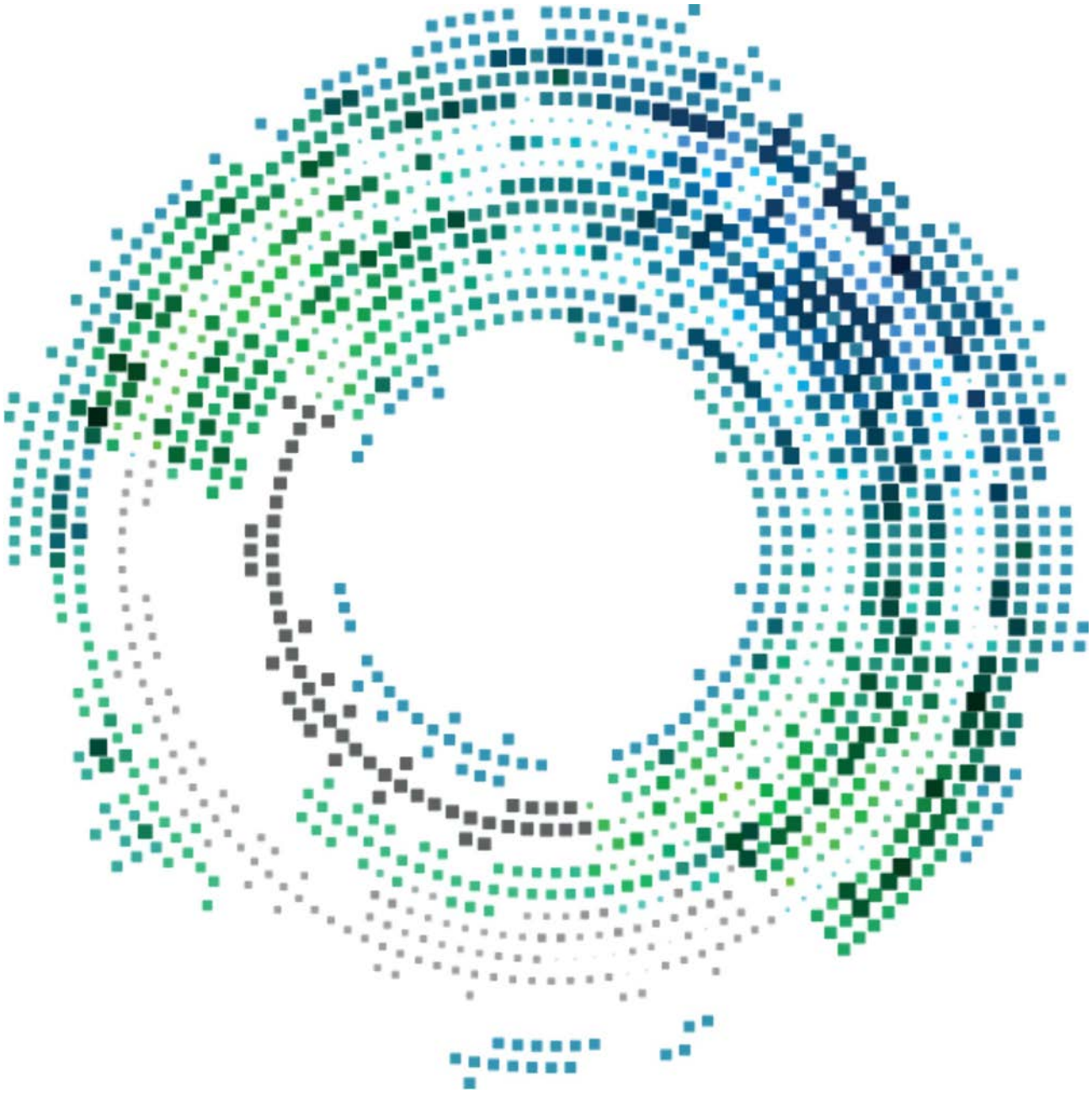
Deloitte.

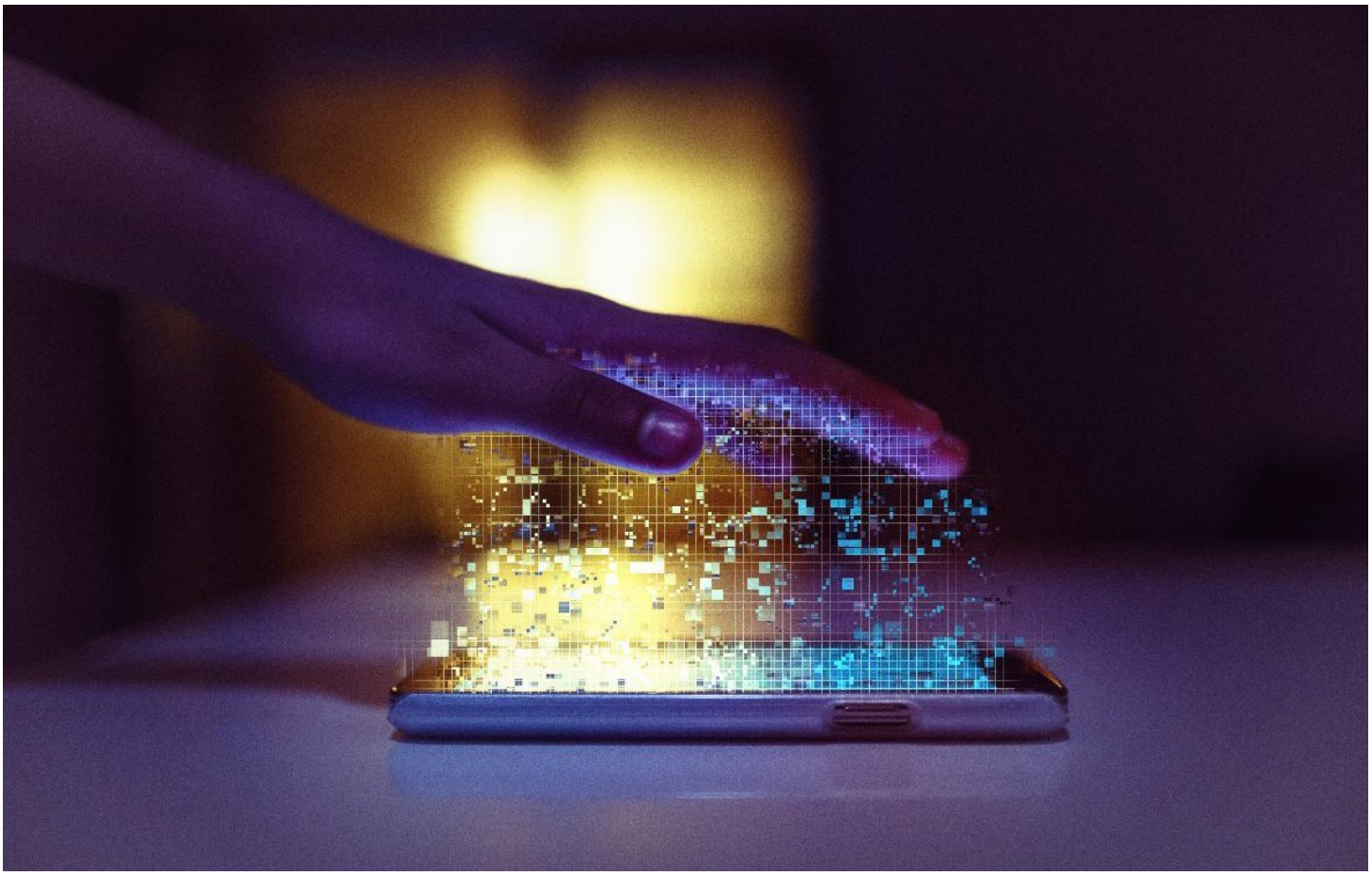


Cultivating a cyber risk-aware culture

The value of people

Table of contents

A cyber risk-aware culture: Why it matters	1
Creating a cyber risk-aware workforce	3
The elements of culture in action	5
Getting started	7
Avoiding common mistakes	9
It’s time to begin	11
References	13



A cyber risk-aware culture: Why it matters

It started with an email. A survey request from Jamie's employer offering gift cards to respondents. Jamie clicked the hyperlink included in the email and completed the survey, submitting sensitive company information in response to survey questions. Jamie, like many employees, was a victim of a spear phishing attack, a targeted email technique used by malicious actors to obtain confidential information from organizations. Jamie's actions resulted in a data breach, which cost the organization millions of dollars in credit monitoring fees to customers and employees, in addition to longer-term damage to the company's reputation, which resulted in lost customers and regulatory fines.

While Jamie's story is a fictional anecdote, situations in which an employee's actions contribute to a cyber incident are very common. According to a Ponemon Institute data breach report, which surveyed 383 companies across

12 countries, human error was the cause of 27% of data breaches.[i] The overall cost of data breaches grows more expensive each year: the average total cost of a data breach in 2016 was $4 million, a 29% increase from 2013.[ii] And recent Deloitte research shows that these costs are just the tip of the iceberg. Deloitte's *Beneath the Surface of a Cyberattack: A Deeper Look at Business Impacts* demonstrates that cases involving intellectual property (IP) theft, or attempts to disable critical infrastructure, for example, can have much more significant financial impacts on organizations.[iii]

Despite a forecasted spending of $170 billion by 2020 on cybersecurity, organizations continue to experience cyber incidents.[iv] Additionally, a 2016 Deloitte Center for Financial Services study found that financial services companies have continued to increase their spending on cybersecurity at a pace that is not sustainable in the long term.[v] While continued cyber incidents can be attributed to the constant changes to technology, regulatory requirements, and threats, **there is also a 'people component' at work — many organizations have not cultivated an organizational culture that reinforces their cyber risk management technology investments.**

If cyber risk values and behaviors are not ingrained in an organization's culture, employees may not be aware of or support their organization's security technology and policies.

Instead, they can become part of the problem, creating attack vectors for bad actors to exploit. Without a cultural focus on cyber risk, some employees follow existing incentive paths to get the job done quickly, which involve 'work-arounds' or avoiding safeguards all together, which can put their organization at risk.

A cyber risk-aware culture also encourages and challenges employees to think "cyber" when the unexpected happens. Rather than attributing a mysterious event to an anomaly or hoping it won't happen again, employees with a cyber risk-aware culture are more likely to report and escalate unknown events. "If you see something, say something." A cyber risk-aware culture exists when an organization's **values and the behaviors of its leaders and employees collectively and actively support the enterprise-wide cyber risk management strategy.**[vi]

Creating a cyber risk-aware workforce

Organizational culture is "'the way things work around here…' it includes the values, beliefs, behaviors, artifacts, and reward systems that influence people's behavior on a day-to-day basis. It is driven by top leadership and becomes deeply embedded in the company through a myriad of processes, reward systems, and behaviors."[vii]

A positive organizational culture leads to higher profitability for organizations, and a negative culture can decrease profitability.[viii] Similarly, an organization that cultivates cyber risk-aware values and behaviors can more effectively manage cyber risk, increasing the effectiveness of its technology safeguards.

Changing culture may seem a daunting task, but by targeting the right elements, organizations can cultivate a culture that mitigates cyber risk.

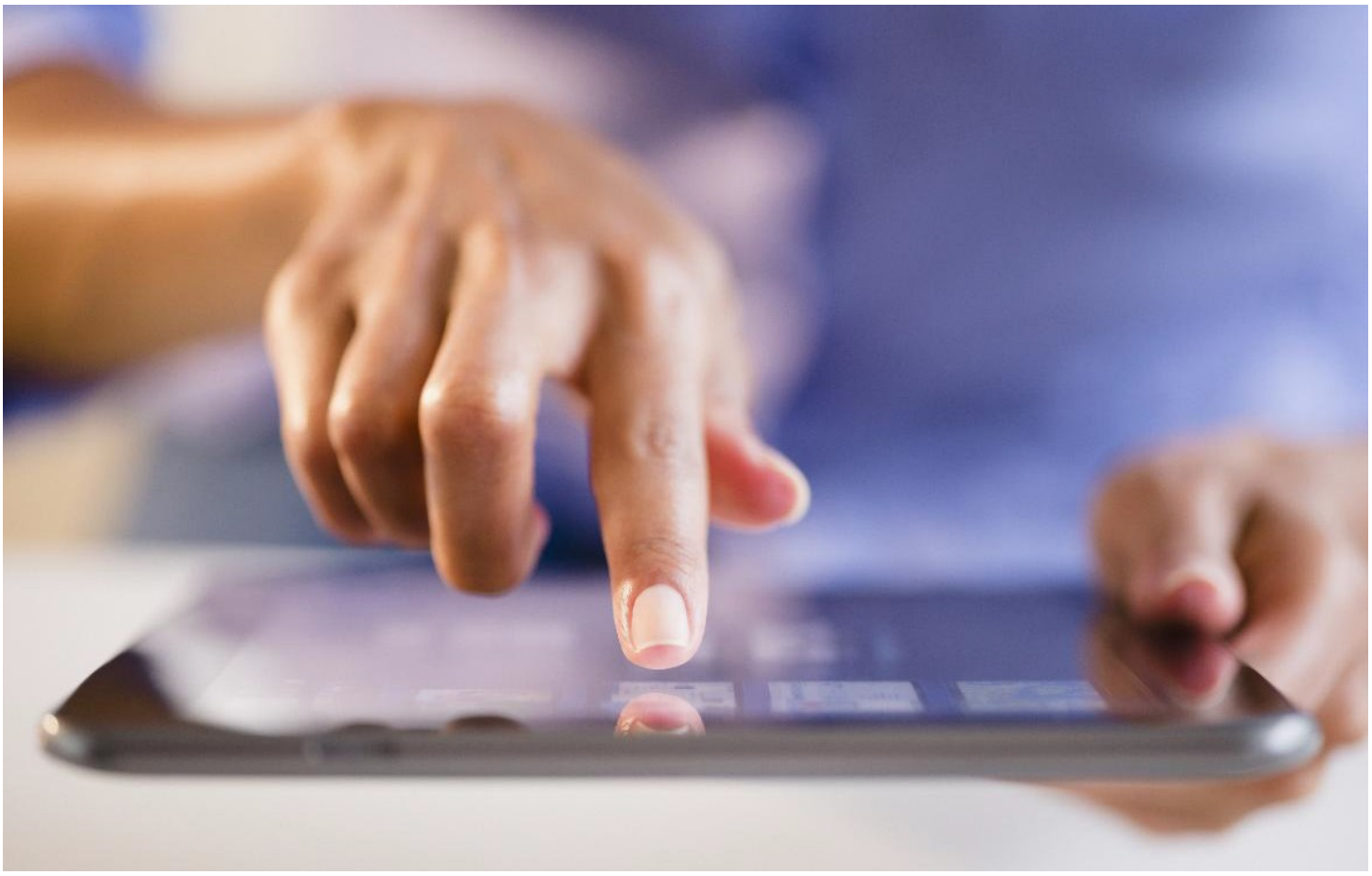
Four key elements that organizations should focus on to cultivate a cyber risk-aware culture are leadership, learning, communications, and the talent lifecycle.

- **Leadership:** Leaders model ideal behavior for their organization, and employees look to company leadership to set expectations for cyber risk management. Leaders must signal to employees that cyber risk management is a top priority if they want employees to adopt cyber risk-aware practices. They can do this through understanding cyber threats to their lines of business or product offerings, fostering collaboration to discuss cyber risk topics such as emerging threats in the news, monitoring cyber risk metrics pertinent to their business area, and elevating cyber risk oversight to visible senior leadership.

- **Learning:** Learning events, usually recognized as formal training, are often an employee's first exposure to their organization's culture. Organizations should require regular-interval cyber training and emphasize the importance of desired cyber behaviors in new hire and other learning events, including inclusion of non-traditional creative learning experiences such as micro-training, gaming, and mobile delivery.

- **Communications:** Communications (or lack thereof) in company policies, from leaders, Human Resources, and other internal sources contribute to and reinforce the organization's culture. Communications should start with a compelling "burning platform" for change and create a personal connection and commitment from individuals to the cyber risk issues by addressing the "how does it impact me" questions and continue to reinforce employee understanding of desired cyber risk-aware hygiene, norms, and compliance requirements. Organizations should use communications through multiple channels (not just email) to tailor to diverse corporate audiences (e.g., text messages, printed material, videos, and collaboration platforms).

- **Talent Lifecycle:** Employees understand the priorities of an organization through its Talent Lifecycle—how it hires, promotes, develops, and recognizes its employees. The Talent Lifecycle can be leveraged to drive accountability for cyber risk-aware practices, signaling that cyber risk management is important to the organization and affirming that it should also be top-of-mind for employees. Linking desired cyber risk behavior to performance management processes may be an the obvious next step, but consider encouraging accountability further by publishing cyber risk metrics by business unit or individual "leaderboards" to foster recognition. Offer (and reward) two-way communication opportunities such as crowd sourcing of threat vectors.



The elements of culture in action

Culture can be difficult to change, but not impossible. Many organizations have successfully changed employee behaviors, resulting in a new culture, by using one or more of the culture elements: leadership, learning, communications, and the talent lifecycle. A few case studies are included below that show how targeted efforts led to the desired business results.

Leadership: Alcoa CEO championed a safety-focused organizational culture.[ix]

When Paul O'Neill became the CEO of aluminum company Alcoa, he emphasized employee safety as his highest priority, requiring that plant managers notify him personally of any accidents in their jurisdiction within 24 hours and immediately develop a plan to make sure a similar accident never occurred again. Mr. O'Neill believed that any accidents were a direct result of leadership failure. Under Mr. O'Neill's leadership, Alcoa significantly decreased its worker accident rate (which fell to 0.05% of the U.S. average), increased its income five-fold, and increased its market capitalization by $27 billion.

Learning: Lockheed Martin managed cyber risk with experiential learning[x]

Lockheed Martin's "The I Campaign" trained employees to detect spear phishing emails and to report them to the company's Computer Incident Response Team, and then tested employees' knowledge by sending them spear phishing emails. "The I Campaign" resulted in a 55% improvement in employee detection and proper handling of spear phishing emails, which helped to foster a cyber risk-aware culture at Lockheed Martin.

Communications: The healthcare industry increased hand-washing compliance by tailoring communications to change healthcare worker behavior.[xi]

Poor hand-washing compliance among healthcare workers contributes to the nearly two million patient infections contracted annually during hospital visits. To change healthcare worker behavior, researchers reframed the language on hospital signage to focus on how hand- washing benefited patients' health, as opposed to hand-washers' health. Simply re-framing the communications on signs posted around hospitals increased the likeliness of healthcare workers to wash their hands by 10%.

Talent Lifecycle: When Delta Air Lines acquired Northwest Airlines, it created a culture of employee loyalty by instituting employee-focused rewards.[xii]

Rapidly merging two companies, labor union relationships, and disjointed manager-worker relationships could have created a negative culture at Delta, but CEO Richard Anderson created a loyal employee culture with rewards such as: generous bonus structure and stock options, high-quality hotels for crew members, and flexible employee scheduling. In two years, Delta's employees voted to eliminate unions and Delta saw an increase in "lifer" employees.

Organizations can change employee values and behaviors to support cyber risk-aware priorities by targeting the same culture levers that Alcoa, Lockheed Martin, the healthcare industry, and Delta used successfully.

Getting started

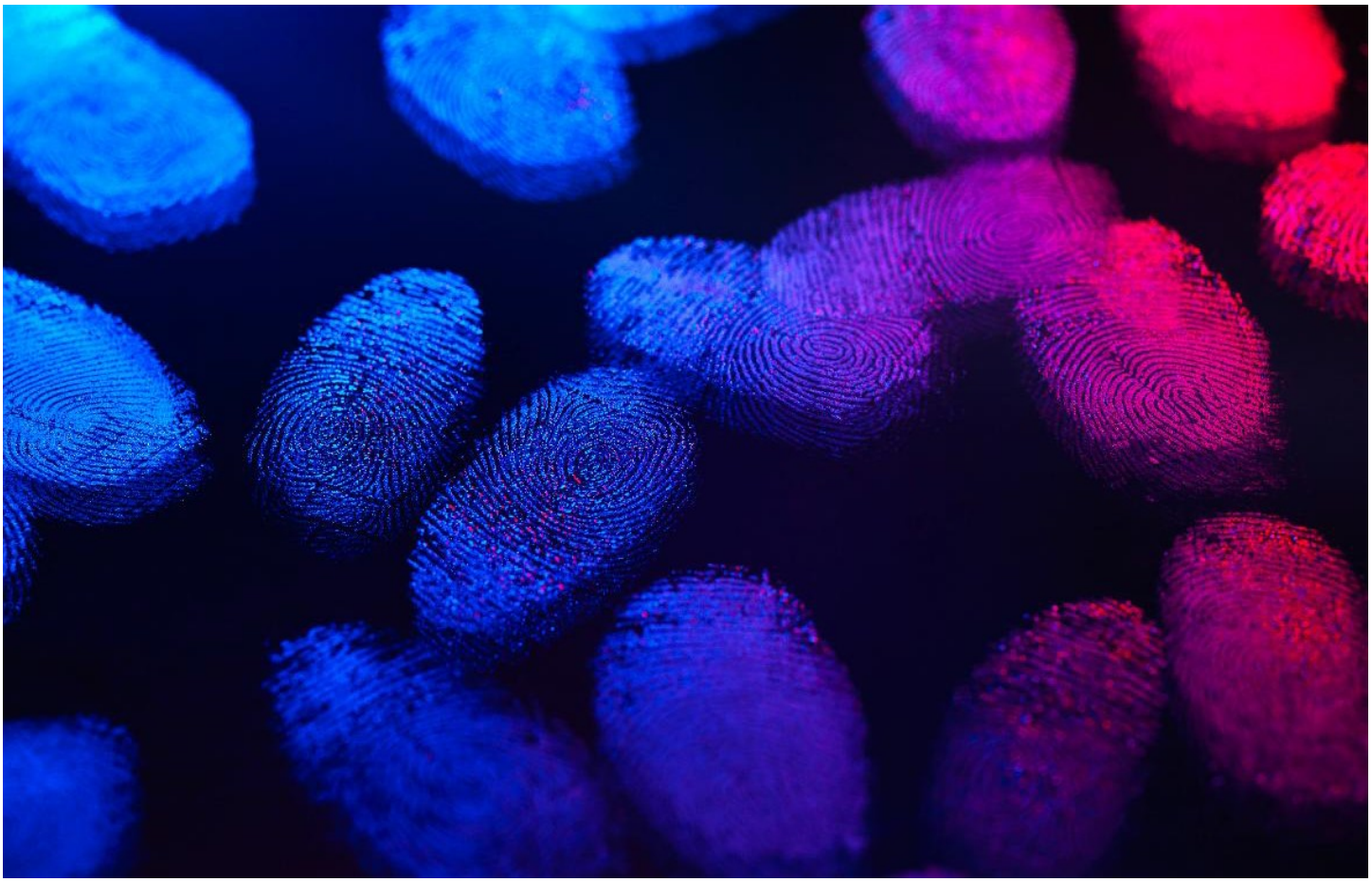
Currently, the focus of many organizations' cyber risk management strategies is technology safeguards, yet threats continue to push through. Using the culture elements to cultivate a cyber risk-aware culture can increase the effectiveness of technology safeguards by arming an organization's people with the right behaviors when a cyber risk comes to them.

Step 1: **Leverage your organization's current culture to create an appropriate cyber risk-aware culture**. What are your organization's mission and core values? What are the prioritized threats, bad actors and "crown jewel" assets within your company that your cyber risk program is focused on? The message and approach for a cyber risk-aware culture should resonate with your employee base, linking incentives and communications to the organization's overall strategy, mission, and core values.

Step 2: **Define a cyber risk-aware culture vision.** Consider the size, governance structure, regulatory obligations, mobility requirements, innovation preferences, and risk tolerance of your organization when designing the future state culture. What does a cyber risk-aware workforce look like in your company?

Step 3: **Articulate the desired values and employee behaviors for a cyber risk-aware culture**. What type of behavioral norms do you hope to ingrain in the new culture? How will you define cyber risk-aware practices for your organization? How will you segment cyber risk-aware practices by department or function to increase adoption (e.g., the sales employees will have different cyber risk-aware practices then engineers)? Messaging should come from the top, disseminated consistently by your organization's leadership. What cyber risk actions do you want employees to exhibit as part of this culture change (e.g., skepticism when receiving unexpected emails, thinking cyber when unexpected events occur, considering cyber risks as they perform their operational tasks, feeling empowered to STOP or escalate if they think a possible cyber risk is present…)?

Step 4: **Develop a plan for getting from where you are to where you want to be.** It can take up to two years to shift a culture, so plan for the short- and long-term. In the short-term, think about quick wins; are there high-risk departments where you can pilot culture efforts that will yield a higher reward?[xiii] Are there one to two high risk behaviors you want to change quickly? Are there threats that are most prevalent or most impactful to your industry today (e.g., ransomware)?



Avoiding common mistakes

Many organizations have attempted to cultivate a cyber risk-aware culture in the past, but have faced challenges. Here we have identified a few common mistakes that can keep organizations from achieving a cyber risk-aware culture, as well as considerations to avoid these mistakes.

1. **Waiting for a breach to happen.** Be proactive, don't wait for a breach to begin cultivating a cyber risk-aware culture. Culture changes happen gradually and by starting early, you can have time to plan and implement a thoughtful culture initiative.

2. **Culture objectives are not aligned to cyber risk management strategy.** Culture objectives and plans should be aligned with the organization's overall cyber risk management strategy. While preventing data breaches is important, make sure your cultural principles include behaviors to mitigate the top cyber risks, such as operational impacts or denial of service.

3. **Not tailoring efforts by employee populations.** There is no one-size-fits-all solution—each company's cyber risk-aware culture will be unique. Segment your employee population based on their respective cyber risk responsibilities, and tailor engagement, learning experiences, messaging and behavioral change to each based on their roles and responsibilities. For example, sales employees will require different training than information technology employees.

4. **You've only got a hammer, so everything looks like a nail**. An effective cyber risk culture campaign should leverage multiple channels to engage with your diverse corporate audience. Organizations should integrate multimedia, mobile messaging, and in-person communication tools along with traditional emails and print material.

5. **Don't wait, act now and learn as you go.** Start small, piloting one or two leadership, learning, communications, and talent lifecycle initiatives to evaluate effectiveness. Then, roll out the top initiatives to the entire enterprise.

It's time to begin

Many organizations are at a crossroads. The rate at which cyber risk management technology investments are increasing is not sustainable; a long-term, cost-effective solution is needed to reinforce technology investments. At the same time, the information technology environment in which today's organizations operate is constantly evolving. Threats are adapting, regulatory requirements are growing, and customer and employee expectations for protection are increasing. Organizations must cultivate a cyber risk-aware culture to address the cyber risks on the horizon.

Including culture in your cyber risk management strategy can increase your ability to manage cyber risk, similar to how changes to organizational culture fostered desired employee values and behaviors at Alcoa, Lockheed Martin,

Delta Air Lines, and others. Through leadership, learning, communications, and the talent lifecycle, you can begin changing the values and behaviors of your people to cultivate a cyber risk-aware culture.

Deloitte delivers Cyber Risk People Solutions that go beyond technology and bring people into the cyber risk management solution.

References

[i] Ponemon Institute, "2016 Cost of Data Breach Study: Global Analysis," IBM, June 2016, http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03094WWEN

[ii] Ponemon Institute, "2016 Cost of Data Breach Study: Global Analysis," IBM, June 2016, http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03094WWEN

[iii] Emily Mossburg, et al., "Beneath the Surface of a Cyberattack: A Deeper Look at Business Impacts," Deloitte, 2016, https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-risk-beneath-the-surface-of-a-cyber-attack.pdf

[iv] Mike Billings, "The Daily Start-up, Increased Spending in Cybersecurity Drives Funding Surge," *Wall Street Journal*, 17 February 2016, http://blogs.wsj.com/venturecapital/2016/02/17/the-daily-startup-increased-spending-in-cybersecurity-drives-funding-surge/

[v] Sam Friedman, "Taking Cyber Risk Management to the Next Level," Deloitte University Press, June 22, 2016, http://dupress.com/articles/cyber-risk-management-financial-services-industry/

[vi] Marc Kaplan, et al., "Shape Culture, Drive Strategy," *Global Human Capital Trends 2016*, Deloitte University Press, 2016, http://dupress.com/articles/impact-of-culture-on-business-strategy/

[vii] Marc Kaplan, et al., "Shape Culture, Drive Strategy," *Global Human Capital Trends 2016*, Deloitte University Press, 2016, http://dupress.com/articles/impact-of-culture-on-business-strategy/

[viii] Alina Dizik, "The Relationship Between Corporate Culture and Performance," *Wall Street Journal,* February 21, 2016, http://www.wsj.com/articles/the-relationship-between-corporate-culture-and-performance-1456110320

[ix] Charles Duhigg, *The Power of Habit*, Random House, February 28, 2012

[x] Kelly Jackson Higgins, "How Lockheed Martin Phishes Its Own," *Dark Reading*, April 25, 2013, http://www.darkreading.com/risk/how-lockheed-martin-phishes-its-own/d/d-id/1139629

[xi] "Patients' Health Motivates Workers to Wash Their Hands," *Psychological Science*, April 29, 2011, http://www.psychologicalscience.org/index.php/news/releases/patients-health-motivates-workers-to-wash-their-hands.html

[xii] Jay W. Lorsch and Emily McTague, "Culture is not the Culprit," *Harvard Business Review*, April 2016, https://hbr.org/2016/04/culture-is-not-the-culprit

[xiii] Alina Dizik, "The Relationship Between Corporate Culture and Performance," *Wall Street Journal*, February 21, 2016, http://www.wsj.com/articles/the-relationship-between-corporate-culture-and-performance-1456110320

Contacts

Sharon Chand
Principal | Deloitte Risk and Financial Advisory
Cyber Risk Services
Deloitte & Touche LLP
shchand@deloitte.com

Elaine Loo
Principal | Deloitte Consulting
Human Capital
Deloitte Consulting LLP
eloo@deloitte.com

Contributors

Debbie Merovitz, Specialist Leader, Human Capital, Deloitte Consulting LLP
Kirti Tidke, Senior Manager, Cyber Risk Services, Deloitte & Touche LLP
Tara Mahoutchian, Manager, Human Capital, Deloitte Consulting LLP
Rachel Stewart, Manager, Human Capital, Deloitte Consulting LLP
Lauren Moreno, Senior Consultant, Human Capital, Deloitte Consulting LLP

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

About Deloitte
Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/about for a detailed description of DTTL and its member firms. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2017 Deloitte Development LLC. All rights reserved.