Email   Save

What Is Red Teaming?

Marketers have a significant role to play with internal teams designed to fortify defenses against cybersecurity threats

By Chuck Kapelke   May 31, 2024   5-minute read

Joey Guidone/theispot.com

Rate This Content
★★★★★

Save to MyANA 🗀 | Share ✉ f 𝕏 in

It makes sense that marketers are getting more spooked about cybersecurity. The average cost of a data breach reached an all-time high of $4.45 million in 2023, according to IBM Security's 2023 "Cost of a Data Breach Report," which is based on a study of 553 organizations impacted by a data breach between March 2022 and March 2023. Loss of business — including reputational damage — accounted for nearly 30 percent of those costs.

A separate survey of 1,000 U.S. consumers conducted by security firm Vercara found that 75 percent of consumers say they would be ready to sever ties with a brand in the aftermath of any cybersecurity issue.

Despite the growing risk, marketers have not traditionally been involved in shoring up their firms' digital walls. But that's going to have to change, because persuasion and behavioral change — two cogs in marketers' wheelhouse — are getting to be major aspects of the defense.

A growing number of companies are creating red teams, or in-house groups that test the company's cybersecurity by applying an adversarial lens. As these groups proliferate, marketers may be recruited to assist in the effort.

Most successful cyberattacks are the result of human error, whether it's someone sharing a password or clicking a link that downloads malware. In fact, 90 percent of data breaches this year will include a "human element," per Forrester. By collaborating with their cybersecurity teams, marketers can help

Find What You're Looking For

Our member-exclusive online content portfolio of best practices, case studies, and research connects you to the knowledge and resources you need to become a smarter, more capable marketer.

Search our extensive collection:

Search

Learn More About the ANA

As the leading organization for client side marketers, ANA collectively elevates the art and science of marketing by helping to build stronger brands and drive greater revenue through smarter marketing decisions.

Learn More

educate their companies' employees.

"Security people tend to be engineers who are technically orientated and don't have communication skills," says Kai Roer, CEO and founder of Praxis Security Labs and co-author of *The Security Culture Playbook*. "In order to build resilient organizations and make employees do the right behaviors, they need to work together with people who know communication — and those are marketing people."

How to Frame the Issue

A company's cybersecurity often hinges on whether its employees understand how their actions online may make them vulnerable to attack. Unfortunately, most companies' efforts to boost awareness are limited to one-and-done training, rather than sustained cultural change.

"In most organizations, people think cybersecurity is the cyber team's problem," says Dr. Keri Pearlson, executive director of the research consortium Cybersecurity at MIT Sloan (CAMS). "They don't stop and think that every single person has a responsibility."

Marketers can lend a hand by developing internal awareness campaigns that get everyone on board. Pearlson cites Liberty Mutual, which reframed the issue from being "cyber secure," which was poorly understood among employees, to fostering a "culture of data protection," which was more in sync with the company's overall mission.

The insurer launched an internal communications

campaign revolving around a branded theme to make every employee a "Responsible Defender." The effort detailed specific practices that made sense to employees in the context of their work and delivered engaging and fun cybersecurity messages through campaigns designed to develop attitudes and beliefs about the importance of proper cyber behaviors. "All of a sudden, everybody knew what they had to do: they had to protect the data," Pearlson says. "And that changed the culture."
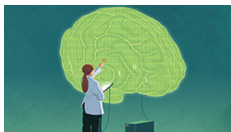
When companies look to raise awareness internally about cybersecurity, it's important that the messaging targets segments of employee groups based on their role and risk profile. "An accountant who opens emails all day is very different from someone who works in a factory," Roer says. "You need to make sure that you adapt the messaging to their needs, not your own."

It's also important to encourage behaviors that align with people's incentives. "If you're told to do something, you may feel that your freedom is being restricted," says Joe Giddens, marketing director at human risk management platform CybSafe. "The most effective

campaigns talk to people in the way that they want to be communicated with. They inspire, rather than direct or wag fingers. Understand your target audience and what incentivizes them, then communicate with them on that level."

Marketers can also help their security teams establish KPIs to measure the success of their awareness-building efforts, ensuring they are focused not on how many people watched a training video, but tangible metrics such as how people react when sent test phishing emails. "In security, the end goal we want is changed behavior," Roer says.

Key takeaway: Marketing tools can nudge employees toward improved cyber practices and feeling like they are vested. "Helping security teams come up with ideas to promote cybersecurity, such as artwork promoting good cybersecurity behaviors, newsletters, or other ways to reach the audience are a great assistance to security teams," says Erich Kron, security awareness advocate at IT security company KnowBe4.

Red Alert

The growing practice of "red teaming" is seeping into the marketing function, as CMOs and marketers can help inform these teams' work by identifying how marketing channels could be manipulated by attackers.

"Some marketing teams work in tandem with security teams in hiring brand protection services that monitor their online channels — for example, to see if there is misinformation being spread around

the company, or fake social media accounts or websites," says Mitchell Schneider, director-analyst at Gartner.

Russell Craig, a cyber and security culture expert at PA Consulting, whose clients include OneSavings Bank and Unilever, adds that marketers can help red teams craft "plausible technical and social cyberattacks."

"The marketing team[s] are experts in customer-journey mapping, so they can highlight potential vulnerabilities, and often have an excellent understanding of how to communicate effectively to their colleagues, thus providing information for mock social engineering attacks," Craig says.

Marketers can also help ensure that the red team's work is taken seriously among upper management. "These mock attacks and exercises are often a very effective way of getting the board's attention," Craig says. "Even when you know it is an exercise, it is very unsettling to see a video naming your organization as being in the news for a cyberattack."

Messaging the outcomes of a red team's efforts via reports or presentations marks another opportunity for marketers to get involved and add value.

"Marketing can help craft messaging in such a way that it does not come across as adversarial when exposing vulnerabilities within the organization," Kron says. "This is especially critical, since often red team exercises involve social engineering tactics that could leave people feeling a sense of shame or

failure, when in reality the point of these exercises is not to make people feel bad but rather to find ways for improvement."

The Front Line

Marketers can also align with red teams by helping employees prepare for the crisis communication plan they would need to execute in the event of a cyberattack or data breach.

"Should an attack occur, marketing and PR will be on the front line, needing to respond within minutes to the inevitable social media barrage, usually before the facts are properly known," Craig says. "Hence, the role of the marketing team in planning, exercising, and enacting this in the event of a crisis is vital."

Key takeaway: Working in collaboration with the security team, marketers should understand what their organizations' vulnerabilities are — and how they can best prepare to minimize the brand damage stemming from a breach. "When a company has a breach, your messaging is super important," Pearlson says. "You don't want to wait until you have a breach, with all the panic and urgency. You want to be able to fine-tune a message that's already been thought through when heads were more level."

Save to MyANA 🗂 | Share ✉ 🅕 𝕏 🔗

Chuck Kapelke

Chuck Kapelke has more than 20 years

of experience as a communications professional. His writing has appeared in publications such as Fortune, Boston Magazine, Continental Inflight, and Rolling Stone. He has also written articles and produced videos for a wide range of companies.

[Read more](#).

Leave a comment

Start typing your message here. Limit is 5000 characters....

SUBMIT

PRIVACY POLICY   TERMS OF USE   ABOUT   PRESS ROOM   CONTACT US   CAREERS

ANA LOGOS   YOUR AD CHOICES   COOKIE SETTINGS

Learn About Membership