MIS Quarterly Executive

Volume 21 | Issue 2 Article 6

June 2022

How Verizon Media Built a Cybersecurity Culture

Keri Pearlson

Josh Schwartz

Sean Sposito

Masha Arbisman

MIS Quarterly Executive

How Verizon Media Built a Cybersecurity Culture

To successfully improve the cybersecurity culture, Verizon Media's security organization, known as "The Paranoids," knew it had to engage every employee and measure progress. It established the Proactive Engagement (PE) Group to lead the culture change project. The group's initial focus on reducing employees' credential capture achieved significant results. The capture rate in phishing simulations was halved, the number of accurate simulated phishing reports from employees doubled and usage of the corporate password manager tripled.[1,2]

Keri Pearlson
MIT Sloan School of Management (U.S.)

Josh Schwartz
Verizon Media [now Yahoo, Inc.] (U.S.)

Sean Sposito
Verizon Media [now Yahoo, Inc.] (U.S.)

Masha Arbisman
Robinhood Financial, LLC (U.S.)

The Need for a Cybersecurity Culture

People are the weakest link in an organization's cybersecurity defenses. Verizon's *2021 Data Breach Investigations Report (DBIR)*[3] stated that "85% of breaches involved a human element and 61% of breaches involved credentials [e.g., username and password]." Verizon found that managers have a hard time keeping their organizations secure. Their challenge is to find ways to motivate employees to perform in ways that ensure company assets are secure, networks remain uncompromised and staff members are not fooled by phishing emails and fake websites. A key element of addressing this challenge is to instill a cybersecurity culture—i.e., a set of values, attitudes and beliefs that drive secure cybersecurity behaviors.[4]

Most employees in an organization want to behave in ways that do not compromise security, but often they do not prioritize cybersecurity, in part because the organization does not let them know it is a priority. Moreover, without careful planning, activities to keep the organization secure might actually hinder employee productivity. Employees are simply trying to get their regular jobs done in an efficient manner, and because cybersecurity security is not prioritized as a primary job objective, secure behaviors get left out or forgotten. Organizational

1 Erran Carmel is the accepting senior editor for this article.

2 The authors thank the leadership at Verizon Media for supporting this research. Since the research for this case study was carried out, Verizon has divested the group that included the security team described in this article. The new company is Yahoo, Inc. This research was supported, in part, by funds from the members of the Cybersecurity at MIT Sloan (CAMS) consortium.

3 *2021 Data Breach Investigations Report (DBIR)*, Verizon, 2021, available at https://enterprise.verizon.com/resources/reports/2021-data-breach-investigations-report.pdf.

4 Cybersecurity behaviors are actions and habits within a specific context of a situation, environment or stimulus that can lead to a cyberbreach.

DOI: 10.17705/2msqe.00064

leaders therefore need to develop specifically targeted managerial mechanisms (i.e., levers or activities that a manager can employ directly to influence values, attitudes and beliefs within an organization) to build a cybersecurity culture.

Most organizations provide cybersecurity awareness training to teach their employees what to do but, as shown by the Verizon report, human errors still occur and these errors are a significant cause of breaches. Many technical and business leaders, however, fail to recognize that training and awareness programs are not sufficient. Our research found that those companies with the strongest defenses build a culture of cybersecurity using mechanisms that go beyond training and awareness campaigns to change the values, attitudes and beliefs of employees so they are motivated to do things that keep the organization secure.[5]

In this article, we describe the mechanisms Verizon Media (now called Yahoo, Inc.) used to instill a cybersecurity culture. Verizon Media's security organization, known as "The Paranoids," not only built a cybersecurity culture for the entire Verizon Media organization, but used metrics to track progress, motivate employees and demonstrate success. Employees responded positively to the behavioral changes managers sought. The Verizon Media case illustrates how The Paranoids changed the behaviors of employees by changing their values and attitudes to cybersecurity. The managerial mechanisms used by The Paranoids to create and reinforce a cybersecurity culture can be adopted by other organizations seeking to strengthen their cybersecurity defenses.

Understanding Organizational Cybersecurity Culture

Cybersecurity culture is one aspect of organizational culture. The concept of organizational culture was first introduced by British sociologist Elliott Jaques in his 1952 book *The Changing Culture of a Factory*.[6] Jaques suggests that culture, in the context of the factories he studied, was the "customary and traditional way of thinking and of doing things, which is shared to a greater or lesser degree by all its members." More recent scholars have defined culture as "a set of shared mental assumptions that guide interpretation and action in organizations by defining appropriate behavior for various situations,"[7] and Cooke and Rousseau suggest that organizational culture is a set of beliefs and values that guide thinking and behaviors.[8] Edgar Schein expanded the notion of organizational culture in his well-known work *Organizational Culture and Leadership*,[9] where he suggested that culture refers to the values and beliefs of an organization that come from the principles, ideologies and policies followed by people in the organization.

Huang and Pearlson built on these organizational culture concepts to explain the cybersecurity behaviors of individuals in an organization.[10] Their definition of cybersecurity culture is "the beliefs, values, and attitudes that drive employee behaviors to protect and defend the organization from cyber-attacks." According to Huang and Pearlson's cybersecurity model, managerial actions and mechanisms such as traditional training classes and awareness programs do not directly change behavior. Instead, these activities change attitudes, beliefs and values, which in turn change behaviors. The Huang-Pearlson cybersecurity model is described in more detail in the Appendix.

5 Huang, K. and Pearlson, K. "For What Technology Can't Fix: Building a Model of Organizational Cybersecurity Culture," *Proceedings of 52nd Hawaii International Conference on System Sciences*, January 2019.

6 Jaques, E. *The Changing Culture of a Factory*, Tavistock Publications Limited, 1951, p. 251. For more on the history of organizational culture in organization theory, see Hatch, M. J. and Cunliffe, A. L. *Organization Theory: Modern, Symbolic, and Postmodern Perspectives* (2 ed.), Oxford University Press, 2013, p. 161.

7 Ravasi, D. and Schultz, M. "Responding to Organizational Identity Threats: Exploring the Role of Organizational Culture," *Academy of Management Journal* (49:3), June 2006, pp. 433-458.

8 Cooke, R. A, and Rousseau, D. M. "Behavioral Norms and Expectations: A Quantitative Approach to the Assessment of Organizational Culture," *Group and Organizational Studies* (13:3), September 1988, pp. 245-273.

9 Schein, E. H. *Organizational Culture and Leadership*, Jossey-Bass, 2004.

10 Huang, K. and Pearlson, K., op. cit., January 2019.

Table 1: Context of Verizon Media's Cybersecurity Behavioral Change Initiative

Date initiative began	2018
Period of evaluation covered in this article	Two years (2018-2020)
Date of this case study	2021
Approximate number of employees at Verizon Media during this period	20,000 employees and contractors
Number of offices/locations of Verizon Media	32
Brands owned by Verizon Media	Yahoo, AOL, RYOT Studio and TechCrunch

Overview of Verizon Media and Its Cybersecurity Behavioral Change Initiative

The case study described below documents the cybersecurity behavioral change activities that took place at Verizon Media over a two-year period, from the summer of 2018 to the summer of 2020. It involved all offices and locations of Verizon Media, which had nearly 20,000 full-time employees and contractors working across dozens of offices worldwide (see Table 1).

In 2020, Verizon Media was a division of Verizon and a sister company of Verizon Business. The Verizon Media website described its business as "combining the power of content, scale and data to drive results for advertisers, publishers and partners." Verizon Media was originally founded in 2017 as Oath Inc., which merged with Verizon in 2019. Verizon Media included many brands such as Yahoo, AOL, RYOT Studios and TechCrunch.

The cybersecurity behavioral change initiative was led by the Proactive Engagement Group, which was established as part of Verizon Media's security team ("The Paranoids"). This name originated in the late 1990s at a time when Yahoo was a separate entity, and was one way the team branded itself within the organization and made its work more accessible to non-cybersecurity colleagues.[11] The Paranoids, and particularly the Proactive Engagement Group, were responsible for all cybersecurity program objectives, activities and guidance, as well as the tools and security operations for Verizon Media.

Role and Actions of Verizon Media's Proactive Engagement Group

Realizing that a cybersecurity culture was fundamental to the success of Verizon Media's mission, the Chief Information Security Officer, in conjunction with a newly hired Director of Offensive testing, established a Proactive Engagement (PE) Group as part of The Paranoids. This group was responsible for security policy and tools, and for instilling the behaviors necessary for a cybersecurity culture. (Note that "PE Group" and "The Paranoids" are used interchangeably in this case study.) The PE Group created shared values, attitudes and beliefs among employees that strengthened the company's security and drove cybersecurity behavior. There were three teams within this group: 1) the Offensive Engineering (Red) Team, which evaluated systems, services, processes and people to discover systemic weaknesses; 2) the Security Education Team, which institutionalized the lessons from the Red Team team's findings and disseminated those learnings to all employees through mandated training; and 3) the Behavioral Engineering Team, which took a data-driven approach to create baselines and subsequently influence security behaviors by emphasizing employee-adoption of cybersecurity values.

The PE Group used managerial mechanisms to encourage cybersecurity values among employees and believed that creating and nurturing these values merited management attention and action. The group identified

11 The name "The Paranoids" was chosen because the team was charged with keeping Verizon Media secure from all types of security vulnerabilities, and to do that it had to be both proactive and responsive to any cyberthreats. Sometimes that meant anticipating issues that might occur and taking action before a breach happened. To some, that is very close to the definition of paranoid.

specific activities that encouraged cybersecure values and subsequent behaviors. The first were "kill-chain-breaking" actions based on realistic cyberattacks.[12] The purpose of these actions was to stop any processes that might lead to a breach. Next, the group implemented technology solutions for those actions and created proactive defenses for all employees to adopt. The technology solutions were disseminated through awareness and "nudge" communications,[13] simulations and training.

By the summer of 2018, the PE Group had recognized that driving behavior change was more complex than simply providing training classes or launching an awareness campaign. At that time, the standard way to teach employees about desired security behaviors was to appoint a Security Awareness Team, which then highlighted every human error that might lead to data loss and "taught" employees what to do differently. However, this approach hardly ever resulted in lasting, long-term behavior change. Recognizing that awareness was useless without actionable advice and practice, the PE Group adopted two ideas from the field of psychology: the "G.I. Joe Fallacy,"[14] which suggests that knowing about a bias or tendency is not enough to conquer it; and Vince Lombardi's advice[15] that "perfect practice makes perfect." By adopting these ideas, the PE Group moved its focus away from security training and awareness campaigns to influencing corporate culture change. The group's approach was based on an education-practice-reinforcement process.

12 The cyber kill-chain framework was developed by Lockheed Martin to identify and prevent cyberintrusions. The cyber kill-chain is the set of activities that malicious actors must successfully complete to achieve a breach. The term was adopted by the cybersecurity community from the military's approach to and structure of an attack. For more information, see Tunggai, A. T. *What Is the Cyber Kill Chain and How to Use It Effectively*, December 16, 2021, available at https://www.upguard.com/blog/cyber-kill-chain.

13 A form of communication that reliably influences choice-architecture (see footnote 19) and alters individual behavior without prohibiting other options/individual choices.

14 The "GI Joe Fallacy" gets its name from a cartoon character (GI Joe) developed in the 1980s by a U.S. Army cartoonist. GI Joe was supposed to be a typical American soldier who would end each film by saying "knowing is half the battle," and the film would conclude with the message "now you know." The GI Joe Fallacy subsequently became a cognitive psychology term that was shorthand for the industry understanding that knowing is *not*, in fact, half the battle.

15 Vince Lombardi was a famous American football head coach during the 1960s. He is widely regarded as one of the greatest coaches in American sports, and often his advice to his teams is used in business to motivate and lead teams.

Distinguishing Between Actions, Habits and Behaviors

The first step for the PE Group was to distinguish between actions, habits and behaviors. This was necessary to create the shared values, or cybersecurity culture, that would ultimately drive desired cybersecurity behaviors. An *action* is something a person does to completion. For instance, Verizon Media employees were required to take an annual security training course. Completing the course was an action. A *habit* is a shortcut made in the human brain for repeatable actions. Logging into a password manager regularly to access corporate assets and secure passwords is an example of a habit. The PE Group wanted employees to rely on a password manager so that passwords could be complex and changed as often as appropriate. For example, a password manager would be able to handle a non-human-friendly password, such as "Rcek!2mr4h7F%3&ZExxR^" as easily as human-friendly passwords, such as "MyDogHas10Lives!2020." Creating the habit of using the password manager was something the group wanted to encourage.

Behaviors are the combination of actions and habits within the context of a situation, environment or stimulus. In the context of passwords, an example of security behavior is not simply "use a password manager" but "when creating or updating accounts, generate and store credentials using a password manager."

To change behavior, The Paranoids first created behavioral goals by identifying the specific context and desired actions. To create a behavioral goal, the PE Group considered the question: in which specific context do we want a specific cohort (or person) to do a specific action? One behavioral goal described by a manager was "When generating a new single sign-on (SSO) password, we want all employees to generate and store the password within our corporate approved password manager." The behavioral goals became the basis for measuring awareness of and attitudes to the cybersecurity culture.

Defining, Measuring and Improving Cybersecurity Behavior Goals

To change the organization's cybersecurity behavior, The PE Group used a three-step process for informing decisions on how to improve

the security behaviors of employees: defining, measuring and acting.

Step 1: Defining the Desired Behavioral Goal. A clear goal for each desired behavior was a prerequisite for any measurable change to occur. The PE Group deliberately avoided defining goals framed in terms of what it called "impossible advice"—i.e., security guidance that required employees to make a qualitative judgment. Examples of impossible advice are "don't click insecure links" or "always use a secure password," which would require employees to make subjective judgments about what was secure. This type of guidance was an inadequate goal for desired behavior because it did not contain enough information for employees to consistently make the right decision.

Step 2: Identifying Appropriate Measures and Creating Baselines. Baselines enabled The Paranoids to show improvement in the organization's goal of more secure behaviors over time. For example, one behavior goal was to reduce the success of phishing attacks. Instead of focusing on measures training employees to not click links (telling employees to not click on links was viewed as impossible advice), the PE Group measured the likelihood of employees entering their credentials into a fake SSO page. Combining this data with logs from the phishing simulation provider and HR data allowed the group to identify which individual employees (as well as employee groups and roles) were most at risk from credential capture phishing attacks. This information provided a clear measure and baseline.

Step 3: Taking Action to Affect the Measured Behavior, Adjusting those Actions Over Time and Repeating the Process. In Step 3, the PE Group designed behavior-changing activities to impact the baselines, and launched new activities to continuously improve behaviors. Equally important to the success of driving appropriate behaviors was learning from the results of these activities, adjusting the activities and creating new activities to continually improve to reach the behavioral goals. For example, to reduce phishing successes, the PE Group engaged in a range of activities, including technology fixes,[16] cascading communications,[17] passive and active competitions,[18] communication nudges and just-in-time training. Progress toward the behavioral goal of continually pushing the credential capture rate down and increasing the rate of reporting phishing attacks was made with the addition of each new activity.

The PE Group used three types of behavior-changing activities: *choice-architecture, communication* and *incentivization*. It found that the most successful change management plans required all three.

Choice-architecture[19] referred to the practice of influencing an individual's choice by setting defaults, framing options in a way that made sense to users and other activities designed into the information systems architecture. Mechanisms such as default options that appropriately update technology and preset design choices made it as easy as possible for employees to adopt the "right" behavior. For instance, the PE Group preinstalled a corporate password manager browser extension and desktop application on every managed device (desktop, laptop, mobile phone etc.), making it the default choice for employees. In this way, the choice-architecture reduced the number of steps and time required for employees to follow security guidance.

The PE Group reinforced a set of security beliefs and values for the organization through *communication* channels such as just-in-time training, tutorials and automated reminders sent over email or the corporate messaging system. It used three categories of communication to inform and "nudge" users to change their behaviors:

1. Top-down passive competition: monthly emails from senior executives, together with universally accessible dashboards, enabled executives to compare their direct reports' activities with teams—for

16 At Verizon Media, "technology fixes" referred to the installation, update or change of technology used to force specific choice-architectures (defined in footnote 19).

17 The passing of information from top executives to managers to employees.

18 The active competition managerial mechanism is when a corporate-wide competition to highlight and reward top performers is announced; passive competition is a managerial mechanism created by default when individual data is grouped by performance and made publicly available to the organization.

19 A choice-architecture is a behavioral economics approach to design in which choices are presented to consumers in a way that impacts their decision-making.

Figure 1: Password Manager Knight Logo

example, the adoption rate of using the password manager.

2. Manager-to-manager peer workshops: this group-level communication included, for example, cyberthreat briefings at team meetings.
3. Bottom-up nudging and active competition: These activities were aimed at the individual level. Emails and corporate communications frequently used positive messages and social proof[20] to "nudge" employees to change their behaviors.

The *incentivization* activities encouraged a change in the attitudes and ultimately the behaviors of Verizon Media's employees. Examples included callouts, such as identifying employees who were "doing the right thing" and rewarding them with gifts, badges or titles, naughty/nice lists built into team managers' dashboards (lists of employees who had exemplary behavior were on the "nice" list and those who were below average were on the "naughty" list) and self-progress dashboards accessible to individual employees. Examples of incentives that worked particularly well were prizes of Paranoid-branded merchandise (which could be earned by the completion of behaviors meeting certain standards) and fun titles awarded to those who entered competitions (such as "[Password Manager] Knighthood"). "Password Knights" were given a laptop sticker with the logo shown in Figure 1.

Making Measured Behaviors Transparent Through Dashboards

Measuring behaviors was fundamental to the success of the PE Group. Behaviors were measured and displayed on dashboards used by managers to track progress and by the PE Group to calibrate success. The measures used a combination of data:

- HR data (for example, employee names, roles and manager)
- Information from vendor systems (for instance, usage of the password manager or results of phishing simulations)
- Data from the security team (for example, tickets relating to phishing reporting or security incidents maintained by the security operations center)
- Data from marketing communications used to nudge employees (such as messages sent, number of messages opened, and links accessed from the communications).

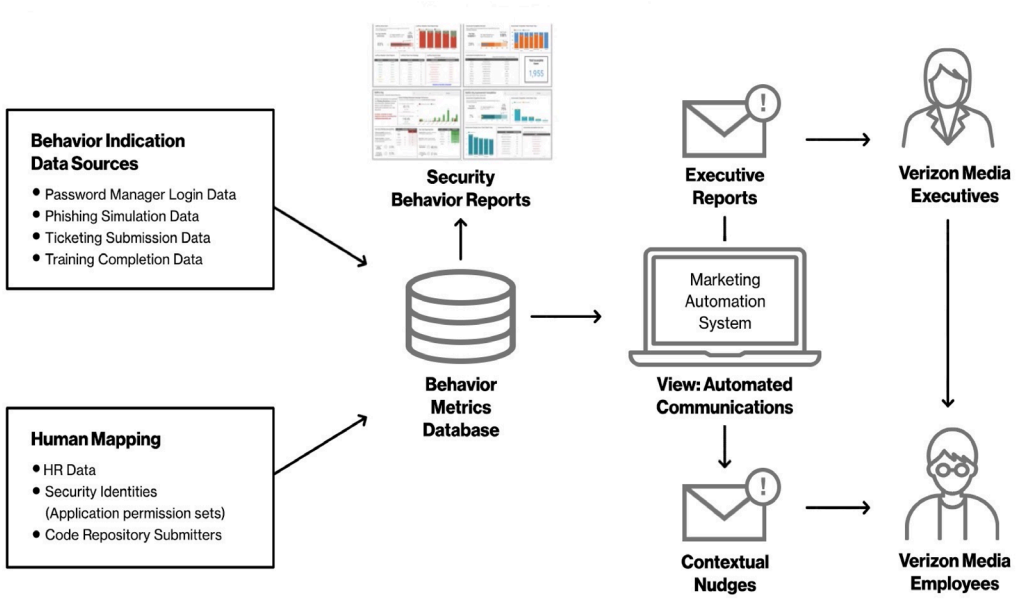
These data sources formed the basis of the behavior measurement and communications system built by Verizon Media's PE Group (see Figure 2).

The system provided three primary behavior metrics:

- Accuracy of employee reporting: This metric was constructed from the percentage of both actual and simulated phishing emails or security incidents

20 Social proof is a psychological and social phenomenon where individuals mold their opinion/actions to match the greater population. It stems from the need to fit in and feel accepted by the larger group. Social proof is used to influence the way individuals act and think by sharing the actions and beliefs of their group. Examples include displaying positive customer reviews on commerce websites, sharing testimonials from those in positions of authority or influence, posting the status of friendly competitions and sharing the number of followers/likes for social profiles and posts.

Figure 2: Verizon Media's Behavior Measurement and Communications System



reported to the Security Operations Center, rather than false positives resulting from, for instance, a "phishy looking" internal communications message.

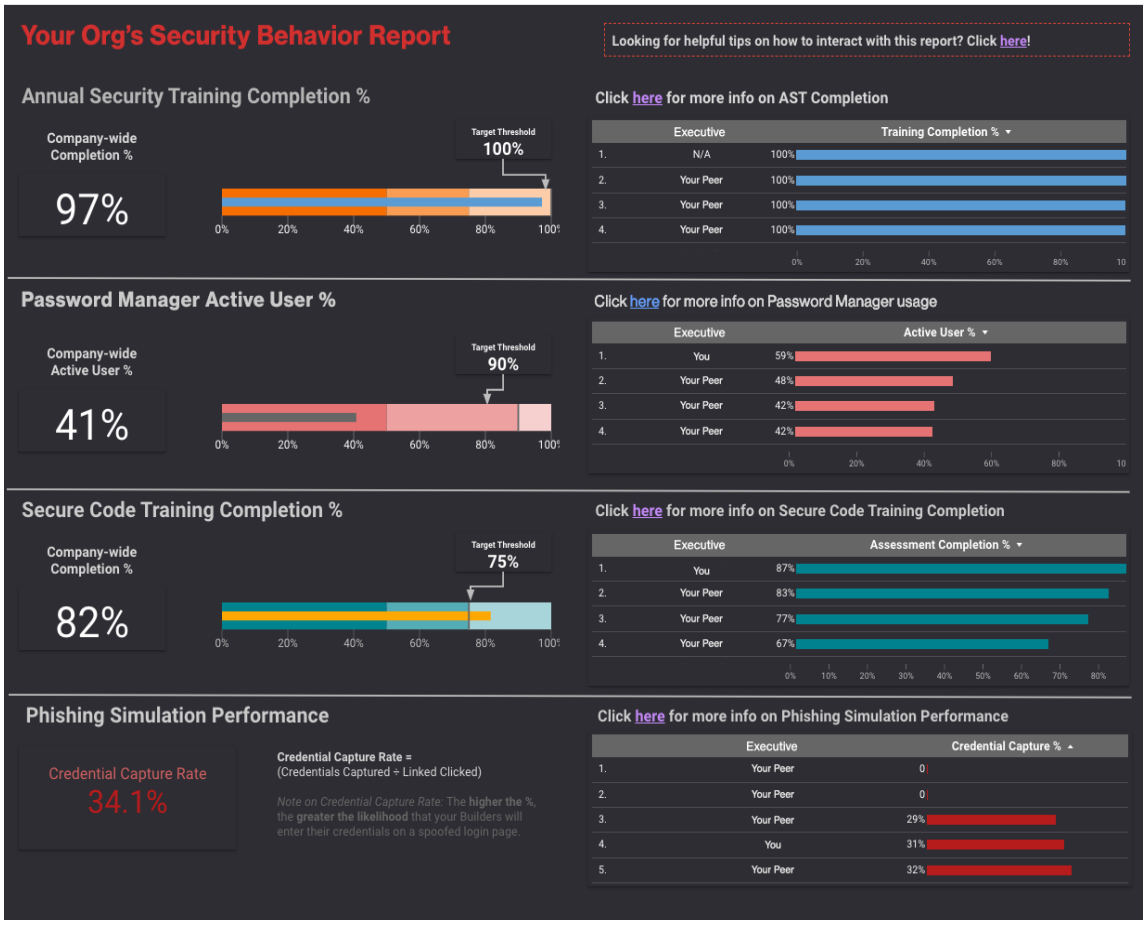
- Increasing usage of tools: Measured an individual's active usage of the security-related tools made available to employees, such as the company's password manager, VPN, reporting shortcut button, security messenger bot, etc.
- Engagement of employee communities susceptible to cyberattacks: The engagement metrics of, for example, newsroom reporters and senior executives included attendance at optional events (such as cybersecurity hygiene workshops aimed at protecting highly visible employees from doxing,[21] impersonation and personal account takeover) and completion of both mandatory and additional training. Engagement metrics also included page views, button interactions, downloaded documents, video completions, survey responses and other link clicks.

These metrics were shared with Verizon Media managers on dashboards that compared individual, team and organization performance. The dashboards provided a way to track progress, compare groups across the organization and demonstrate the success of the PE Group's initiative. Managers used the dashboard information to help their teams become more secure. For example, metrics about adoption of the password manager, security training completion and susceptibility to phishing simulations identified specific areas where managers' actions could have an impact on security behaviors. Other dashboard data, such as credential capture metrics, provided a useful way to understand the extent of possible vulnerabilities that might occur should someone's credentials be stolen and used inappropriately. An example of a manager's dashboard is shown in Figure 3.

Dashboards were also made available to individual employees, allowing them to benchmark their personal security behaviors against their peers (a typical dashboard is shown

21 Derived from the term "dropping docs," doxing is the act of publicly revealing previously private personal information about an individual or organization, usually via the internet.

Figure 3: Example of a Manager's Dashboard



This dashboard enables managers to review risks and understand their direct reports' cybersecurity behavior

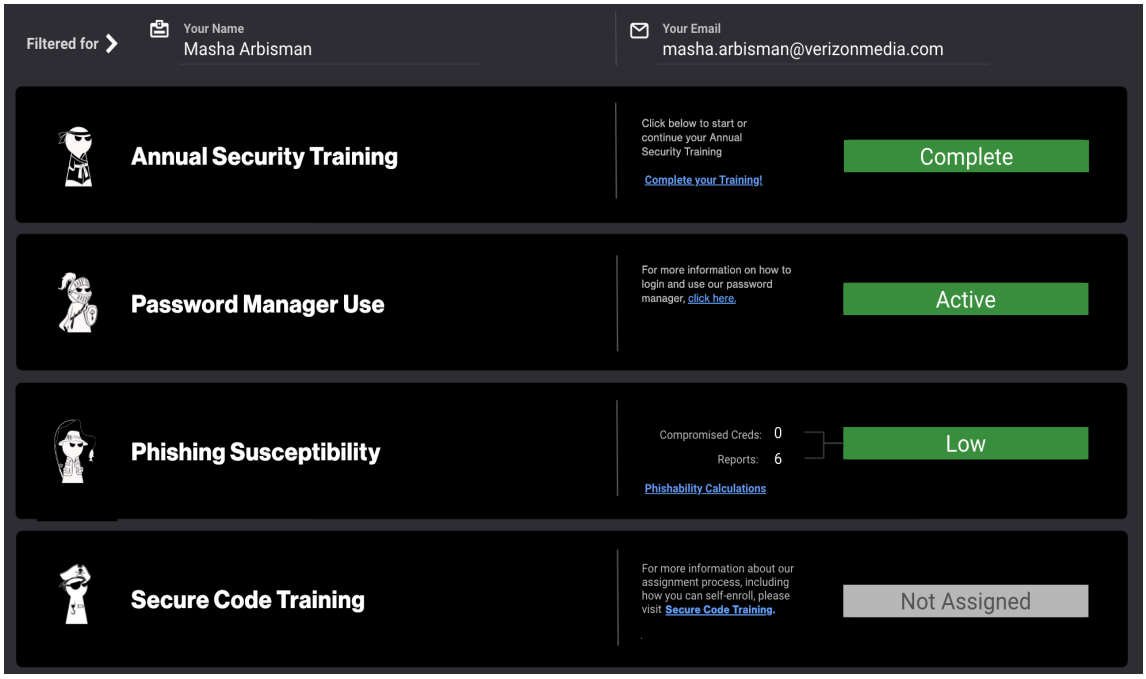
in Figure 4). These dashboards gave employees a visual picture of their activity completion and motivated accountability.

Both the manager and individual dashboards provided:

- Behavioral indicators: Discrete, measurable and attributable metrics that showed the state of the desired security behavior
- Human mapping: Data mapped to individual employees within their contextual organization structure, such as leaders, teams or products
- View mechanism: The dashboards provided both the PE Group and the target population with a visual way to interact with the output of the behavior measurement system.

Action measurements were an important component of the PE Group's success. Without such measures, it would have been difficult for the group to holistically understand cybersecurity behaviors. Key behavioral metrics enabled the group to test and evaluate experiments in changing cybersecurity behavior and thus determine which managerial mechanisms had the biggest impact on employees. For example, the dashboard in Figure 4 shows that Masha Arbisman had completed the annual security training, was an active password manager user and had a low susceptibility in phishing simulations to provide credentials. From this

Figure 4: Example of an Individual's Dashboard



This dashboard enables individual employees to review their cybersecurity activity status

information, the PE Group hypothesized that completing the annual security training had taught Masha to report suspicious emails and that actively using a password manager had shown her that she could personally prevent credential capture, resulting in a low phishing susceptibility score. The group might also have hypothesized that training and knowledge of tools had changed Masha's attitude about the importance of her personally adopting these behaviors to help keep the organization more secure.

By evaluating how the metrics included in managers' dashboards (see Figure 3) change over time, the PE Group could determine which choice-architectures, communication strategies and incentivization programs have been most influential in changing values, attitudes and beliefs about cybersecurity, and ultimately driving more secure behaviors.

Enabling Change Management Requires Radical Transparency

The Paranoids' management felt that security awareness activities were a key component of behavioral change but, by themselves, were not sufficient to effect change. "Awareness activities alone do not change values, attitudes and beliefs necessary to create a culture of cybersecurity," one manager shared, "but awareness is an important tool of transparency. And we want to be radically transparent with our security goals." Awareness campaigns were used to answer the larger question of why someone should change their behaviors to support a greater good and to motivate change by transparently and proactively answering these questions:

- What's changing?
- Why is it changing?
- Who does this change affect?
- What does this change demand of those affected?

These questions were answered for each behavioral goal, and responses were tailored to the specific work groups and job profiles of targeted employees, thus ensuring that messages were personal and relevant to everyone in a larger group. The dashboards provided transparency. By making team performance data available to business leaders, everyone knew

how they were doing compared to others, and that drove competitive instincts to be the best. Sanctions or negative reinforcements were not needed.

Business leaders from around the company who bought into the concept of radical transparency and understood why changes were happening, were labeled "trusted messengers" and celebrated. This was a strategic activity of the PE Group designed to support and get the support of business leaders.

Providing a Feedback Loop to Ensure Continuous Improvement

The final step in the PE Group's process was a feedback loop, which provided employees with a way to share their experiences and thoughts. Feedback was collected on how technologies were working, what disruptions to daily activities were occurring, and how new policies impacted everyday tasks and challenges.

The group reviewed and responded to every piece of feedback, and created or updated customized security controls based on the feedback. Employees responded positively because the feedback loop facilitated the implementation of secure practices with little disruption to employees' regular work tasks.

In summary, managers of the PE Group credited the three components of the change management process—early communication of changes, radical transparency and the feedback loop—as key success factors that reduced any potential pushback or concerns from employees. Treating employees as respected individuals who could understand the how and why of the behavioral change initiative encouraged acceptance rather than defiance or pushback. As a result, Verizon Media successfully created a culture of cybersecurity with impactful behavioral changes that contributed to a more secure workforce.

Successful Outcomes of the Proactive Engagement Group's Cybersecurity Culture Initiative

Verizon Media's PE Group was successful in using its three-step process to affect cybersecurity behavior change, as illustrated by its efforts to reduce security vulnerabilities by focusing on credential capture from both phishing and spoofed websites. Phishing simulations had shown there was potentially a high rate of account takeover. The group had initially focused on providing prescriptive advice about actions that break kill chains. But after a series of simulated offensive operations (run by the Red Team) had shown the potential scope for capturing credentials, the PE Group questioned the usefulness of the then-standard measure of the rate at which employees clicked links within phishing simulations. Instead, the group decided to base its efforts to reduce vulnerabilities on a different measure—credential capture—and switched its focus to changing behaviors that directly led to credential capture.

This change of focus led to a clear behavioral goal. The PE Group took the view that asking employees "to determine if a link was suspicious and report it" was impossible advice to follow correctly. It was too general and left the decision of defining "suspicious" up to the individual and did not give enough guidance on what should be reported. Instead, the group defined a new behavioral goal for employees: "When your corporate account receives an email sending you to a website asking you to enter credentials, we want you to report the email to our defense team and not enter your credentials." This goal was specific and actionable for all employees.

Identified Three Key Measures and their Baselines

To achieve this behavioral goal, the PE Group defined three key measures and then designed new managerial mechanisms to reduce the rate of credential capture:

1. Phishing susceptibility rate: Number of employees who entered credentials and did not report a phishing email divided by the total number of phishing simulation emails sent. This measured how many employees entered credentials on a page they went to from a phishing simulation.
2. Credential capture rate: Number of employees who entered credentials (and did not report) divided by the number of employees who both opened the phishing simulation and landed on the fake login

page. This measured how many employees entered credentials on a fake login page.

3. Reporting rate: Number of employees who reported the phishing simulation divided by the number of total simulation emails sent. This measured reporting of phishing emails, which indicated employee ability to identify phishing.

Together, these measures enabled the PE Group to track progress and ultimately demonstrated the success of the cybersecurity culture initiative.

To obtain a baseline for the credential capture rate, the PE Group used data from phishing simulations. It calculated the rate to be 50% in 2018, meaning that one out of every two employees' credentials were being captured when they both opened a test email and clicked a hyperlink that took them to a fake login page. Only 10% were accurately reporting the original simulated phishing email, and the simulations measured the phishing susceptibility rate for the company at 14%.

Introduced New Managerial Mechanisms

Having defined the behavioral goals and key measures, the group then implemented new managerial mechanisms to reduce the rate at which employees divulged their credentials and to change cybersecurity behaviors. This would not have been possible without the involvement of the Security Operations team (the Blue Team), which had noted that real-world credential capture phishing attempts were a major vulnerability for Verizon Media and helped to gather the reporting data of both simulated and real attacks.

When deciding which mechanisms to use, the group looked at already available tools and the previously given advice. One such tool given was the corporate password manager that had been introduced a few months earlier and was available via the browser or as a desktop or mobile app. Though there had not been an official push to use this tool, the group used the number of Verizon Media employees actively using it as the baseline. At the time, roughly 3% of all employees were logging into the tool at least once a month.

Encouraged Use of the Corporate Password Manager

The next step was to encourage use of the password manager through behavior-changing activities by making it part of the choice-architecture because it was a technology fix to spoofed domain detection. The PE Group installed the corporate password manager browser extension on all managed devices, so it become the default choice for all employees.

Incentives to become active password manager users included being recognized as a "Password Manager Knight" and prizes such as T-shirts, hoodies, hats and laptop stickers, all branded with the Paranoids' keyhole knight logo shown in Figure 1. These prizes were popular and sought after, making them a successful incentive for adopting the password manager.

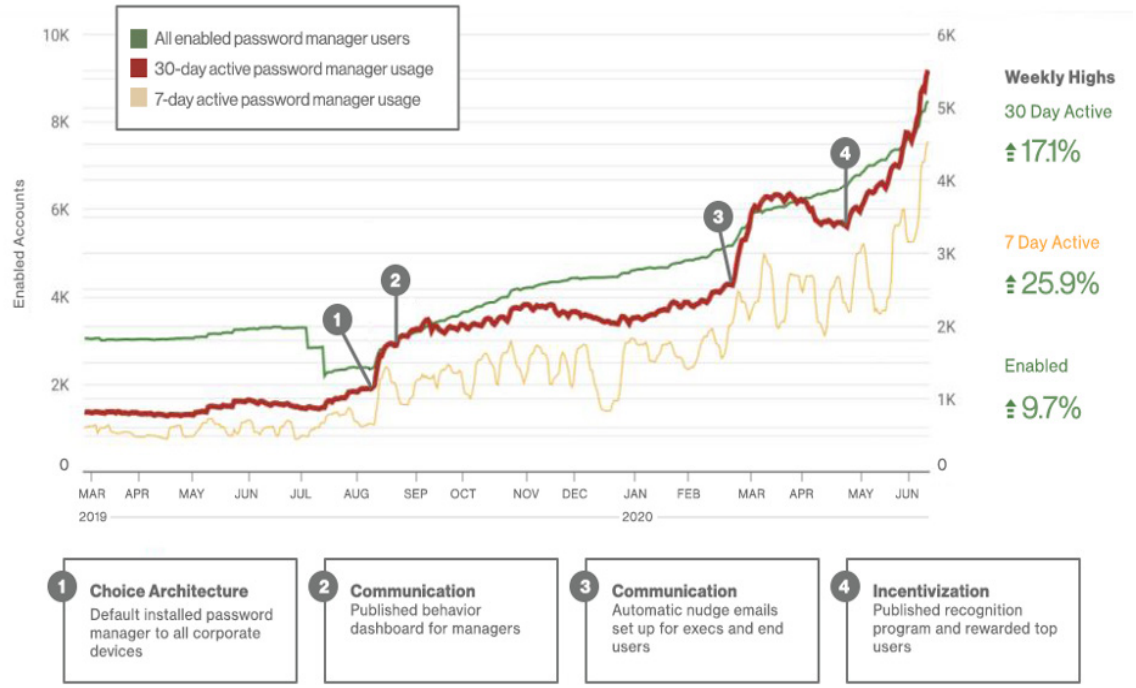
Communication campaigns were used in conjunction with the incentives and the choice-architecture activities to educate users about the value of using the password manager. The PE Group created videos and other content on how to enable the password manager on user devices, how to use it for everyday password generation and storage, and, most importantly, how to spot fake domains within phishing emails using the password manager.

The tone of the communications program showed respect for employees and recognized that each person had their own personal set of values and beliefs. The program was not designed to embarrass employees or dictate new behaviors. One manager explained:

> *"By treating employees as 'whole people,' we show respect for the individuals. They take on new beliefs and values because they believe that what we are asking them to do is what is best for them. When employees take on something for themselves, it changes their values and beliefs, and they include these new things in their behavior. It's a way to empower our employees to make changes."*

Top managers were also involved in promoting the use of the password manager. They emphasized that keeping employees safe was one of their priorities and allowed the PE Group to purchase a premium password manager

Figure 5: Dashboard Showing Impact of Behavior-Changing Mechanisms on Password Manager Usage



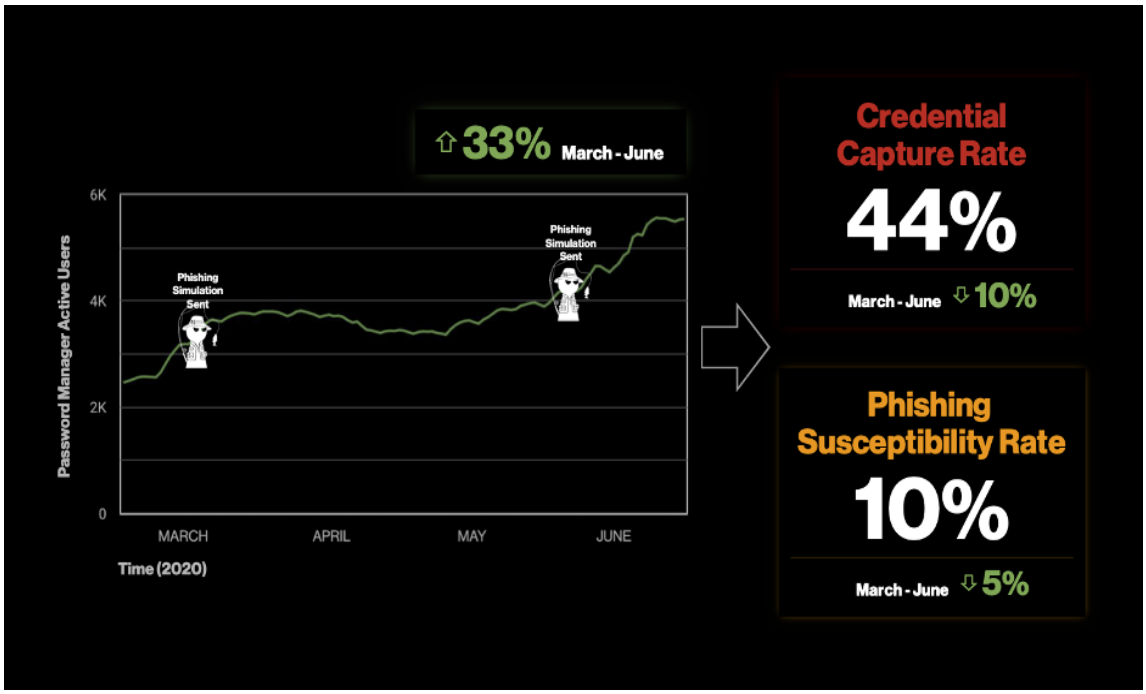
This chart measures the active usage of the corporate password manager (y-axis) over time (x-axis). The green line represents all enabled password manager users, the red line shows the 30-day active password manager usage and the yellow line represents the seven-day active password manager usage.

subscription. This provided employees with free personal accounts as a reward for setting up and using the corporate system, enabling them to be safer from phishing emails on both corporate and personal devices. However, employees who responded to phishing simulations were urged to consider additional education and to use the corporate password manager solution. These communication mechanisms were well received and contributed to the adoption of the password manager.

Finally, password manager dashboards helped managers benchmark their team's performance and compare it to their peers. These dashboards showed password manager usage and the impact of each behavior-changing activity used to drive usage (see Figure 5). Combining the dashboard information with additional information enabled managers to create naughty/nice lists. One manager explained: "We created both naughty and nice lists, but we did not publish the naughty lists for individuals to see. We did not want to shame employees for poor behaviors, only offer applause for good behaviors." Managers would send emails to all employees to encourage positive behaviors, not to embarrass those who did something wrong.

In partnership with the Security Operation Center, the PE team used the information and trends in the password manager dashboard to improve cybersecurity practices. Replies to phishing queues were revised, an incident response runbook on cybereducation was developed, an antiphishing footer was created for all internal communications and reporting of phishing emails was made easier. Finally, the password manager dashboard was also used by senior Verizon Media leadership as a means

Figure 6: Correlation of Increased Password Manager Usage with Decreased Credential Capture Rate



of communication to better understand the activities and impact of the PE Group.

Improved All the Key Measures

From March 2019 to June 2020, all the key measures showed improvement. The rate at which Verizon Media employees' credentials were captured in phishing simulations was cut in half, the number of accurate phishing reports doubled, the company's phishing susceptibility percentage fell to 9.6%, and usage of the company's corporate password manager tripled (see Figure 6, which shows the 2020 data used to inform top management of the success of increasing password manager usage in reducing the credential capture rate).

In the second half of 2020, the PE Group was expanded by adding the Security Engineering Team, which worked with the Behavioral Engineering Team to create additional technology solutions to further drive security behaviors. These solutions included external email labeling, URL rewriting[22] and an in-application function for reporting phishing emails. These technology solutions were incorporated as choice-architecture components, and associated communications and incentives were expanded to include them. As a result, there was further improvement in key measures: the credential capture rate dropped to 34% while the company's susceptibility rate fell to 2%.

Other Indicators of Success

The success of the PE Group's behavioral change initiative was evident in several other ways. Managers within Verizon Media proactively reached out to the group requesting both tool and training support for their team members. Individual employees used their cybersecurity behavior performance data in career development conversations, reported incidents correctly at a higher rate and even reported

22 Modifying a URL structure while loading a page. One cyberdefense is to scan incoming emails for known malicious hyperlinks or attachments that may contain malware. Rewriting URLs allows potential malicious content to be tracked.

phishing emails that arrived in their personal inboxes because the group stressed personal as well as company safety. Some parts of the company were divested or sold during this time and managers who moved to a new organization insisted that the security tools and policies they had come to rely on moved with them. The importance of cybersecurity was evident at every level of Verizon Media. Cybersecurity had become part of the company's values, attitudes and beliefs through the systematic behavior change approaches and managerial mechanisms enacted by the PE Group.

The Paranoids, the wider Verizon Media security team, used the process designed by the PE Group to promote additional security behaviors. The concepts of behavioral design became common practice, unlocking additional opportunities to minimize employees' digital footprints, which reduced their vulnerability to cyberattacks. For example, hackers seeking ways to steal credentials can find multiple digital footprints and triangulate information and use it to impersonate someone or trick them into revealing credentials in some other way. With the success of the PE Group's behavioral design framework, the company began to look into ways to apply these same concepts to consumer security behaviors.

Recommendations for Creating a Cybersecurity Culture

The Verizon Media case shows that the company took a novel approach to changing the values, attitudes and beliefs of its employees to motivate new and safer behaviors with respect to cybersecurity. It recognized that although cybersecurity issues are often addressed with technical solutions such as stronger firewalls and better incident-identification software, there is another, equally important—if not more impactful—defense mechanism: creating a cybersecurity culture.

From our analysis of the Verizon Media case, we have derived five recommendations for effectively building a cybersecurity culture that reduces vulnerabilities potentially introduced by employees. Although these recommendations are based on the experiences of Verizon Media, we believe they can be adapted for different contexts and business environments. Following these recommendations will enable managers to improve the cyber-resilience of their organizations.

Recommendation 1: Recognize that Cybersecurity is as Much a People-Management Issue as a Technology Issue

While regular headlines of cyberbreaches may cause managers to become blasé about their own potential vulnerabilities, there is a common thread among many breaches: the root cause of the majority of them is human error. Research has shown that people are the weakest link in cybersecurity strategies. Managers must therefore face up to the challenge of finding better ways to manage their teams' behavior because changing behaviors is critical to making an organization more secure. However, employees often feel that cybersecurity is not their responsibility but is the job of someone else (usually the IT or security team). Managers need to build a cybersecurity culture that redresses this misperception.

Verizon Media began by identifying appropriate behavior goals, then setting baselines and sharing progress transparently through dashboards. The Proactive Engagement Group recognized that, while it was easy to measure the number of phishing emails reported to company authorities, that was not really a useful measure for how secure the organization was. Instead, the group defined behavioral goals that fit the organization's overall culture and that measured behaviors that actually kept the organization secure. The goals focused on reducing the capture of credentials because this was the group's main concern about creating vulnerabilities.

Once appropriate measures were identified, the Proactive Engagement Group established a baseline by measuring the rate of credential capture and created a plan to improve this metric. Progress on improving the metric was communicated through a dashboard that not only provided managers with a clear indication of how their teams were doing but also shared the progress of other teams, which gave rise to friendly competition between teams. As a result, the mere action of sharing the information

motivated managers and individuals to put in extra effort to improve their metrics.

Recommendation 2: Drive Behavior Change by Changing Values, Attitudes and Beliefs

Recognizing that behavior change is not primarily driven by training classes or commands from top management, Verizon Media built a multidimensional program of managerial mechanisms that altered how team members viewed their role in keeping the organization secure. This program ultimately resulted in the behavior changes necessary to create a cybersecurity culture. The approach adopted by the company was that if employees truly valued something and had the attitude that they could personally do something about it, their behaviors would be consistent with their values and attitudes.

Verizon Media's Proactive Engagement Group treated employees with respect and made tools available (through the choice-architecture) that they could use to be more secure. Successes were highlighted in dashboards and in communications around the organization. Feedback loops facilitated dialogue with employees who wanted to do better but were unsure about how to proceed. The group found that the mechanisms for listening to how employees described the impact of behavioral change policies made them feel more involved, which motivated additional behavioral changes. Employees felt their input and feedback were of value, and that translated into valuing the behavior change goals set by the group.

Recommendation 3: Communicate Successes Widely, but Don't Shame Employees or Embarrass them with Negative Comments

It is common management practice to call attention to great performers; often this is done to show examples that motivate lower performers to raise their game. But in the case of cybersecurity behaviors, this practice can backfire if not done appropriately. Employees can often see through false or contrived messages designed to promote new behaviors. The Proactive Engagement Group at Verizon Media understood this dynamic and used it to reinforce the importance of the sought-after cybersecure behaviors.

Successes and gains made over time were widely shared. The ease of adopting and using the new solutions, such as the corporate password manager, was constantly reinforced in messaging and more informal discussions about rankings on the dashboards. While great performers were rewarded with gifts, electronic badging and other means of showing success, it was done in a way to make them feel good, not to make the less-than-great performers feel bad.

Moreover, the Proactive Engagement Group took great pains not to embarrass employees. If someone was struggling, team members were available to help them. They were not shamed by highlighting their poor performance—a practice followed by all great managers. However, other research we have conducted showed that some organizations use shaming practices such as posting the name of poor performers in public spaces, calling them out in front of co-workers and generally embarrassing them for their poor performance. Not only was this inconsistent with the Verizon Media corporate culture but it was also common knowledge that this type of management would backfire and jeopardize the gains resulting from positive reinforcement.

Recommendation 4: Extend Cybersecurity Practices into Employees' Personal Lives

The research for the Verizon Media case study was carried out during the Covid-19 pandemic when workplaces were already stressed, and workers were forced to work remotely for much of the time. The uncertainty created by this new work arrangement made it easier for cybercriminals to launch successful social engineering campaigns aimed at stealing the credentials of employees who were working from home. This meant that families, friends and others in employees' personal lives were potentially impacted by cybercriminal activity and the Verizon Media PE team recognized that. The Proactive Engagement Group therefore offered employees a license for personal use of the credential management tool, helping them and their families keep their personal lives safer.

This simple action sent a clear message that Verizon Media wanted to help employees be

safe in general, not just at work Not only did this reinforce the belief that cybersecurity was important but it also translated into greater adoption of cybersecure behaviors at work. We recommend that all organizations consider extending their cybersecurity practices beyond the corporate sphere into the personal lives of their employees.

Recommendation 5: Create an Engaging Internal Brand for the Cybersecurity Team

The Verizon Media case illustrated several interesting approaches to managing cybersecurity, starting with the name of the team. By internally branding the cybersecurity team as "The Paranoids," it positioned the team and, by extension, recommendations from the team in a way that all employees could connect with. The name itself was a way of poking fun at the very serious issue of keeping everything secure. Moreover, the team's name made it clear to the average employee that although the actions of the team may feel different, cybersecurity is something they can engage with.

Other mechanisms that reinforced the message that everyone can connect with cybersecurity included a series of actionable recommendations, presented in an equally interesting and engaging way, that every employee could do. For example, the choice-architecture both helped employees be safer at work and at home. It also promoted a strong belief that they can take action to help keep the organization secure (known in the Huang-Pearlson model as the "employee's self-efficacy,") which drove cybersecure behaviors. Another example of a mechanism for connecting cybersecurity with every employee was the use of dashboards, which provided managers and employees with information on their contribution to security and gave rise to friendly competition that encouraged additional secure behaviors. To promote a cybersecurity culture, we recommend that organizations give cybersecurity a current, approachable and engaging image—i.e., an internal brand.

Concluding Comments

Cybersecurity awareness, combined with techniques from applied behavioral science, influenced employees' attitudes and values at Verizon Media, resulting in a strong cybersecure culture. The Verizon Media case reported in this article describes the managerial mechanisms used by the company's Proactive Engagement Group to build a cybersecurity culture and how the group measured the results. Creating shared values was at the core of the group's behavioral change framework. The cybersecurity culture was built by supplementing security awareness with actionable advice and opportunities to practice the desired behaviors.

The mechanisms included reinforcing technological solutions with systematic and well-thought-out communications and providing incentives such as awarding "Password Knighthoods" and gifts. Measuring the activity and reporting results on transparent dashboards provided additional motivation and served to reward those who succeeded while also flagging up those who were not as successful. Training programs and awareness campaigns were part of the mix, but were not the only mechanisms used to create the desired culture. Another key success factor was the group's constant monitoring and tuning of all mechanisms based on what worked best. This attention to detail, together with employee feedback that helped the group to identify new mechanisms for promoting the desired behaviors, was the cornerstone of the successful drive to create a powerful cybersecurity culture.

The Proactive Engagement Group also measured the success of its efforts to build a cybersecurity culture. By measuring the reduction in the number of credentials shared by employees, rather than the less useful number of phishing emails reported to the security team, the group was able to highlight the importance of behaviors that made a difference in day-to-day security. Creating meaningful measures of the actual sought-after behaviors was critical to the success of the Proactive Engagement Group.

In summary, the Verizon Media case illustrates how this organization successfully built a cybersecurity culture. The Proactive Engagement Group used managerial mechanisms to promote shared values, attitudes and beliefs, which drove cybersecurity behavioral change. The group recognized that training and awareness campaigns were necessary but not sufficient cybersecurity investments and that changing

behaviors was best done by changing employees' values, attitudes and beliefs. The innovative mechanisms used to empower employees to keep the organization secure included a choice-architecture, communications, radical transparency, feedback loops, dashboards, friendly competition and more.

Based on our analysis of the Verizon Media case, we have provided actionable steps and activities that other organizations can use to change or create their cybersecurity culture. The investment in building a systematic approach to changing cybersecurity behaviors has significant payback: it increases the resilience of an organization and reduces the chance that employees will inadvertently open up the organization to cyberattacks and breaches.

Appendix: The Huang-Pearlson Cybersecurity Culture Model

Verizon Media's approach to building a cybersecurity culture is an excellent example of the application of the Huang-Pearlson Cybersecurity (HPCC) Model. Huang and Pearlson define cybersecurity culture as the "beliefs, values and attitudes that drive employee behaviors to protect and defend the organization from cyberattacks."[23] As shown in the figure below, the HPCC model suggests that cybersecure behaviors are driven by the values, attitudes and beliefs of an organization, which are visible at the leadership, group and individual levels. People in the organization act in the way they do, in part, because they believe it is important, they know how to do it and it is a priority of their leaders. These values, attitudes and beliefs are influenced by external factors such as the organization's industry, the local country culture, regulations and other factors that company managers have little or no control over. Moreover, the values, attitudes and beliefs of the organization are influenced by managerial mechanisms that managers do control.

At the leadership level, the value placed on cybersecurity is evident by the priority placed on cybersecurity projects by top management, and by leaders' participation in keeping the organization secure and the knowledge they seek on cybersecurity. At the group level, beliefs are apparent by understanding community norms, seeing teams work together to keep the organization secure, and by nontechnical staff enlisting the technical staff's support for security issues. Finally, at the individual level, attitudes about cybersecurity are observable in the employee's self-efficacy (i.e., the belief that one can take action to help keep the organization secure). Individuals also convey their attitudes by demonstrating their awareness of the organization's cybersecurity policies and of the general cyberthreat landscape.

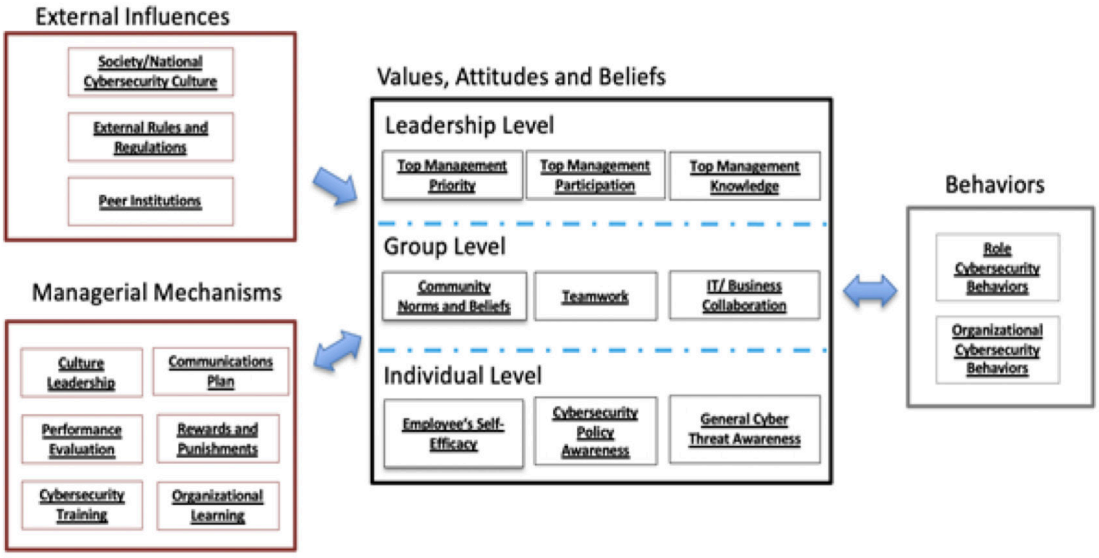
In the HPCC model, values, attitudes and beliefs are influenced by two sets of constructs: *external influences*, which are mostly outside management control, and *managerial mechanisms*, which are levers or activities a manager can employ directly. External influences include things like data protection legislation and regulations. For example, hospitals, consumer product manufacturers and banks have to comply with very different regulations for handling personal data. These regulations influence attitudes about data protection. Peer institutions also influence the attitudes of a firm. If peer firms are cybersecure, it's more likely that a firm will think cybersecurity is of value. External influences are outside the direct control of the organization's leaders, but they still influence values, attitudes and beliefs around security in the organization.

On the other hand, an organization's managers can influence values, attitudes and beliefs through managerial mechanisms. For example, if the performance review process incorporates an evaluation of cybersecurity behaviors, employees are more likely to value the importance of cybersecurity. When managers reward (or penalize) cybersecurity behaviors, it sends the message that these behaviors are valued. Likewise, mechanisms such as training programs, awareness campaigns, communications plans, rewards, incentives, consequences and dashboards showing metrics about behavior are ways that managers can reinforce values, attitudes and beliefs about the importance of secure behaviors.

There were numerous examples of managerial mechanisms in the Verizon Media case study, including password managers, dashboards, badges, stickers and branded gifts, which

23 Huang, K. and Pearlson, K., op. cit., January 2019.

Huang and Pearlson's Cybersecurity Culture Model



reinforced strong attitudes about how important it was for employees to be cybersecure. These values were demonstrated at the leadership level through senior leaders' support of the Proactive Engagement team; at the group level, with friendly competitions being set up by the dashboards; and at the individual level, with a large number of employees downloading the password manager and completing the training to obtain Knighthood status. Cybersecurity behaviors, such as using the password manager and reporting phishing emails, were driven by these values, attitudes and beliefs.

The HPCC model highlights that the primary methods most organizations use to instruct employees regarding how to keep the organization safe, such as training and awareness campaigns, are only nominally effective. The model shows that managers should expect to find more positive impacts from activities and initiatives that promote the belief that it is important for employees to behave securely, that reinforce a value system about the importance of cybersecurity being everyone's responsibility and that instill attitudes that each employee can do something to keep the organization secure. Training and awareness campaigns set the foundation for what leaders want from their employees, but it is the beliefs, values and attitudes that drive behaviors. Unless the values, attitudes and beliefs are changed, there will not be any behavioral change.

About the Authors

Keri E. Pearlson

Dr. Keri Pearlson (kerip@mit.edu) is the executive director of the Cybersecurity at MIT Sloan (CAMS) research consortium. She conducts research that addresses the challenges of senior-level executives' role in keeping their organizations cybersecure. Her work in this area has been published widely, including articles in Harvard Business Review and Sloan Management Review.

Josh Schwartz

Josh Schwartz (josh.schwartz@yahooinc.com) is the senior director of the Proactive Engineering Team within Yahoo's (previously Verizon Media's) information security team known as "The Paranoids."

Sean Sposito

Sean Sposito (sean.sposito@yahooinc.com) is a member of the Behavioral Engineering Team within Yahoo's (previously Verizon Media's)

information security team known as "The Paranoids."

Masha Arbisman

Masha Arbisman (masha.arbisman@robinhood.com) is the engineering manager of behavioral engineering in Robinhood Financial LLC's security organization. She was previously the manager of the Behavioral Engineering Team within Yahoo's (previously Verizon Media's) information security team known as "The Paranoids."