BEST PRACTICES FOR ENGAGING EMPLOYEES IN CYBERSECURITY

BACKGROUND

We're all vulnerable. That's just one of many lessons to take from the recent Equifax data breach, which affects an estimated 143 million consumers. While by far the largest we know of, Equifax is one of nearly 1,000 data breaches to date in 2017, according to the Identity Theft Resource Center.

Whether due to malware, social engineering, lost devices or other causes, data breaches affect companies of all sizes in every industry. And, unfortunately, employees often are a factor. IBM estimates that 60 percent of breaches can be linked to insiders, including both human error and criminal behavior.

While most companies have increased their budgets to secure their networks and enhanced their policies and procedures, many underestimate the importance of data security to how customers perceive value. In FleishmanHillard's 2017 Authenticity Gap Report, Authenticity in an Uncertain World, 59 percent of consumers said companies are not taking data security threats seriously and are not investing enough in their IT to protect against breaches, which creates a gap between what customers expect and experience.

Educate and Engage Your Employees

Information security, corporate compliance and ethics are serious business, but many companies take a check-the-box approach to educating and engaging their employees. If you haven't rethought your program in recent weeks, now's the time. Here are some best practices to consider.

- **Mix it up**. Use posters, video, games, intranet ads — in addition to training and email — to keep your messages in front of your employees. Consider emotion, humor and animation as hooks to get their attention. Use analogies (e.g., leaving keys in the car with the car running) to make information relatable.
- **Revamp your training**. Use your training to truly engage your employees and challenge them to think through different scenarios and outcomes. Use real-world events to illustrate the threats your company encounters and potential repercussion to your brand, reputation and results. Vary training and scenarios each year to further educate and enlighten your team, including those that spotlight malicious actions from employees. Shift from annual 'one and done' training to quarterly modules that foster retention, such as experiential approaches that push employees to stop, think and act in a way that involves more than just clicking a mouse.
- **Focus on the frontline**. Customer service, field representatives and other customer-facing employees (and third parties) are your first responders. Are they trained to address potential issues in ways that protect your brand and reputation? Do you have a plan to quickly activate them in the event of a breach?

- **One team, one fight.** Keeping your corporate network secure is a team sport, and one that requires active collaboration across your company, including IT, Legal, Risk Management, Human Resources and Corporate Communications. Not only do these groups need to work together if your network is compromised, they also need to align around everything from employee engagement programs to network vulnerability tests.
- **Keep it simple.** While detailed policies and procedures are important, boil it down for your employees. In 2009, GM distilled a 10-page dress code into two words: dress appropriately. How can you simplify your messages and policies?
- **Make it shareable.** Provide employees with tips they can share with family and friends. And ask them to share their tips and stories through video, blog posts and other employee communications channels.
- **Plan, drill, repeat.** While it's impossible to predict what the next threat will be, thinking through the hypotheticals will benefit your organization and your customers in the end. Revisit your crisis plan to keep your response acumen sharp, and refresh it frequently to ensure your plan is relevant in today's dynamic, digital business environment. Enlist the services of third-party consultants to help you think through threats you may not consider on your own.

Offer Protection

With half of Americans potentially at risk from the Equifax breach, consider helping your employees understand the issues and risks they may face. The Federal Trade Commission website provides information you can share. Given the potential long-term threats posed by the breach, consider offering employees reimbursement or discounts on credit monitoring or identity-theft protection services.

FLEISHMANHILLARD AS YOUR PARTNER

FleishmanHillard has helped leading companies develop strategic and effective programs to educate and engage employees in protecting company data and complying with policies. Our global crisis and issues management team provides a full range of services to help companies prepare for and respond to cyber issues and attacks. We've also worked with technology leaders to articulate a business case for funding security enhancements. For more information about these programs or our Authenticity Gap research, contact one of our counselors:

Kristin Hollins
Corporate Reputation Lead,
Americas
415-318-4107

Chris Nelson
Crisis Management Lead,
Americas
212-453-2238

Josh Rogers
Employee Engagement and
Change Communications,
St. Louis
314-982-7743

LEARN MORE
For more information about FleishmanHillard's reputation management expertise,
please visit *fleishmanhillard.com/reputation-management.*