Security Awareness at Unitil Corporation

An Inside Look at Running an Effective Security Awareness Program Using SANS Securing the Human End User Solution

Executives on the Front Line of Cybersecurity Awareness

The phishing email to the senior executive of Unitil Corporation was good. Very good. It appeared to come from a local district court relating to jury duty and was sent directly to the executive. He was, like all executives, very busy and pressed for time. The phishing email had an attachment attempting to collect personal information.

Despite being busy and distracted, which is a common situation phishers try to exploit, the executive did not click on the attachment. Instead, he immediately forwarded the email to the information security team and derailed the phishing attack. While the phishing attempt was good, the security awareness training program put in place by the Unitil information security team was better.

Such a vigilant response did not happen by chance. The executive's awareness was the result of thoughtful decisions and actions by the security awareness team at Unitil, a regional gas and electric utility based in Hampton, NH, to upgrade their security awareness program around the SANS Institute Securing the Human End User Security Awareness solution. The End User solution is a comprehensive security awareness training program that enables security awareness officers to efficiently manage human cybersecurity risk across diverse threat vectors.

The SANS Securing the Human End User solution enables security awareness officers to efficiently manage human cybersecurity risk across diverse threat vectors.

The Need

Like many of his peers, Jonathan Everett, chief cybersecurity officer at Unitil, had wisely invested in technical solutions to protect the organization and safeguard information. But he came to realize that such hardware investments are "really worthless if somebody has the keys to get in there." The organization had good success with creating awareness about private, personal identifiable information (PII) and it adhered to state and federal data protection laws. But Everett and his team realized that "it doesn't matter how much we spend on securing the systems, somebody who has those keys will be able to come right in and bypass all of that." So the team realized they had a gap that needed to be filled. The human side of cybersecurity was poised to play a critical role in the company's overall cybersecurity posture.

Beating the Spear Phishers

The team at Unitil noticed that spear phishing attacks were becoming more sophisticated and sometimes the spear phishers seemed to understand the organization and even the style of the different executives. By rolling out a comprehensive security awareness program in partnership with SANS Institute, the Unitil security team stayed one step ahead of the spear phishers as evidenced by two examples from the field:

Widespread Attacks Defeated

In early 2015 a barrage of nearly 80 spear phishing emails came into the organization at once to different departments across all parts of the company. The physical footprint of the attack spanned multiple buildings on the corporate campus. Having been trained in security awareness fundamentals and knowing what to look for, a significant number of people reported the attack soon after it started, which meant the security team was able to quickly check the mail server. The team could see where the attack propagated, alert people at risk, and successfully block the attack. Kimberly Hood, Unitil's data security compliance manager, noted after the attack: "If I hadn't had more than one person in more than one place report the situation, I wouldn't have realized it was a widespread attack."

Remote Employees Defend the Organization

In another example of the power of building a culture of cybersecurity, a Unitil employee working remotely who had just completed security awareness training had a suspicious email land in his inbox. The employee immediately suspected a phishing attack and reported the email to information security. The employee felt a sense of accomplishment for reporting the incident and the security team had a clear data point showing their awareness efforts were effective.

The Solution

Like many organizations, the workforce at Unitil is diverse and distributed - from field technicians to corporate executives spread across multiple states. And, like many organizations that are improving their human cyber security, it's a challenge to engage employees in both the larger program and specific training. Stephanye Schuyler, communications lead for the awareness program, noted, "One of the challenges we have is everyone is very busy, and getting some of their mind share can be difficult." Schuyler and her team were drawn to the SANS Securing the Human End User solution because:

> They (SANS training videos) have a reputation for being short and to the point, so people don't do the eye roll and say we're going to have to allocate an hour to do this. They can click on the video, they can view it, they can do the test, they can learn something and then they can move on to another task on their desk.

Everett echoed Schuyler's point when he added, "These quick hit videos actually make a very dry subject interesting and engaging. And that's really been the key to success for the program." The Unitil team also noted that a key factor in their success has been the Security Awareness Program "Cookbook" that SANS provides to its clients.

"Another thing that I really appreciate about the SANS program is they give you a cookbook on what to do."

The Security Awareness Program "Cookbook"

When discussing the challenges of building a program from the ground up, Schuyler made a point of mentioning the benefit of having a solution that is holistic rather than piecemeal. "Another thing I appreciate about the SANS program is they give you a cookbook on what to do. It's not 'here are the videos, now go and do it.' There are instructions on how to put together a program, and a guidebook on how to manage the program, which I found very helpful."

Schuyler makes generous use of the templates to inform strategy, set direction and help in scheduling. She added that "it really is an entire process guideline which helps us to better utilize the videos and newsletters." And the guidance from a "cookbook" comes in handy when dealing with the detailed nature of compliance where having a vetted solution makes life much easier for the compliance team.

Compliance Made Easy

Unitil's manager of data security compliance, Kimberly Hood, knows all too well the burden placed on organizations by compliance and regulatory requirements. Unitil must follow federal, state and industry regulations which make it challenging to keep up with the codes, requirements and audit windows. "We have a lot of different bodies that are looking at us," said Hood. She was appreciative of the deep industry experience that anchors the Securing the Human solution. "A lot of folks on SANS staff have either come from the regulatory environment or from our industry, so they understand what regulators are looking for and what needs to happen in order to be compliant." And one way to make compliance easy, and take your program to the next level, is to perfect program reporting. Auditors don't want to be told you're compliant, they want to be ***shown***.

> "This isn't some homegrown program, this is something that has a lot of years of experience and knowledge behind it and a respected name."

Doughnuts at Zero Dark Thirty: Lessons from the Front Line of Awareness Training

Stephanye Schuyler and Kimberly Hood outline what they've learned rolling out an effective security awareness program, including chilly pre-dawn chats over coffee and doughnuts with line employees.

1. **Set up a steering committee** - One of the first things Schuyler and her team did was get cross-functional input through a steering committee.
2. **Identify at-risk departments** - Get feedback and enroll those teams that are most vulnerable.
3. **Launch a pilot** - Partner with a few departments to see what employees think of the program and what their acceptance is of the proposed program.
4. **Meet employees where they are** - Hood and Schuyler got up at "zero dark thirty" and met line workers in the field to bring security awareness training to the front lines.
5. **Teachable moments beat gotcha moments** - Instead of chastising employees for clicking on a phishing email, Schuyler and her team used the event to celebrate the fact that the employee alerted IT and to reinforce the desired behavior of sending suspicious emails to IT before clicking.

Measurement Matters

In many ways compliance is about documentation and proof. Proof that an organization followed procedure. Proof that an organization deployed the right content to the right employees at the right time. The best way to have proof is to have a management platform that makes it easy to generate reports documenting compliance. Hood, the compliance manager, spelled out the power of having easy proof and documentation through the SANS End User program:

> If we get called upon and they (regulators) say, "I want to see evidence of your training program. What have you done? Who's taken it? What are your percentages of who completed what and when and all of that?" Then those reports are at our fingertips. I don't need to go and compile something at that point.

Easy and powerful reporting is the byproduct of a robust measurement and management system. You have to have metrics and systems in place to measure those metrics in order to report on them. And nowhere does great measurement matter more than when it comes to actually changing behavior. The best way to modify behavior is to show the old way doesn't work and the new way does work.

Better Behavior Change

Unitil is working hard to foster more secure employee behavior, not just check the box that teams have completed training. They are maturing from measuring knowledge and knowledge retention to measuring behavior change. Unitil uses the SANS Securing The Human phishing solution and the number of emails proactively sent to IT as possible phishing emails as one indicator of behavior change in the right direction. Hood noted that "… I definitely see an increase in how many people are sending me emails they're concerned about." But great security awareness programs are much more than just phishing awareness - they are end-to-end and comprehensive. Schuyler and Hood took advantage of the templates, tools, and program support assets provided by SANS to move beyond just phishing. Schuyler pointed out:

> We use all of the back-end reports…and one of the things that SANS has provided is a questionnaire, which has been helpful and we use it every year to measure risk. So it really is an entire process guideline, which helps us to better utilize the videos and the newsletters.

And the back-end data is also showing the security team where to focus for behavior change. For Unitil, the measurement and reporting capabilities help answer three key questions when it comes to zeroing in on the right behavior change:

1. What teams are we having more phishing issues with?
2. What groups do we need to focus more on?
3. What kinds of emails are employees having trouble deciphering as a phish, versus which ones are easy for them?

How does a security team make the case for investing in awareness training?

Bringing in a Cost-Effective Solution

Making the Case for an Awareness Program in General

For Unitil, the first step in addressing the human side of cybersecurity was to make the case for a security awareness solution. Like many organizations, the company historically spent a much larger portion of the IT budget on servers and hardware. Everett, the chief cybersecurity officer, noted that the buying hurdle tends

not to be as high for awareness training as it is for enterprise infrastructure components, for example. He reiterated his point about how, regardless of the amount spent on hardware, humans historically represented the weakest link and biggest vulnerability in their cybersecurity approach. Relative to a hardware acquisition, Everett noted that "the SANS program and licensing was quite reasonable and that made it much easier to get involved." After making the case that dedicated budget was needed to focus on managing human risk, Everett and his team shifted to looking for the best security awareness solution for their needs.

> "It's probably the most cost-effective solution when it comes to preventing malicious activity issues."
> Jonathan Everett
> Chief Cybersecurity Officer,
> Unitil Corporation

Making the Case for SANS Securing the Human End User

Many companies are faced with a make or buy decision when it comes to awareness products. For Schuyler, it was an easy choice. "Why make when you can buy from the people who are the experts and this is what they do every day?" Everett summarized the most compelling reason for selecting SANS Securing The Human:

> Cybersecurity is something you have to keep front and center with people; you can't just do it once and then be done with it. And so with an outside entity such as the SANS Institute, which is very well respected with a good program, when we saw that, that was the 'ah-ha' moment. And we jumped in and said, "This is exactly what we've been wanting to do for quite some time."

What's Next

The team at Unitil is just getting started in their journey building a more secure workforce and organization. The team is bolstering their onboarding process for new hires to put more information in front of new employees on day one. They're soliciting more feedback from employees and calibrating the phishing program to achieve just the right level of difficulty to engage employees while making them more aware. The team continues to identify departments that need special focus. And, they continue to engage all employees, especially senior executives on the front lines of defending the organization against increasingly sophisticated threats.

So a fake district court jury summons isn't enough to get through Unitil's human cybersecurity defenses. Schuyler put it best, "Our senior executives have become more expert in forwarding spear phishing attempts, especially the fund transfer requests. Because of the cybersecurity training, we've become more sophisticated than the spear phishers."

About Unitil

Unitil provides energy for life by safely and reliably delivering natural gas and electricity in New England. Unitil Corporation is a public utility holding company with operations in Maine, New Hampshire and Massachusetts. Together, Unitil's operating utilities serve approximately 103,300 electric customers and 78,700 natural gas customers. The Company supports the development of strong, successful communities through investments in its infrastructure as well as local economic and community development programs.

About SANS Securing the Human

SANS is the most trusted and the largest source for information security training in the world. With over 25 years of experience, SANS information security courses are developed by industry leaders in numerous fields including cybersecurity training, network security, forensics, audit, security leadership, and application security.

SANS Securing the Human provides organizations with a complete and comprehensive security awareness solution enabling them to easily and effectively manage their human cybersecurity risk.

SANS Institute has worked with over 1,300 organizations and trained over 6.5 million people around the world. Security awareness training content is translated into over 20 languages and built by a global network of the world's most knowledgeable cybersecurity practitioners. Organizations trust Securing the Human content and training is world class and ready for a global audience.
