your lines, while also checking their personal email through a web browser on those same computers? Is it a mix with diverse issues across your organization? A holistic way to undertake both a big picture and granular view of how your employee population works, as well as any third parties who use your systems, is through a cybersecurity culture survey. You can not only assess how those populations work and leverage your technology, but also their beliefs and understanding about what they should be doing from a best practice cybersecurity perspective.

Know where you need to plug the dam

Once you assess your population and understand the behaviors that are creating drag on the culture you want to achieve, begin taking an inventory of the behaviors you want to shift. These may range from the hyper-technical (e.g., individual security configurations in the set-up of a SharePoint site) to very mechanical behaviors (e.g., connecting to unsecured wireless networks). You can then leverage that inventory as a platform to prioritize where you will focus your education and behavior expectation efforts, as well as your resources.

Don't go it alone

Compliance professionals experienced in leading the charge on any culture shift know how valuable their cross functional partners can be. A cybersecurity focused culture shift is no different. Ensure you are establishing a team that includes your internal IT team, your HR partners, your communications subject matter experts, the right players from your legal team, and a representative from your corporate security team. In addition, if your company has the benefit of an organizational change group, tap into their expertise to help deliver against your culture change goals. Separately, do not forget to leverage your own internal and external network for lessons learned on culture change, and unofficial benchmarking on best practices and most likely potholes.

Find diverse and imaginative avenues to communicate and tell stories

No culture shift will hinge on a company's standard suite of annual training. To drive change in behaviors as imbedded as the day to day practices of your employees' interaction with your technology, you have to find multiple and impactful ways to reach them. And those avenues must resonate with them in an authentic way.

That is not to say that you should not use your periodic training programs through your LMS. You should. However, you should also find the right regular drumbeat of communications for your organization that are focused on your overall communication strategy, using the priorities you identified in your initial assessment. Send visually engaging emails with key lessons and stories. Develop short films you can deploy on your company portal. Leverage your leaders as cause champions to talk about how they are changing their behavior, and why they care about the issue. Ask your Board to talk about the importance of employee behavior in furtherance of cybersecurity at your annual meeting. The options available to you are only limited by your creativity.

Which leads us to the final critical reminder, namely that you should not forget to bring your imagination to the table as you seek to deploy your culture strategy. Your employees are always looking for new and creative ways to engage with their employer, and particularly in the compliance space. Most employees want to do the right thing, they simply need to understand the "what", but more importantly need you to inspire the "how."

There is no compliance topic that has more firmly shifted itself to center stage than cybersecurity.

To that end, be thoughtful about how you can catch employees' attention and engage with them real time. Create a competition to "catch" employees in the act of engaging in a cybersecurity best practice and leverage your internal social media outlet to celebrate the success. Create a false "breach" where you have managers who print confidential information, so they can be "caught" by employees to test understanding of your polices and your reporting systems. Create a system of employee issued rewards for those who are witnessed heading off a cybersecurity failure, like deploying a phishing email immediately to the IT cybersecurity team. In short, do not use the same old strategies, or you will get your same old culture.

By taking the time to thoughtfully understand your culture, your priorities, and your desired future state, while bringing the right dose of imagination to your process, you will be on the path to driving the culture and behaviors you aspire to build. Without leveraging those steps and the key stakeholders in your organizations, you leave your employee population unprepared and your company ripe for a cybersecurity breach. If you bring a strong game on the culture front, your strategy will thrive.

Author Biography

Megan Belcher *joined ConAgra Foods' legal department in 2007 and was promoted to be the company's Chief Employment Counsel in 2009. Megan has been the Vice President & Chief Counsel – Employment Law and Compliance at ConAgra Foods since 2014. In that role, she established and launched the company's first enterprise-wide compliance initiative, Integrity First. Before joining ConAgra Foods, Megan practiced with Am Law 200 firm Husch Blackwell LLP in its labor and employment department. Megan has over 15 years of experience in the compliance, litigation, and labor and employment spaces.*