FORTRA

The Future of Security Awareness

THEO ZAFIRAKOS, CISO AT FORTRA'S TERRANOVA SECURITY, ON MODERN AWARENESS PROGRAMS

iSMG
INFORMATION SECURITY MEDIA GROUP

Theo Zafirakos

Zafirakos is a CISO, trusted cybersecurity adviser and expert in security awareness strategy, governance, privacy and more. He works with security leaders worldwide to help identify, evaluate and manage security awareness strategies that align with their organizational objectives. He's responsible for internal cybersecurity policies and awareness initiatives at Fortra's Terranova Security and leads the professional services team in implementing and executing personalized security awareness training campaigns. He also helps organizations assess their security awareness training program's success with actionable metrics that facilitate long-term optimization and growth. Before joining Terranova Security, Zafirakos spent 20 years at Canadian National Railway, a leading North American transportation and logistics.

Security awareness training programs are maturing as security teams recognize the need to secure the "human element" of cyber risk. But in the face of more sophisticated attacks using MFA bypass techniques, advanced persistent threats and generative AI, it's time for organizations to create more tailored education programs.

"Generative AI not only adds to the complexity in the terms of risks and threats like advanced social engineering, malware creation, scenarios that have been tailored to the audience - vishing over the phone, phishing their text with automated responses," said **Theo Zafirakos**, CISO at Fortra's Terranova Security. "Now we have to make our users be smarter than artificial intelligence and be able to detect a fake audio of the president asking you to do something."

Zafirakos advises cybersecurity organizations to partner with the business to promote a cyber-aware culture, not just one-off training. And the C-level needs to embrace the program for it to be truly effective. "We need to have proper ambassadors within the different departments that are not necessarily cybersecurity experts but understand cybersecurity and also understand the business," he said.

In this audio interview with Information Security Media Group (see audio link below photo), Zafirakos discussed:

- The state of cybersecurity awareness training and the sophisticated threats enterprises now face;
- Strategies for creating modern awareness programs and a culture of security;
- The latest training techniques for measuring success and benchmarking potential problems, such as the annual Gone Phishing survey by Fortra's Terranova Security.

Cybersecurity Awareness

TOM FIELD: How would you describe the current state of cybersecurity awareness?

THEO ZAFIRAKOS: Cybersecurity awareness varies by organization and especially by organization size. In recent years, there's a higher awareness of the need for investment for cybersecurity, and organizations are investing a lot more resources in buying services and hiring people to do cybersecurity. That tends to happen in large organizations and a bit less in small organizations as they're trying to catch up.

Organizations also have more comprehensive, all-inclusive security awareness programs. They have established a certain level of maturity in cybersecurity controls and procedures, and now they're starting to focus more on the human element, on the people. Organizations now may have regular training instead of just one time upon hiring and may provide best practices, going down to specific procedures like: Here are the instructions for reporting a phishing event. A lot of organizations did not communicate that in the past. But now they're putting more proactive and complete awareness programs in place.

Everybody's purchasing the latest and the greatest tools, and with that comes the increased need for cybersecurity awareness. We can't adopt two-factor authentication without explaining to our users the risks associated with two-factor and the different attack tactics that cybercriminals may use with these tools because as we know, the criminals adapt. The more technology that we use, the more targets that they have in place.

There is also a need for regulatory compliance. There are a lot of new laws coming into place,

“Getting users to change their behavior is very difficult. Even if a user can detect a phishing message in training, in a real-life event where they’re distracted, they may not remember their training.”

especially for privacy and cybersecurity across the globe. That increases the need for organizations to implement cybersecurity awareness programs and educate their staff.

Awareness Challenges

FIELD: Why is awareness such a complex challenge for enterprises?

ZAFIRAKOS: Large organizations that have the resources and investment struggle because they also have a large and complex environment. They may not have full visibility on all their users, and also they are high-value targets because they have a lot of data, resources and money. And they’re dealing with users that have a lot more different profiles, risk levels and needs for training. Small organizations may suffer because a lot of times they think they will not be a target. They think that we’re too small to be targeted, but that is making them an even more attractive target because everybody has something that cybercriminal organizations are looking for.

Resource constraints are another issue. Cybersecurity awareness programs tend to fall off the priority list. When we start cutting budgets, awareness and training is one of the first things to go. Organizations also may suffer with being able to demonstrate the benefits of cybersecurity, such as, “How do I demonstrate that it was because I trained my users that they did not click?” Organizations need to measure the effectiveness of the program and justify why they are asking users to spend one or two hours per year on training. Getting users to change their behavior is very difficult. Even if a user can detect a phishing message in training, in a real-life event where they’re distracted, they may not remember their training.

Generative AI

FIELD: How does generative AI add to this complexity?

ZAFIRAKOS: Generative AI not only adds to the complexity in the terms of risks and threats like advanced social engineering, malware creation, scenarios that have been tailored to the audience - vishing over the phone, phishing their text with automated responses. Now we have to make our users be smarter than artificial intelligence and be able to detect a fake audio of the president asking you to do something. How are you supposed to know that when AI is becoming so much better because the business asks it to be better?

The use of AI for legitimate business purposes is also a concern. Organizations are implementing policies completely banning AI until they’re ready to adopt it. What are the acceptable use cases? When is it OK to use AI within organizations,

and what are the concerns around data privacy and data handling? Do we upload confidential or personal data on AI cloud, which is going to use it after to learn and become smarter and incorporate our data?

Regulatory compliance is going to come around AI. So, especially for federal agencies, governments have started putting in place when it is acceptable and not acceptable to use AI. And as for employee interaction with AI, we can tell employees what they can and cannot do, but we know that it's going to pique their interest. They're going to use AI. So, how can we provide them proper training on how to securely use AI, taking into consideration privacy, ethics and making sure that we have proper oversight on the use of AI?

Top Threats to Organizations

FIELD: What are the threats of greatest concern to organizations today?

ZAFIRAKOS: Third-party ecosystems are a top priority for many organizations. Statistics show that a large number of organizations work with third parties, and they have potentially experienced an attack that has originated from a third party. Several of our clients have taken the time to sensitize and train their users on ransomware, but when an attack came in from a third party, no one was prepared for it because this person had access to the network and the system.

How can we extend cybersecurity awareness to those third parties? Organizations may be dealing with mature third parties that have mature security programs, but many others are dealing with smaller entities that may not have such an investment in cybersecurity. So, third-party risk

– especially in the software product, application, technology, supply chain – is a high priority.

There are also advanced persistent threats, which are typically carried out by sophisticated attackers. They want to get a foothold on the network and the systems, and they want to go undetected for as long as possible. We have even observed persistent threats that had taken a foothold and were patching the system's other vulnerabilities so the administrator wouldn't go in and see something was going on. They were keeping their gate open and patching everything else. That is typically done for corporate espionage, stealing data or intellectual property and in some cases causing damage, disruption, fraud or financial threat.

Attackers will use the traditional methods of phishing, zero-day exploits, malware and social engineering, but getting in through the employees of the organization has become the easiest way. Once they're in, they can do lateral movements, look at other applications and systems that may have vulnerabilities and get a foothold. Organizations have to up their security program, especially with threat intelligence and exchanging information with their colleagues, peers, cybersecurity groups and even their governments to know how to detect those indicators and prevent them. They need to have proper network and system hygiene, patches, firewalls and tools in place, but they also need cybersecurity awareness because cybercriminals are going to use the human element to get in the door.

A Culture of Security

FIELD: How do you build a culture of security that can last?

ZAFIRAKOS: When we talk about culture of security, we're talking about the ideas, perceptions and feelings that individuals have about cybersecurity. It's not just a technology or an IT thing. We have to start from the top with the executive leadership. We have to lead by example, and we have to be able to show that this is important across all levels of the organization. Also, business areas have to take cybersecurity into consideration. When we are adopting new tools, technologies and business ventures or ideas, we need to think about cybersecurity and the potential risks associated and explain those to the team that is responsible for software and system development. Say, "These are the concerns that we have. Can you make sure the system that we put in place addresses these issues and risks?"

Also, a lot of organizations have an IT and a help desk department. People often call there when they have problems. Use that group as an awareness moment or an awareness point of view. If a user calls in because they have a virus, take the time to explain to the user how the virus got in. Ask them if they went to a malicious website or used a foreign USB key. There is education across all departments and levels. It's not just at the very end. We've been taking decisions from the very beginning, and those accumulate to the end users who have to use the systems and applications. We put the burden on them. Let's look at all levels of the organization.

Awareness Program Players

FIELD: Who needs to be included in creating and sustaining a modern awareness program?

ZAFIRAKOS: First is the learners. The people in your audience have to be engaged and interested in learning. Organizations are starting to expand their training. It's not just for the employees anymore. They're training their clients because the clients may have access to systems or data. They want to minimize the number of times their clients get breached or cause incidents.

In the education sector, we see a lot of schools, universities and colleges focus on their students. What better place to train the next future workforce than the universities? They come out of school, get a job and know about cybersecurity even before they get in the workplace. There are also the third parties. But in order to reach those groups, the responsibility cannot fall just within the IT department.

The IT department understands technology, cyber and risk, but when we want to change people's behaviors, we need a change management team and a change management approach. How do we reach that ultimate goal? We need to have proper ambassadors within the different departments who aren't necessarily cybersecurity experts but who understand cybersecurity and also understand the business. They can act as a two-way communication channel between cyber and the business, explaining the benefits and the risks.

Marketing groups, marketing departments and communications departments are great at crafting messages with impact that grab the audience's attention. If you have access to individuals trained in the behavioral sciences and psychology, they can help. And your HR department or labor relations is a very critical component if you're dealing with a unionized environment because now we are asking individuals to take some time away from their regular day to complete this training. They're nonoperational, so include those groups as well.

Topics for 2024

FIELD: What topics need the most attention in 2024?

ZAFIRAKOS: Our clients want to talk about the importance of cybersecurity, so we're addressing why we need to have a cybersecurity-aware culture. What does it mean to you? What does it mean to the future of your organization? What does it mean to the future of you having a job?

We explain the potential risks to the users and we discuss being able to detect the new levels of attacks that use AI for deepfakes, voice cloning and image cloning. That is becoming a lot more sophisticated, so the users have to know about it. We talk about the acceptable and secure use of AI tools, the associated risks and the risks related to third parties.

As more users and organizations are adopting multifactor authentication, we talk about QR code threats, alternative login methods and password managers. Passwords are being used less, but they're not going away yet. Since we'll use them less often, we won't remember them when we need them. So password managers are a topic of interest.

Measuring Success

FIELD: How do you measure the success of your program?

ZAFIRAKOS: It's important to measure the success of your program to know if it is effective, where it needs improvement and how to justify to the business leaders why you need to continue investing. The program manager is responsible for doing that. We always recommend that our clients have an evaluation every 12 months and identify some metrics. For example: What are my phishing simulation metrics? What am I looking at? Am I looking at click rates, password submission rates or open attachment rates?

How about reporting rates? How many people are taking time to report? The same way that it takes one click to infect a network, it takes one person to report a catastrophe. The SOC team is able to implement controls, so know where you're starting from, where you want to go and where you are at any point in time by measuring that data.

Also, look at your training metrics and your course completion and success rates. That will demonstrate whether your users are engaged with your training program. Are they interested? Do you start off strong? As time progresses, if the participation drops, it means the users are losing interest. You have to reverse that trend, and you an only do that by monitoring.

Incident tracking is interesting, but you have to make sure that you capture the right data at the time of the incident to be able to identify if you could have prevented the incident with proper training. Also, was the impact of the incident minimized because of proper training? Have this data and have those questions at the time that an incident happens.

Behavioral changes and indicators are a bit more difficult to track. It may take some additional tools and technologies, like user behavior analytics, to see how users are conducting themselves on the internet and using technology. We recommend soliciting feedback from your users. Once they complete an activity or complete a yearly training, get their input. If you make adjustments to the program based on their feedback, they'll know that their voice is heard and that you're taking their needs into consideration when you're building your program.

Questions to Ask

FIELD: What questions do our attendees need to ask about their awareness programs and cultures? What do they need to take a measure of?

ZAFIRAKOS: Look at your program to see if it's working. Is it engaging? Is it relevant to the audience? Do you have the right metrics? Are you communicating well to the users in a language they understand? Are you communicating the proper risks or just throwing out information for the sake of communicating? Check if your program is up to date with the latest trends. Does it cover the new techniques? You could hammer phishing year after year, but phishing tactics evolve. Evolve your training to cover that. Bring it up to date.

> “Make your training all-inclusive, region-specific and specific to the language of the learner, especially when you’re talking about cybersecurity concepts. Information is better learned when the program is delivered in the native language of the learner.”

Make your training all-inclusive, region-specific and specific to the language of the learner, especially when you’re talking about cybersecurity concepts. Information is better learned when the program is delivered in the native language of the learner. Show that management is leading by example and taking the training too. Make sure you have a feedback mechanism. Do you have a regular cadence for collecting feedback and verifying your program?

Is your cybersecurity awareness program properly aligned with your cybersecurity strategy? Review your strategy, align your strategic objectives with the human element and demonstrate how your awareness program supports your overall cybersecurity strategy.

The Terranova Security Approach

FIELD: How does Terranova Security help its customers usher in the future of security awareness?

ZAFIRAKOS: The landscape of cybersecurity is changing, and it’s going to continue to change. Cyberthreats are going to become more challenging and sophisticated. Large organizations may have more resources for these threats, but small organizations are becoming more aware and interested, and that’s where we come in. We can help organizations of all sizes and all sectors by putting emphasis on ongoing education awareness and teaching users best practices. We also help them adopt a security-aware culture that is suitable to their organization’s risk profile. Not every organization has the same risk profile. Not every user has the same risk profile. So how do we put a program in place?

We also help organizations by providing the annual Gone Phishing Tournament. This event takes place in October, and anyone, whether they are our clients or not, can participate and receive a benchmark report that shows how their employees’ behavior compares to the industry and to others. The 2023 report is available for download on our website, where you can register early for next year’s tournament.

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 36 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

(800) 944-0401 • sales@ismg.io

BANK*i*NFO SECURITY® • Just for Credit Unions CU*i*NFO SECURITY® • GOV*i*NFO SECURITY® • HEALTHCARE*i*NFO SECURITY®

*i*nfoRisk TODAY® • CAREERS*i*NFO SECURITY® • Data Breach® Prevention. Response. Notification. TODAY • CyberEd.io

CIO.inc • DeviceSecurity.io • PaymentSecurity.io • FraudToday.io

CYBER THEORY • CyberEdBoard • Xtra mile LIFECYCLE MARKETING • GREYHEAD

*i*SMG
INFORMATION SECURITY
MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io