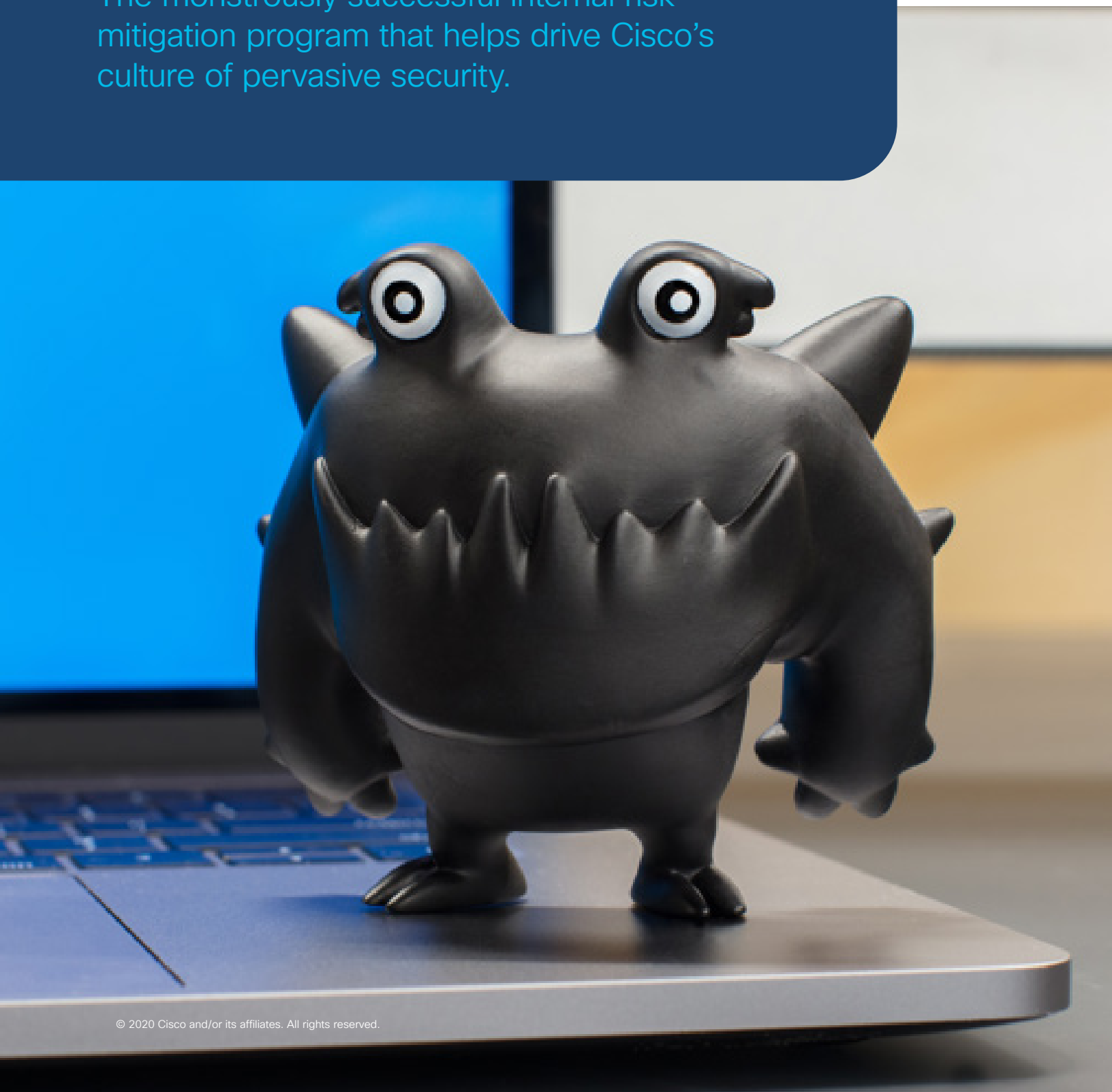
Keeping Cisco Safe

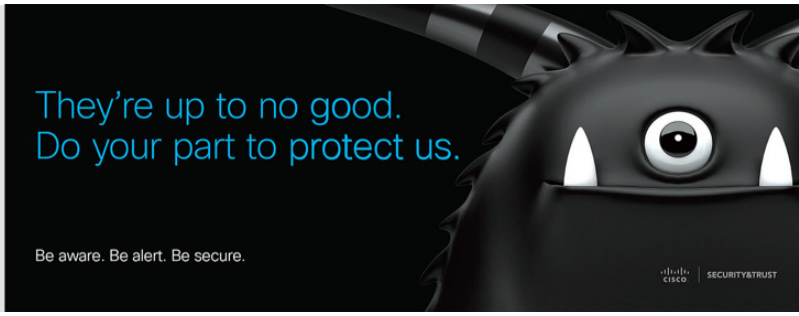
The monstrously successful internal risk mitigation program that helps drive Cisco's culture of pervasive security.



How do you get 130,000 employees and contractors to take personal responsibility for cybersecurity, data protection, and data privacy? For *Cisco's Security and Trust Organization*, the team responsible for mitigating risk and exposure for the company, it took creativity, a global village of security champions, and the help of a few "mischievous" monsters.

Program

A pervasive, interactive multimedia internal risk mitigation awareness and education program.



Objectives

Drive a culture of pervasive security to mitigate cyber risk and exposure.

Motivate the entire Cisco population into sustained action and behavioral change with regard to practicing good digital hygiene.

Introduce new methods for engagement and retention, including gamification, 1–2–minute videos and a rewards system.

Prove that security awareness and education can have an impact on cyber risk reduction.

Results

Gained widespread adoption, engaging more than 97,000 Cisco workers across the enterprise. Now acting as cybersecurity advocates for Cisco around the globe.

Increased companywide understanding of potential threats, good digital hygiene, and how to report a suspected cybersecurity incident.

Won the National Cyber Security Alliance's first annual award for cyber safety in the workplace.

Gold Winner of Info Security PG's Global Excellence Awards® Cyber Information Security Risk Mitigation Marketing Campaign.

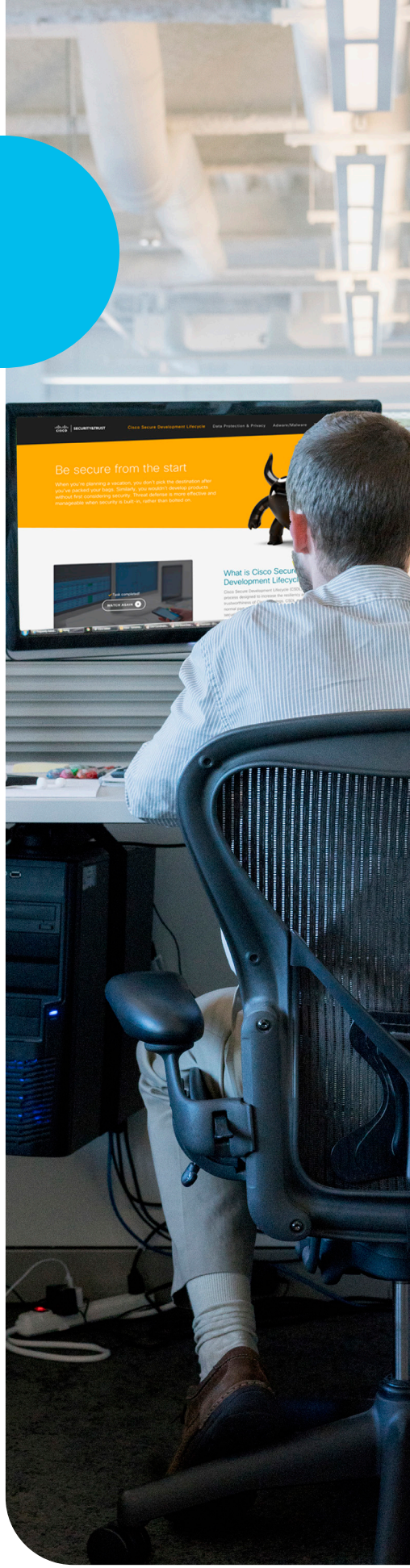
“Be aware.
Be alert.
Be secure.”

Technology alone can’t protect us from every cyberthreat. Often, the weakest link in a company’s line of defense is the human factor. According to the Ponemon Institute’s Cost of a Data Breach Report, “24% of root causes of a data breach is human error,” while retruster.com states that “90% of data breaches start with a malicious phish.”

Any workforce can easily fall for sophisticated and clever phishing scams. They unintentionally click a malicious link, unknowingly download malware or accidentally send confidential information beyond the firewall. That’s why, if you want to reduce your threat profile and mitigate risk to your organization, it’s critical to educate everyone inside your organization about the various types of cybersecurity threats you face and how to mitigate them. Your workers must not only be aware of the types of activities that can lead to breaches, they must understand your data security policies and be properly equipped and motivated to act on them.

As the Cisco Security and Trust team discovered, getting people to take time from their busy schedules to learn about seemingly dry topics such as phishing, and the data lifecycle is not an easy task. To solve the problem, they developed Keep Cisco Safe, an innovative internal risk mitigation awareness and education program. It combined out-of-the-box creative thinking, gamification, digital signage, a personalized rewards system including achievement badges and top-down executive sponsorship to change worker’s security behaviors. The goal was to drive a culture of pervasive and proactive security throughout the enterprise while creating personal responsibility and accountability towards the initiative.

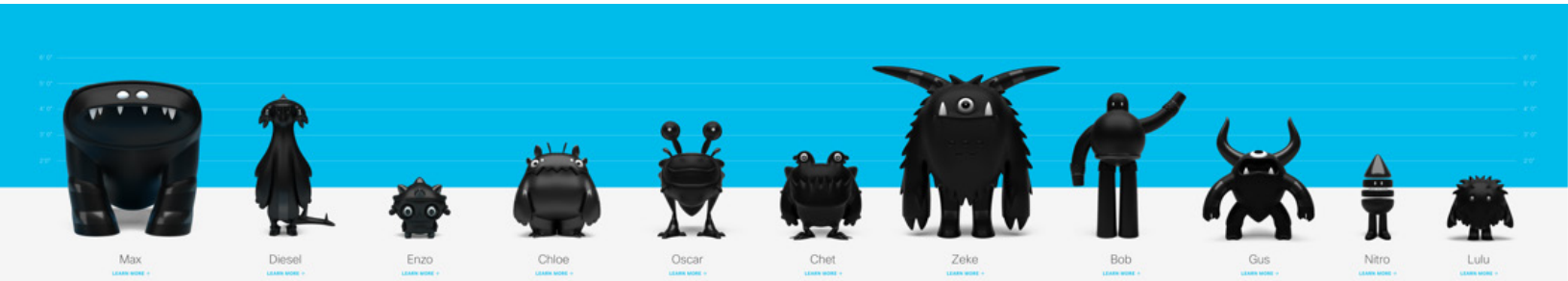
“The threats are real. Do your part to protect us.”



Cisco’s IT and InfoSec organizations have built a strong enterprise security foundation through technologies, policies and processes. But, to make security truly pervasive, people all across Cisco, including employees, contractors and partners needed to understand why and how to keep Cisco safe. Changing the behavior of an entire company is no small task. When Cisco’s Chief Operating Officer presented at a company meeting, the timing could not have been better. As they were kicking off their internal efforts, she told the entire workforce that “cybersecurity is everyone’s responsibility.” Upon hearing this, the team knew they were on the right track.

That onerous job fell to Awareness and Communication leads, Jeanne Hernandez and Marianne Currier. “It started as a compliance issue,” said Hernandez. “We knew that GDPR [the EU General Data Protection Regulation] was coming, so we needed to be prepared for the new regulations. We needed to educate people on how to report cybersecurity incidents and how to properly manage confidential and Personally Identifiable Information (PII).” The team also used the opportunity to educate workers and customers on the company’s commitment and accountability to security and privacy. “Cisco follows the practice of Privacy by Design,” said Currier. “We build security and privacy into our products from the ground up, so it was also important to communicate the value of the Cisco Secure Development Lifecycle (SDL).” Their ultimate goal, however, was to help the general Cisco population understand that it’s not just IT and Information Security’s responsibility to protect the network, but it was everyone’s responsibility to keep Cisco safe.

“While people naturally wanted to keep Cisco safe, it’s not like they were clamoring to be trained on policies and standards,” joked Hernandez. “We had to figure out how to make learning this critical material interesting to the workforce so that they would care enough to act on what they learned every minute of every day.”



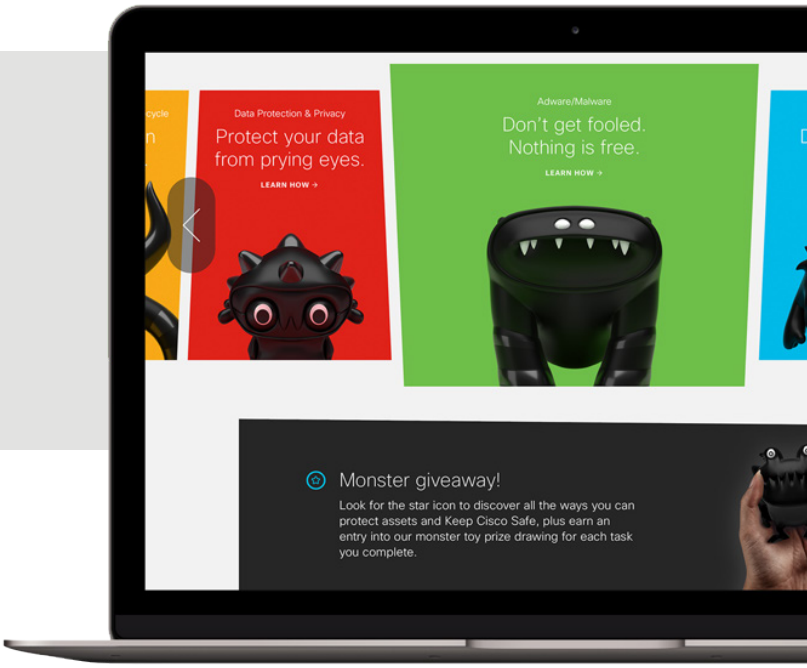
Cue the monsters

Given the challenges, the team knew that they needed to tackle them with a fresh perspective. “Images of keys and locks just weren’t going to cut it,” said Hernandez. “If we were going to break through the noise of all the other competing workforce communications, we needed breakthrough creative—something different enough from the Cisco brand to stand out, but professional and not so “off brand” that we wouldn’t be taken seriously.”

Once they pitched the creative concept to executive leadership and global allies, it was clear they had a winner. It was also clear that if they were to truly keep Cisco safe, they needed to ensure they were covering the topics that would have the greatest impact on risk mitigation. Cisco’s Chief Security and Trust Officer made it clear that the team would have to demonstrate the impact of any training and awareness program. So, the team worked with subject matter experts across the broader security community to identify the most important security topics, what they needed workers to know, and how they would measure success. The partnership of these subject matter experts was imperative to our success.

The program consists of five major topic areas:

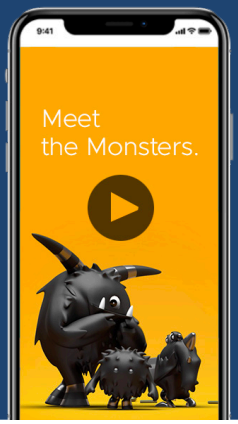
- Adware/Malware
- Cisco Secure Development Lifecycle (SDL)
- Data Protection and Privacy
- Multifactor Authentication
- Phishing



The team launched a dedicated website with each topic having a landing page, an intro video, training modules, and deeper-dive supplemental materials. The creative was deliberately more whimsical than the typical Cisco approach in an attempt to break the traditional mold.

Short videos worked best

The team conducted research to determine how to educate the masses. Did they want to sit in a classroom? Be self-taught? Would they like the information all together in a session of a few hours, or spread out in smaller increments? They discovered that people wanted to receive the data in 2-3 minute videos or 10-15-minute training segments, something they could knock off one at a time over several lunch breaks.

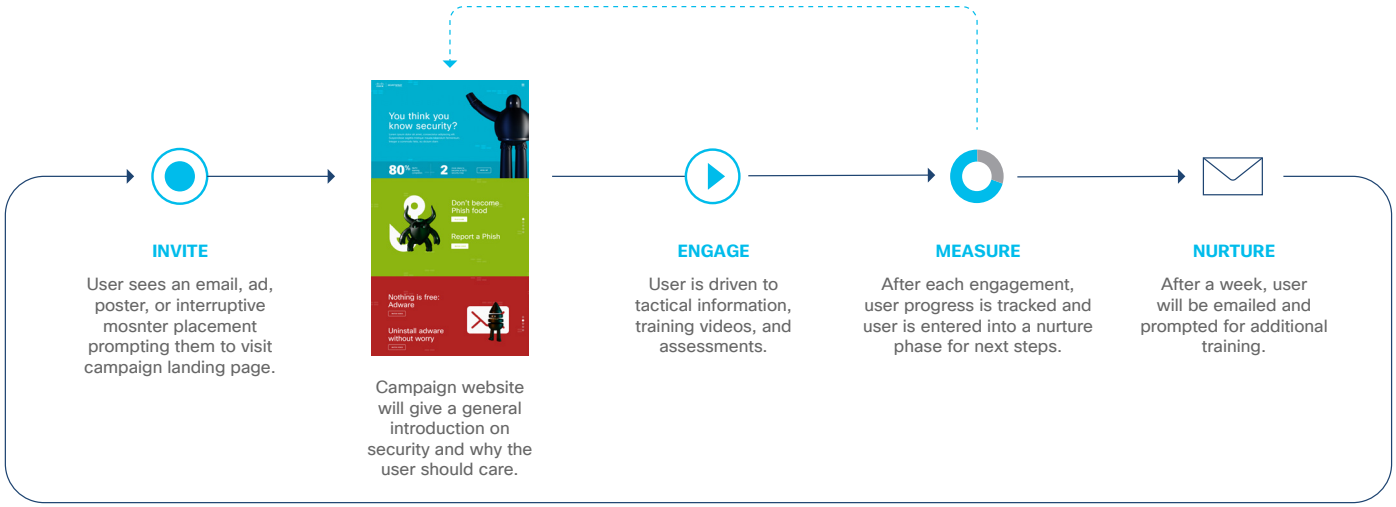


Now that the team had a comprehensive program, it was time to generate awareness and drive adoption. Being mindful not to spam the entire workforce with email, the team had to get creative on how best to spread the word and drive engagement to their new Keep Cisco Safe website. Their communication and change management strategy had two main components: a teaser campaign and executive sponsorship.

The teaser campaign

To generate awareness, the team created large monster cut-outs, window clings, posters, stickers, and small standups to go on people's desks. They used these physical assets as a teaser and a way to stop people and get them interested in learning more. The eye-catching monsters in building cafeterias, on the walls, on desks and elsewhere were coupled with statistics that got straight to the point—such as "81% of data breaches involve a weak or stolen password" or "The average cost of a breach is $3.92 million."

Then, they deployed a traditional nurture program to drive employees deeper into engagement through monthly email and digital signage campaigns. "We had to consider the digital aspects and how to engage the remote workforce who would not see all of the physical assets without a visit to campus," said Currier. The digital and physical program elements drove people to the website, where the team was then able to track those worker's actions and record who did what, how many



videos they watched or which training modules they completed. “For instance, we could see who completed what tasks and target specific groups with awareness and educational content they had not yet engaged in, to further increase adoption,” said Hernandez.

The creative monster assets turned out to be powerful motivation to keep workers moving through the program. People loved the monsters and began to ask the team for replicas they could keep. Capitalizing on that idea, the team devised contests to give away T-shirts and other monster swag each month, drawing 100 winners from everyone who had completed at least one training module. For the ambitious workers that completed all program tasks, the team rewarded those individuals with monster toy replicas made from recycled and biodegradable materials.

It took a village

Global dissemination of the physical creative assets posed a big challenge. After reaching out for global volunteers to receive the items in their regions, the team formed an ad hoc partnership with Cisco Women in CyberSecurity (CWiCS).

The group had formed several years previous and was a natural fit because they are located all over the world and had a passion for cybersecurity. With their help, the team was able to set up creative assets in over 81 Cisco buildings across 26 countries and still growing.

Executive buy-in and sponsorship

In addition to the creative teaser campaign and CWiCS partnership, the team leveraged security advocates from across the enterprise to help drive awareness within their organizations. While Hernandez and Currier didn’t have the authority to mandate that workers take the training, the leaders of each department certainly did. Most leaders immediately saw the value and urged their people to participate.

Getting executive buy-in was critical. It became clear that every time a leader showed commitment to the program via email or other actions, adoption spiked. “We could see which organizations were doing the training and which were not,” added Currier. “No one wanted to be on the bottom of the list so one by one, each department began driving adoption from the top down.” This provided further incentive for leadership to spread the word and create a spirit of friendly competition that kept up the momentum.

Moving the needle, making a difference

The team's two-pronged approach to generating awareness and driving adoption was a great success. The Executive sponsor, Cisco Chief Security and Trust Officer wanted to see real results, and the team had some exciting numbers to share.

"When we launched Keep Cisco Safe, we had approximately 1,800 people engage in the program within the first quarter," said Hernandez. "The numbers kept climbing, 3,000, 27,000. By the end of the third quarter, we had engaged nearly 55,000 workers."

While the worker's response to the program was certainly heartening, the real question was whether the training would ultimately change people's behaviors and decrease security risks.

"We developed a new process for reporting and managing data incidents," said Steve Sigel, Senior Manager, Data Protection and Privacy Response. The number of departments following this new process as well as the number of incidents being reported grew in direct proportion to the number of people and organizations who completed the training, clearly demonstrating increased awareness. "We were a lot less busy before the Keep Cisco Safe program was launched," joked Sigel.

"It's not that there were suddenly more incidents," explained Currier. "It just showed that we were bringing people's attention to and what they should be reporting." By reporting these risks, the response team has more visibility into potential dangers and can review the situation to determine whether they are dealing with a serious event that needs remediation.

Another mechanism for testing the success of the program—and providing another "teachable moment," was through the use of mock phishing expeditions. The team sent out simulated phishing emails and monitored how many workers opened them, how many clicked the links, and how many reported each email. "We saw dramatic improvement across the board whenever workers took the training," said Hernandez.

Overall, the program has significantly increased awareness of many security risks and how to take action to minimize them. “There are always new threats and regulations,” said Hernandez. “The security landscape is forever changing. Therefore, we need to stay ahead of the curve and make sure Cisco workers are aware of these changes and understand how to mitigate the risks.”

Making everyone safer

The Keep Cisco Safe program continues to evolve and grow. To promote good digital hygiene at home, Cisco recently launched the Keep the Cisco Family Safe Online program. They have also integrated the Keep Cisco Safe program into SecCon, their annual internal global security conference. They’re also introducing Keep Cisco Safe-as-a-Service as a way to scale and ensure consistent security messaging and best practice adoption as they grow their security portfolio and integrate acquisitions.

Cisco is sharing its success to help its customers and all organizations to understand the importance of launching their own cybersecurity awareness and education programs. “A side benefit of sharing our security best practices with customers is earning their trust,” explained Currier. “Security isn’t just something we talk about at Cisco. We’ve prioritized it and made it a part of our culture. It’s something we focus and act on every day.”

Winner of the NCSA Cyber Safety in the Workplace Award

Implementing and encouraging all employees to practice cyber safety is fundamental to helping an organization be safer and more secure. Cisco was selected based on its outstanding commitment to implementing and encouraging all employees to practice cyber safety and for fostering a culture of cybersecurity in the workplace.

Gold Winner of Info Security PG's Global Excellence Awards®

Cyber Information Security Risk Mitigation Marketing Campaign

These prestigious global awards recognize cybersecurity and information technology vendors with advanced, ground-breaking marketing programs, solutions, and services that are helping set the bar higher for others in all areas of security. Cisco was awarded the highest distinction with the Gold Award for its internal Cyber and Information Security Risk Mitigation Marketing Campaign - "Keep Cisco Safe."