Building a Security Propaganda Machine: The Cybersecurity Culture of Verizon Media

(A CAMS MIT Whitepaper)

Dr. Keri Pearlson, Cybersecurity at MIT Sloan, kerip@mit.edu
Sean Sposito, Verizon Media, sean.sposito@verizonmedia.com
Masha Arbisman, Verizon Media, masha.arbisman@verizonmedia.com
Josh Schwartz, Verizon Media

February 28, 2021

Abstract: When the security organization inside Verizon Media decided to improve its cybersecurity culture, its leaders knew they'd need to find a way to engage every employee and measure progress to find success. They created the Proactive Engagement team to oversee the corporate defense of Yahoo, AOL, and their other media brands. The team created a way to measure the impact of their user-centric approach to cybersecurity culture and created a step-by-step plan to improve the numbers.

Using the lens of the Huang and Pearlson Cybersecurity Culture Model (2019), this paper discusses cybersecure behaviors the company encouraged and the managerial mechanisms they used to drive them. Those mechanisms included choice architecture, communication techniques, incentivization, and training that they used to build a culture of cybersecurity that changed the values, attitudes, and beliefs of employees. The results have been significant. Since shifting to this new approach, the rate at which Verizon Media employees' credentials were captured in phishing simulations has been cut in half, the number of accurate phishing reports doubled, and the usage of the company's corporate password manager tripled. The team claims its success relies on three steps: identify a kill-chain breaking action, measure it, and test managerial mechanisms to improve the numbers.

A Model of Organizational Cybersecurity Culture.

Keeping our organizations secure from cyber breaches has never been more important. Guarding assets against malicious actors is one of the top priorities of every CIO, and the importance of protecting digital and physical assets from cyber-attacks has reached boards of directors. But technology can only do so much to protect organizations. People are the weakest link in security strategies. In the 2020 Data Breach Investigations Report, Verizon Corporate highlighted that "sixty-seven percent of all breaches come from three attack types: credential theft, errors and social attacks," all of which can be attributed to human risk. Managers are having a hard time. They are challenged to find ways to motivate employees to perform in ways that ensure company assets are secure, networks remain

uncompromised, and staff are not fooled by phishing emails and fake websites. This means that a culture of cybersecurity must be created, and that does not happen easily.

Organizational culture as a construct is often attributed to British sociologist Elliott Jaques, who, in 1952, introduced the concept in his book *The Changing Culture of a Factory.*[1] 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."[2] 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."[3] Cooke and Rousseau suggest that organizational culture are beliefs and values that guide thinking and behaviors.[4] Edgar Schein expanded the notion of organizational culture in his well-known work *Organization Culture and Leadership* (Jossey-Bass, 2004) 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 (2019) applied the concept of culture to explain the cybersecurity behaviors of individuals in an organization. Their definition of a culture of cybersecurity is the "beliefs, values, and attitudes that drive employee behaviors to protect and defend the organization from cyber-attacks."[5] Huang and Pearlson's cybersecurity culture model (see FIGURE 1) suggests that cyber secure 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 do what they do, in part, because they believe it is important, they know how to do it, and it's a priority of their management. These values, attitudes, and beliefs are influenced by each individual's environment and external influences such as the industry of the organization, the local country culture, regulations, and other influences that internal leaders have little or no control over. Further, the values, attitudes, and beliefs of the organization are also influenced by managerial mechanisms that managers do control.

---

[1] (Reference: Hatch, Mary Jo; Cunliffe, Ann L. (2013) [1997]. "A history of organizational culture in organization theory". *Organization Theory: Modern, Symbolic, and Postmodern Perspectives* (2 ed.). Oxford: Oxford University Press. p. 161. ISBN 9780199640379. OCLC, 809554483).

[2] Jaques, Elliott (1951) *The Changing Culture of a Factory.* Tavistock Publications Limited. p. 251 ISBN 0415264421)

[3] Ravasi, D.; Schultz, M. (2006). "Responding to organizational identity threats: Exploring the role of organizational culture." *Academy of Management Journal*. **49** (3)).

[4] Cooke, Robert A, and Denise M. Rousseau,(1988) "Behavioral Norms and Expectations: A Quantitative Approach to the Assessment of Organizational Culture". *Group and Organizational Studies*, 13(3)).

[5] Huang, Keman, and Pearlson, Keri (2019). "For What Technology Can't Fix: Building a Model of Organizational Cybersecurity Culture." HICSS URI: https://hdl.handle.net/10125/60074 ISBN: 978-0-9981331-2-6

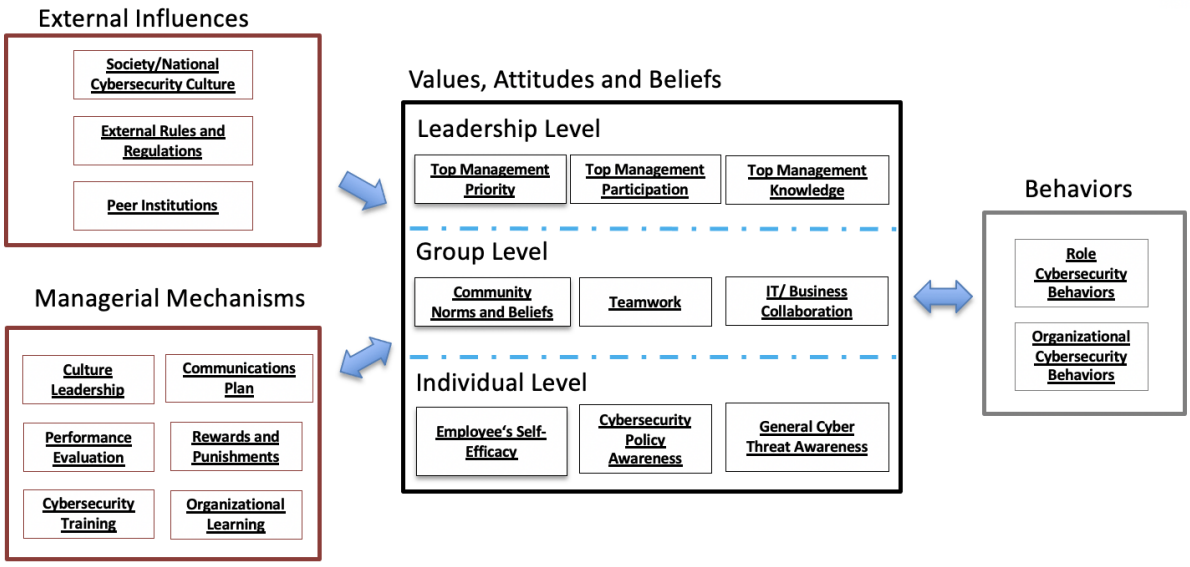


FIGURE 1: Model of Cybersecurity Culture
(Reference: Huang, Keman, and Pearlson, Keri (2019). "For What Technology Can't Fix: Building a Model of Organizational Cybersecurity Culture." HICSS URI: https://hdl.handle.net/10125/60074 ISBN: 978-0-9981331-2-6)

Diving deeper into this model, the values, attitudes and beliefs can be seen at three levels of the organization: leadership, group, and individual. At the leadership level, the value placed on cybersecurity is evident by the priority placed on cybersecurity projects by top management, the participation in keeping the organization secure, and the knowledge top management seeks on cybersecurity. At the group level, beliefs are apparent by understanding community norms, seeing teams work together to keep the organization secure, and by non-technical staff enlisting technical staff's support around security issues. Finally, at the individual level, attitudes about cybersecurity are observable in the employee's self-efficacy or the belief the employee can take action to help keep the organization secure. Individuals also convey their attitudes by demonstrating their awareness of the cybersecurity policies of their organization and of the general cyber threat landscape.

Values, attitudes, and beliefs are influenced by two sets of constructs: External Influences, which are mostly outside the general manager's control, and Managerial Mechanisms, which are levers or activities a manager can employ directly. External influences include things like the data regulations operating on the organization. For example, a hospital has different regulations about handling data than, perhaps, a consumer product manufacturer, and a bank has different regulations than both. These regulations influence attitudes about data protection, as do geographical differences. Peer institutions also influence the attitudes of a

firm. If peer firms are cyber secure, it's more likely that a firm will think cybersecurity is of value.

Managerial mechanisms are the area of most interest to managers since they are the actions a manager can take to influence values, attitudes, and beliefs. 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 punish) cyber-secure behaviors, it sends the message that these behaviors are valued.

Verizon Media's Culture of Cybersecurity: Defining Proactive Engagement.

Verizon Media, a division of Verizon and a sister company of Verizon Business, is an advertiser, publisher and global partner that drives opportunities for its clients through search, media and mobile opportunities. The company was previously named Oath until early 2019 and houses brands such as Yahoo and AOL, as well as RYOT Studios and Techcrunch, among many others. Verizon Media's security team is called The Paranoids, a name that originated in the late '90s at a time when Yahoo was a separate entity. The Paranoids are responsible for all cybersecurity program objectives, activities, and guidance for Verizon Media.

Realizing that a culture of cybersecurity was fundamental to the success of their mission, their Proactive Engagement group set out to enable shared values, attitudes, and beliefs among employees by rewarding behaviors that improved that company's security posture. This group encompassed three teams. **Offensive Engineering** (**Red) Team** evaluated systems, services, processes, and people to discover systemic weaknesses. **Security Education** institutionalized the lessons from the Red Team team's findings and scaled those learnings to the entire population through mandated training. And **Behavioral Engineering** took a data-driven approach to baseline and influence security behaviors with an emphasis in employee value adoption.

Using the Model of Cybersecurity Culture, the Proactive Engagement group sought to answer how to use the listed managerial mechanisms to encourage value adoption within employees. The team came up with a very specific set of activities that they used to encourage cybersecure behaviors of employees in the company. They first identified specific kill-chain-breaking actions based on realistic cyber-attacks. Then they found both technology fixes to those actions and actionable advice rooted in those actions across the entire company. They enabled the technology fixes and broadcasted this advice in the form of awareness and nudge communications, simulation, or training, as well as a combination of all three.

The Difference Between Actions, Habits, and Behaviors.

In the summer of 2018, the Proactive Engagement group noticed that driving behaviors and actions was more complex than simply requiring a training class or bringing awareness to unwanted habits. To create the culture and shared values that would result in desired actions and behaviors, the group's change in focus began by defining the distinction between actions, habits, and behaviors. The team started by defining each as:

An *action* was something a person does to completion. For instance, Verizon Media employees were required to take an annual security training course. The desired result, taking the class, is an *action*.

A *habit* was a shortcut made in the human brain for repeatable actions. For example, training employees to rely on a password manager, instead of an individual's creativity, to create corporate secrets whenever prompted to change credentials can lead to a formed habit. An example of this is the creation of a non-human-friendly password that looks like "Rcek!2mr4h7F%3&ZExxR^" instead of a human-friendly "MyDogHas10Lives!2020." This leads to the creation of a habit because it requires logging into the password manager regularly to maintain access to corporate assets and secure password generation.

Finally, *behaviors* were defined as the combination of both actions and habits within the context of a situation, environment, or stimulus. In the prior example, the security behavior is not simply "use a password manager" but "when creating or updating accounts, generate and store credentials using a password manager."

Attempting to change a behavior meant first identifying the specific context for the desired action. The Paranoids called this the creation of a *behavioral goal*. When creating a behavioral goal, the Proactive Engagement team aimed to answer the question: "In which specific context do we want a specific cohort (or person) to do what specific action?" An example of which is, "When generating a new single sign on password, we want all employees to generate and store the password within our corporate approved password manager." The ability to define these goals became the basis of effectively measuring the awareness and attitude of individuals as it relates to cybersecurity culture within the organization.

Proactive Engagement: Define, Measure, Act.

Changing behavior, according to the Huang and Pearlson model, is done by setting up values, attitudes and beliefs that align with desired behaviors leaders seek to drive. To change behavior in their organization, the Paranoids used a seemingly simple but effective, three-step-process to drive experiments and make decisions aimed at improving the security behaviors of employees:

Step 1: Identify the desired behavioral goal. A clear goal for a specific behavioral outcome is a prerequisite for any measurable change to occur. The goal avoids what the team called "impossible advice," which is any security guidance that requires the end user to make a qualitative judgement about security. Examples of impossible advice include "don't click insecure links" or "always use a secure password". In these cases, the judgement of what is deemed secure is a matter of perspective, so the desired behavioral goal does not contain enough information.

Step 2: Find an appropriate measure, and create a baseline. Figuring out which baseline measurements impacted contextualized actions was critical to the team's ability to influence behavior. Having baselines then gave the team a way to show improvement in the organization's goal for more secure behaviors over time. In the case of the behavior goal of reducing the success of phishing attacks, instead of focusing on training employees to not click links (impossible advice), the team measured the likelihood of employees to enter credentials into a fake SSO page once on that page. Using this measure alongside vendor logs from the phishing simulation provider and HR data allowed them to identify which individual employees (as well as employee groups and roles) were most at risk for credential capture phishing attacks and that gave the group a clear measure and baseline to improve.

Step 3: Take actions to affect the measured behavior, adjust those actions over time, and repeat the process. Activities were then designed to impact the baselines. But equally important to the success of driving appropriate behaviors was the learning from the results of these activities and the cycle of adjusting and doing new activities to continually improve. In this way, the desired behavior goals were achieved. In the case of the phishing behaviors, the Proactive Engagement team used technology fixes, cascading communications, passive and active competition, communication nudges, and in-time training to push credential capture rate down and drive the increase of reporting rates.

This three-step process became the bedrock for behavioral-change-based experiments the Proactive Engagement team conducted. The group broke down those experiments into categories: **choice-architecture**, **communication, and incentivization**.

Choice-Architecture referred to the practice of organizing context to influence individual choice by the use of defaults, framing, and other choice options. For the team, this meant making the "right" behavior as easy as possible through contextual change streaming from updates to technology and choice design. For instance, in 2019, the Paranoids pre-installed 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 while reducing the number of steps and time required to follow security guidance.

Communication was further broken down into three categories that match the Huang and Pearlson model: **top-down passive competition** (leadership level), again, in the form of monthly emailed and universally accessible dashboards where executives could compare their direct reports' adoption of, for instance, active password manager usage against one another; **manager-to-manager peer workshops** (group level), including threat briefings at team meetings; and **bottom-up nudging, active competition, and incentivization** (individual level) encompassing positive messages and using social proof, often sent over email and corporate communication applications to 'nudge' users to change their behaviors.

Incentivization tactics were management mechanisms that provided incentives to change the attitudes, and ultimately the behaviors, of the group. Examples included **callouts**, such as identifying employees who were 'doing the right thing; **recognition** of those employees with swag (gift rewards), badges, or titles; and **naughty/nice lists** that typically took the form of team dashboards accessible to managers and self-progress dashboards accessible by individual employees.

The group encouraged each behavior by first selecting a **choice-architecture** to make the desired behavior an easy, if not the default, action. Next the group influenced the beliefs and values of their organization through **communication channels** such as just-in-time training, tutorials, and automated reminders sent over email or corporate messenger. Then they created **incentives** to change attitudes to inspire employee actions, such as fun titles ("[Password Manager] Knighthood") for competitions and branded Paranoids merchandise prizes earned by the completion of these behaviors to a certain standard (see an example of a laptop sticker in Figure 2).

FIGURE 2: Brand and Logo of the Paranoids Password Manager Knight.

The Paranoids found that the most impactful changes required all three techniques.

Dashboards Made Measured Behaviors Transparent.

Measuring behaviors was fundamental to the success of the Proactive Engagement team and is key to successful use of the managerial mechanism described in the Huang and Pearlson

model. Measures resulted from three primary employee behavioral sources: *reporting security incidents/events*, *tool usage,* and *feedback*. Each one was measured using a combination of data maintained by human resources (identifying employee names, roles, and managers), vendor information (for instance, usage of a password manager or results of phishing simulations), the security team (think, tickets relating to phishing reporting maintained by the Security Operations Center), and data from marketing automation used to nudge users. Figure 3 shows the integrated system that the team built, integrating all of these different data sources into one behavioral engineering machine.

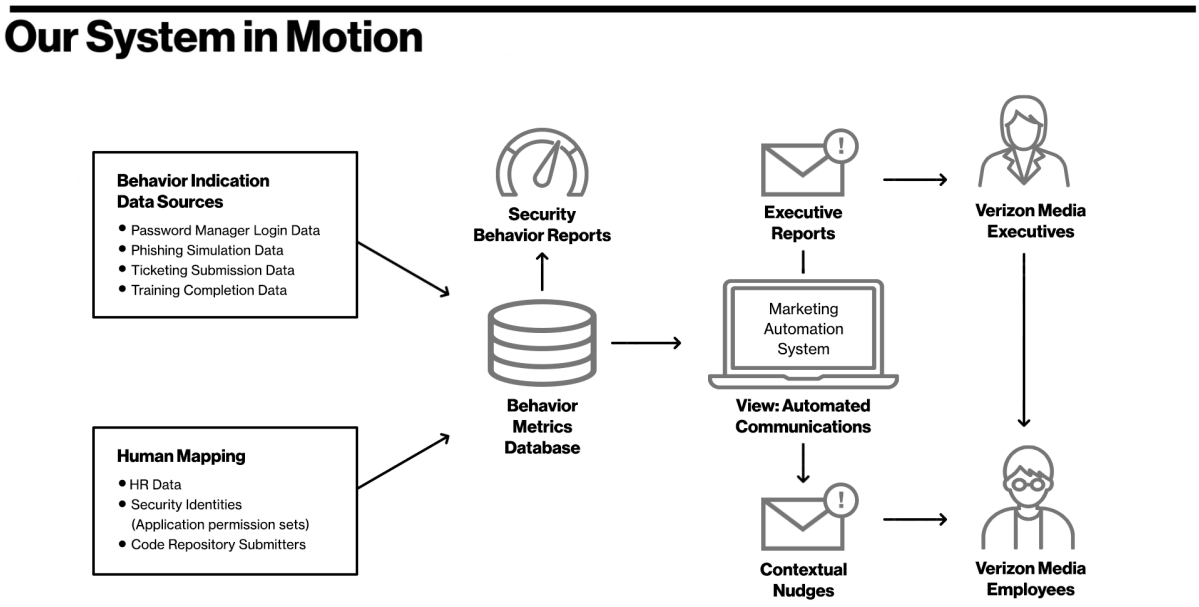


FIGURE 3: Behavior Measurement and Communications Automated System built by Proactive Engagement.

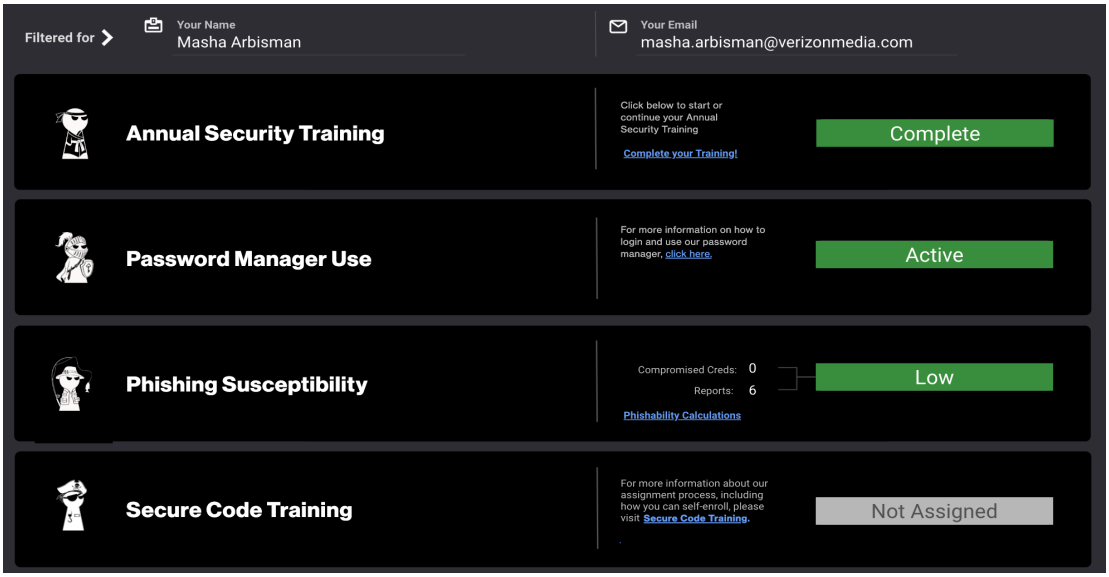
The Proactive Engagement group used these three key metrics to measure its own success:

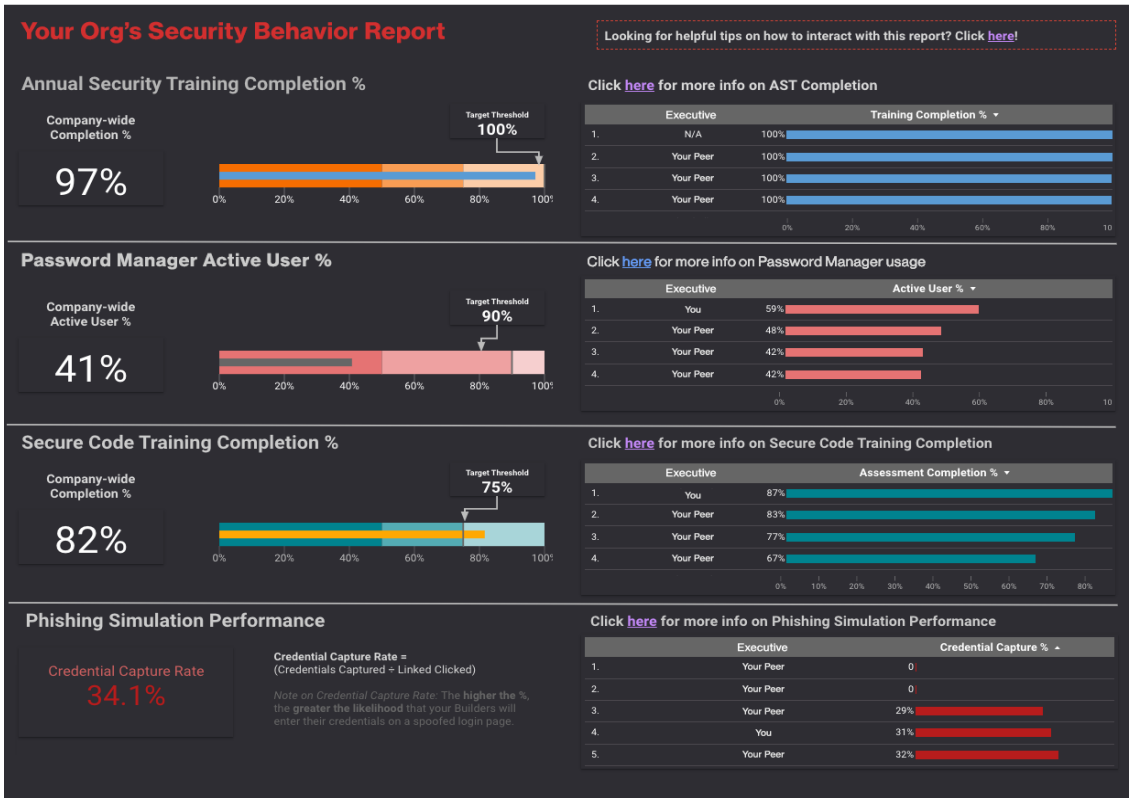
- Accuracy of employee reporting,
- Increasing usage of tools,
- Engagement among vulnerable communities of employees, the reporters in the newsrooms, and the company's executives.

Accuracy in reporting referred to the percentage of actual phishing emails or security incidents reported to the Security Operations Center as opposed to false-positives resulting from, for instance, a *phishy-looking* internal communications message. Increased tool usage referred to an individual's active usage of the company's password manager, VPN, reporting shortcut button, security messenger-bot, etc. And engagement, for instance, referred to attendance at optional events such as cybersecurity hygiene workshops aimed at helping highly visible employees avoid doxing and impersonation, including personal account takeover.

The team measured these metrics and displayed them in dashboards that compared individual, team, and organization adherence. The Proactive Engagement group created these dashboards for managers and executives to track the adoption of password managers, security training completion, and susceptibility to phishing simulation covering both credential capture and reporting rates. They were also made available to individual employees so they could benchmark their personal security behaviors against their peers. The dashboards made it possible to visualize the data produced from employee completion of the managerial mechanisms implemented in a way that created accountability and competition, impacting value change at the leadership, group, and individual levels mentioned in the Model of Cybersecurity Culture. As shown in Figures 4 & 5 the dashboards included:

- **A behavioral indication** -- a source of discrete, measurable, and attributable artifacts that indicate the state of the desired behavior.
- **Human mapping** -- a way to map data points to individual employees within their contextual organization structure, such as leaders, teams, or products.
- **View mechanism** -- the ability for the Proactive Engagement team or the target population to interact with the output of the behavioral change system.





FiIGURES 4 & 5: *The Proactive Engagement team has created dashboards for both individual employees (Fig.4) and managers (Fig.5) to review risks and understand direct reports' behavior, respectively.*

In the absence of measuring actions — such as secure code training and annual security training completion — it was difficult (at least in the Proactive Engagement group's view) to holistically understand behaviors. For example, Figure 4 shows that Masha has completed the annual security training, is an active password manager user, and has a low susceptibility when it comes to phishing simulation. With this information, the Proactive Engagement group can hypothesize that completing the annual security training taught Masha to report suspicious emails and actively using a password manager has shown Masha how to prevent credential capture, both leading to a low susceptibility score. Looking at company behavior averages (Figure 5) and their changes over time have helped the Proactive Engagement group determine which choice-architectures, communication strategies, and incentivization programs have been most influential in changing values, attitudes and beliefs about cybersecurity. Without key behavior metrics, the team would have trouble testing and proving hypotheses around implementing new managerial mechanisms and their impact on the employee base. One of the team's most profound findings came from trying to solve for a high credential capture rate within phishing simulations.

Decreasing Credential Capture.

Since its inception, the Proactive Engagement group focused on prescriptive advice predicated on actions that break kill chains. After learning of successful simulated account takeover from a series of offensive operations (run by the Red team), the Proactive Engagement group decided to focus on changing attitudes that would result in decreasing behaviors that directly led to credential capture. The team questioned the industry standard of measuring the rate at which employees clicked links within phishing simulations, and ultimately decided to abandon the measure altogether.

Upon making the conclusion that asking employees to determine if a link was suspicious was impossible advice as the decision was completely subjective the individual making it, the Proactive Engagement group defined a new behavioral goal for employees: "when your corporate account receives an email sending you to a website asking for you to enter credentials, we want all employees to report the email to our defense team." The team highlighted three key measures: (1) how many employees entered their credentials on a fake login page that they got to from a phishing simulation, (2) how many employees entered their credentials on a fake login page once they've already landed on said page, and (3) how many employees reported the phishing simulation email. They named each metric and calculated them as follows:

1. Susceptibility Rate = number of employees who entered credentials and did not report phishing email divided by total number of phishing simulation emails sent.
2. Credential Capture Rate = number of employees who entered credentials (and did not report) divided by number of employees who both opened the phishing simulation and landed on the fake login page.
3. Reporting Rate = number of employees who reported the phishing simulation divided by the number of total simulation emails sent.

With a behavioral goal and key measure defined, the team set out to implement new managerial mechanisms to diminish the rate at which employees gave up credentials. This feat would not have been possible without the close partnership of the Security Operations (Blue) team who had noted that real world phishing attempts were a major vulnerability for Verizon Media and helped gather the reporting data of both simulated and real attacks.

First, the team needed baselines. In early 2018, the Paranoids measured credential capture rates from phishing simulations as 50%, meaning that they were capturing nearly one out of every two employees' credentials when those employees had both already opened a test email and clicked a hyperlink that took them to a fake login page. One out of every 10 employees were accurately reporting the original phishing simulation and the simulations measured a phishing susceptibility rate for the company at 14%.

When deciding on which managerial mechanisms the team could use to influence a change in credential capture behavior, the Proactive Engagement group looked at other tools and advice given within their ecosystem. The Paranoids had introduced a new corporate password manager tool a few months prior and although there was not an official push to use the tool, the Proactive team baselined the number of Verizon Media employees actively using it. At the time, roughly three percent (3%) of all employees were logging into the tool (either browser, desktop, or mobile option) at least once a month.

It did not take long for the team to realize that they could use the password manager as a technological fix to spoofed domain detection and used the first managerial mechanism of choice-architecture. They pushed the corporate password manager browser extension to all managed devices, allowing the **password manager to become the default choice.** The group offered **incentives** for active usage, such as "[Password Manager] Knighthood '' recognition and swag prizes. Merchandise such as T-shirts, hoodies, hats, and laptop stickers -- all branded with the Paranoids' key-hole knight logo.

The team created how-to videos and content to educate users on how to enable the password manager on their devices, how to use it for everyday password generation and storage, and most importantly, how easy it is to use the password manager to spot fake domains within phishing emails. The Paranoids highlighted treating employees as whole humans, setting company safety de facto to individual cybersecurity health. Top management prioritized employee individual health by purchasing an elevated password manager subscription which provided each employee with a free premium personal account as a reward for setting up and using a corporate one. The team stressed to users that their goal was to keep employees more aware and possibly safer from phishing emails, whether they came to either their corporate or personal devices. These **communications** were paired with emails that **nudged** those who failed phishing simulations to offer more education and point them toward the corporate password manager. The group also created dashboards for managers to benchmark their corporate pillar's performance against their peers -- providing both an incentive to employees through naughty/nice lists that would result in emails from their managers and a communication tool between Proactive Engagement and senior Verizon Media leadership. All of these implemented managerial mechanisms promoted password manager use as shown in Figure 6.

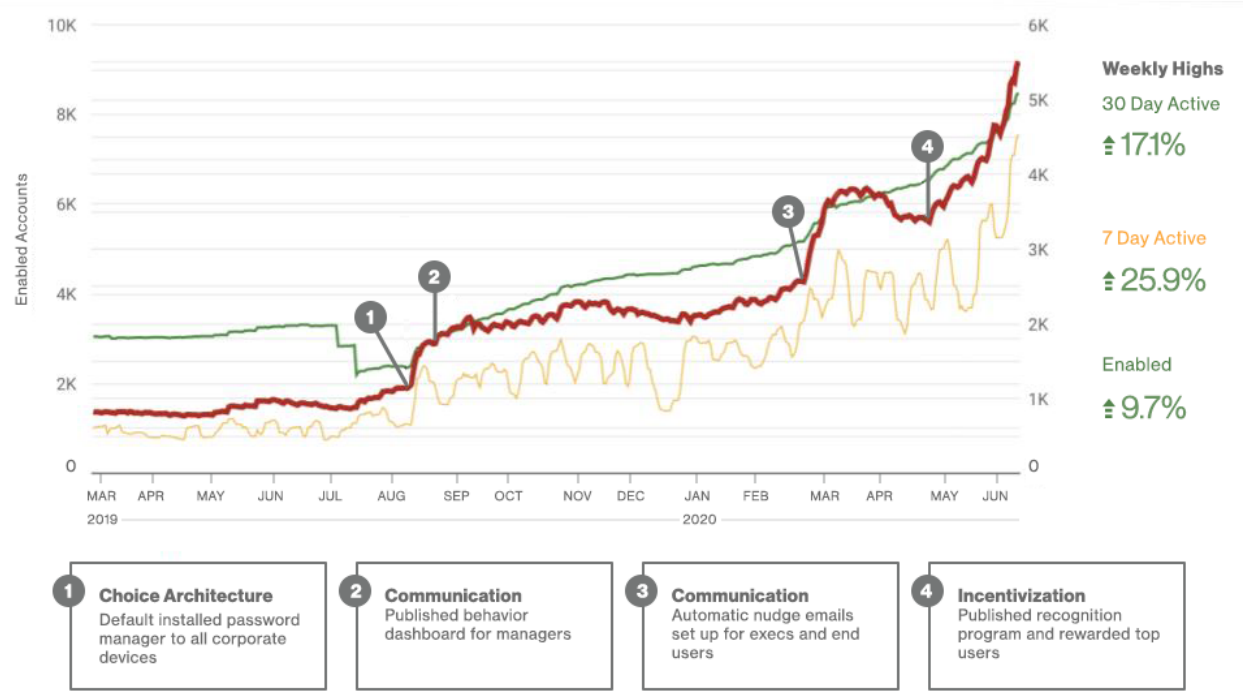


FIGURE 6: *The Proactive Engagement team enacted a series of experiments to increase password manager adoption, and measured their success. The chart measures the active usage of the company-managed password manager (y-axis) over time (x-axis). The green line represents all enabled password manager users, 30-day active password manager usage is denoted by the red line and 7-day active password manager usage is shown by the yellow line.*

The Proactive Engagement team also partnered with the Security Operations Center to revise replies to phishing queues, develop an incident response runbook focused around education, and make reporting easier. From March 2019 to June 2020, 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 the usage of the company's corporate password manager tripled. Figure 7 shows the 2020 portion of this data that was sent to leadership to promote top management knowledge as specified in Huang and Pearlson's model.

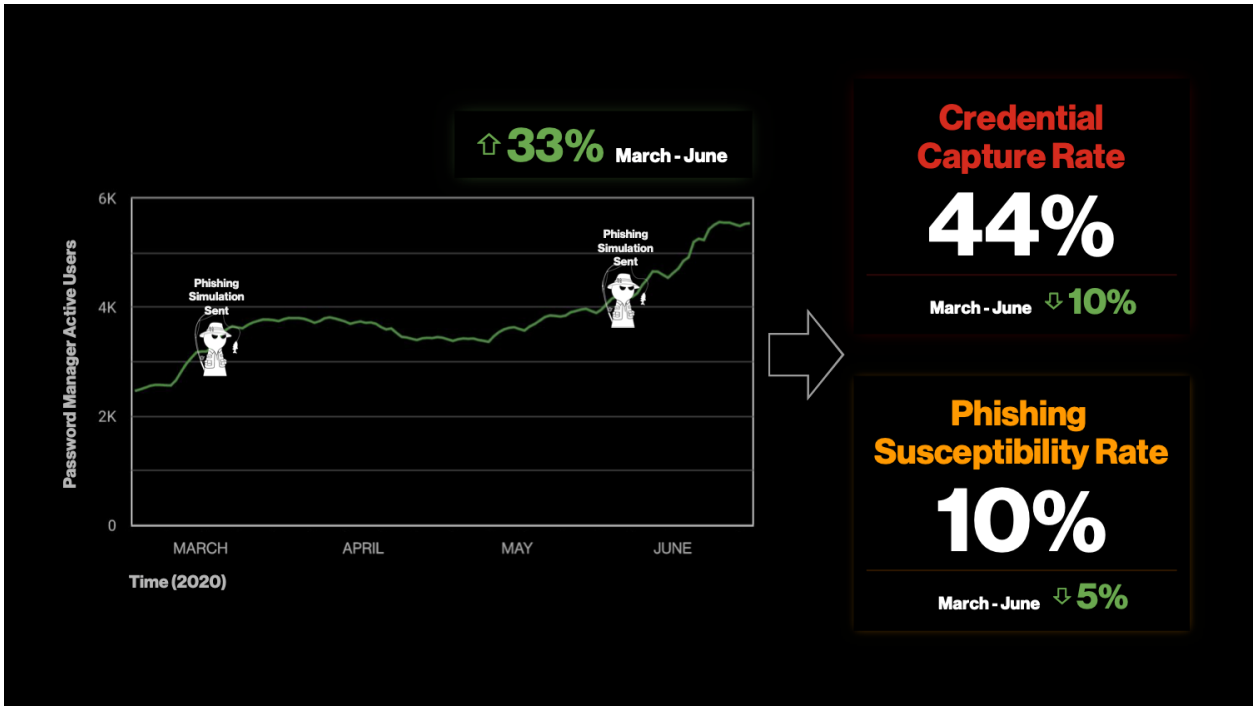


FIGURE 7: Slide taken from executive mid year read out showing the password manager use and its correlation to the decrease in phishing simulation credential capture rates for the first half of 2020.

In the second half of 2020, the Proactive team grew to include a fourth team called Security Engineering. This team worked with Behavioral Engineering to enable more technology fixes including external email labeling, URL rewriting, and an in-application function for phish reporting, all while continuing both the communication and incentivization programs that they previously set up. They saw credential capture rate drop to 34% while the company's susceptibility rate fell to 2%.

Not only did the team see employee behavior change over time, but they saw values, attitudes, and beliefs develop. Executives began using the behavior dashboards as evidence for reasoning behind organizational and purchasing decisions. Managers reached out to the team proactively requesting both tool and training support for their team members before enforcing usage. Individual employees used their performance data in career growth conversations, reported incidents correctly at a higher rate, and even reported phish against the company that came into their personal inboxes because The Paranoids stressed their individual safety over just that of the company. Companies under the Verizon Media umbrella that were sold over the year also insisted that the security tools and policies they came to rely on moved with them. Security was written into the company culture through a shift in values enabled by the systematic behavior change approaches and managerial mechanisms enacted by the Proactive team.

Conclusion: Security awareness Is no longer enough.

The Verizon Media case illustrates how to use the managerial mechanisms from the Huang and Pearlson Culture model, and most importantly how to measure them. This case describes cybersecure behavior goals targeted by the security team and how to use managerial mechanisms to influence them. The case study specifically highlights the team's experience in reducing the number of credentials shared by employees through phishing emails. The Proactive team successfully drove these behaviors by building a culture of cybersecurity and changing the values, attitudes, and beliefs of employees through a series of managerial mechanisms that included integrating technological fixes, systematically sent communications, incorporating incentivization, measuring activity, reporting activity on transparent dashboards, providing training, and tuning all of the above based on what was most successful.

This case suggests six things managers can do to drive cybersecure behaviors in their organizations.

1. **Identify behavior goals to be driven**. This case study demonstrated a behavioral goal that significantly blocked an attacker's ability to breach a corporation- stop sharing credentials. While it may be easy to measure the number of phishing emails reported to company authorities, that behavior does not directly make the organization more secure. Pick behavior goals that create a more secure organization, not behaviors that are simply easy to measure.
2. **Identify measures and set a baseline**. Once preferred behaviors are identified, the measures and baseline give a starting point so improvements can be observed. The well-known phrase "what gets measured gets managed" is appropriate here. Communicating desired behaviors will increase awareness of what is to be done, but measuring it and communicating the progress drives the attitude that this is really something important and worth doing. Constant evaluation and improvement of these activities was an important component to keep employees engaged and measure success from the investments. The Proactive Engagement team went further with their data-driven approaches. They centralized security behavior data and analytics in one database then used the analytics to prescribe personalized training, communication, and choice-architecture.
3. **Build a multi-dimensional program of mechanisms that mean something to employees.** The Proactive Engagement team used activities such as rewards that reinforced successes toward the behavioral goals, communications programs that used multiple ways to keep the behavioral goals top of mind, training programs that showed employees how to achieve the behavioral goals, tools and choice-architectures that made it easier for employees to achieve behavioral goals, and evaluation so employees knew how they were progressing toward their goals. This

multi-dimensional approach ensured that the largest number of employees possible would follow the policies and help keep the organization more secure.

4. **Create a transparent dashboard**. If measures indicate movement toward or away from the goals, creating a transparent dashboard makes them widely visible. Having a dashboard that draws data automatically from relevant systems gives managers both a clear indication of how their teams are doing and also sets up a friendly competition between groups which, in this case, motivated leaders and individuals to try harder to improve their results.
5. **Develop a feedback loop that prioritizes user experience**. The behavior changes that drive security in the organization can be intrusive, causing employees to block or reject them. The Proactive Engagement team found that by creating a mechanism for listening to employees and how the policies impacted them also created additional attitudes about the importance of each employee helping keep the company secure. This feedback loop provided a better understanding of who the users were and how they interacted with the tools and policies the team sought to implement, which further informed future activities, tools and policies the team devised.
6. **Publicize successes and iterate on deficiency**. The Proactive Engagement team was not shy about sharing successes. Their program not only encouraged secure behaviors, but the dashboards and communications plans made sure the entire organization knew about the behavior goals and the successes they were having. The measurement and analysis cycle gave the team additional content to share with managers by highlighting the improvements over time.

The Paranoid's story from Verizon Media Illustrates key components of the Huang and Pearlson model, including how their team built a culture of cybersecurity by using managerial mechanisms to promote values, attitudes, and beliefs of their leaders, teams, and employees to drive cyber-secure behaviors. This case study provides actionable steps and activities any organization can use to change the cybersecurity culture of their business. This investment in building a systematic approach to changing behaviors is worth it to increase the resilience of an organization to prevent their employees' actions, attitudes, and beliefs from opening the corporation up to attack and potential breach.

DICTIONARY OF TERMS.

- Proactive Engagement - A Cybersecurity team at Verizon Media that consists of four smaller teams including Offensive Engineering, Security Engineering, Behavioral Engineering, and Security Training/ Education.
- Behavioral Engineering - A team within the Proactive Engagement group that uses behavioral and cognitive science approached to solve for kill-chain breaking behaviors (human risk).
- Kill-chain Breaking Action - An action or behavior that can preemptively stop or defend from an attack.
- Cyber Breaches / Cyber Attacks - An incident that results in unauthorized access to company information, data, applications, or devices.
- CIO - Chief Information Officer, the executive that oversees technology, people, and process and is the top leadership within the company's IT organization.
- Malicious Actors - those who are responsible for security incidents.
- Managerial Mechanisms - levers or activities that a manager can employ directly to influence values, attitudes, and beliefs within an organization, as defined by Huang and Pearlson.
- Credentials - the secrets that authenticate a user when logging into accounts. Credentials are usually made up of a username and a password, but can also include a pin, biometric event, two-factor or other type of authentication.
- Phishing Simulations - a test in which simulated deceptive emails are sent by an organization to their own employees in order to baseline and train responses to phishing emails.
- Password Manager - A computer program that allows users to generate, store, and manage passwords in an encrypted database.
- Choice Architecture - A behavioral economics approach to design in which choices are presented to consumers in a way that impacts their decision-making.
- Incentivization - The practice of offering incentives to motivate consumers.
- Phishing Reports - The act of reporting a phishing email to the security team of an organization.
- Technology fixes - The installation, update, or change of technology that is used to force specific choice architectures.
- Action - Something a person does to completion.
- Habit - A shortcut made in the human brain that causes repeatable actions.
- Behavior - Actions and habitPage 17 of 18s within the context of a situation, environment, or stimulus.
- Cybersecurity Behaviors - Actions and habits within a specific context of a situation, environment, or stimulus that can lead to cyber breach.
- Corporate Secrets - The intellectual property of an organization. This can comprise data, information, employee records, formulas, processes, designs, or any proprietary information.
- Behavioral Goal - A goal in which a specific context is identified for the desired actions and habits.
- Cascading communications - The passing of information from top executives to managers to employees.
- Passive competition - A managerial mechanism that is created by default when individual data is grouped by performance and made publicly available to the organization.
- Active competition - A managerial mechanism that is announced within the organization and used to highlight and reward top performers.
- Communication nudges - a form of communication that reliably influences choice-architecture and alters individual behavior without prohibiting other options/ individual choice.
- In-time training - training offered at the point of interaction between the individual and the thing they need to be trained on.
- Social Proof - a psychological phenomenon in which individuals mimic the actions of others in an attempt to conform.
- Security Incident - any attempted or successful unauthorized access, use, modification, disclosure, or destruction of information.
- External Labeling - a practice in which emails sent by external senders to the organization are labeled as such. The label is used as a warning to take extra precautions as they come from a source that is not considered trusted by the organization.
- URL Rewriting - a process of modifying a url structure while loading a page. In the case of defense, incoming emails are scanned for known malicious hyperlinks or attachments that may contain malware. Rewriting URLs allows for tracking of potential malicious content.

ABOUT THE AUTHORS.

All Authors contributed equally to this article.

Dr. Keri Pearlson is the Executive Director of Cybersecurity at MIT Sloan (CAMS) research group.

Sean Sposito is a member of the Behavioral Engineering team inside the Paranoids, the information security team at Verizon Media.

Masha Arbisman is the manager of the Behavioral Engineering team inside the Paranoids, the information security team at Verizon Media.

Josh Schwartz is the senior director of Proactive Engineering inside the Paranoids, the information security team at Verizon Media.