THE HUMAN READINESS COMPANY
CYBEREADY

THE INSURANCE INDUSTRY: SAFEGUARDING SENSITIVE DATA

Possessing a wealth of confidential data has placed the insurance industry squarely within hackers' sightlines. In these large, often geographically-distributed organizations, the best line of defense continues to be maintaining the most well-trained employee base.

Imagine a veritable treasure trove of highly sensitive data that belongs to individuals and companies across a variety of sectors and geographic locations. This is the insurance industry.

Handling such confidential information, which includes a range of data, such as financial histories, personal assets, health conditions and histories, requires the utmost care. In an industry where data is required to be stored for decades, security professionals are wary of the dangers that phishing presents. Cyber criminals are making nearly constant attempts to breach systems.

Their goals could involve one of three disaster-level scenarios:

- the theft of confidential information, in order to ultimately profit from its on the Dark Web to the highest bidder;
- gaining control of an authorized workstation or credential, in order to remain unseen while sabotaging processes over a longer period of time;
- or maliciously disrupting or disabling operations, either for financial gain via ransomware, or to destroy entire businesses.

In the first (and most overt) scenario, a theft occurs and damage is done in the blink of an eye—often well before security professionals have a chance to identify the threat, let alone respond to it. The second, more insidious effort provides criminals with 'a man on the inside,' enabling fully authorized access for hackers who are operating behind-the-scenes. If undetected, they can spend months or even years successfully siphoning off funds via seemingly legitimate payment transfers, or collecting and distributing actionable business intelligence from executives' confidential correspondence.

Last, but not least, hackers are eyeing the insurance industry as a means for total takedowns. Hackers are well aware of the fact that insurance companies must answer to governmental regulators as well as to their customers; preventing or even delaying operations for the latter, which often must occur within a precise timeframe, brings them into unbelievably hot water with the former.

THE INSIDE STORY: MITIGATING AN EVER-PRESENT THREAT

An executive who leads security efforts from the Office of the CIO at Ayalon Insurance knows that such exposure to hackers could lead to total catastrophe within seconds.

It's a battle of good versus evil taking place on a daily basis, although it's not occurring among skyscrapers in a modern metropolis as in some superhero comic; rather, it's within the encrypted servers and many workstations that contain individuals' most personal data.

As headquarters manager, Ronen Ahuvia is responsible for defining comprehensive processes and secure assessment methods to ensure that operations continue to run smoothly, in addition to developing a budget for the department. He leads a small team that includes a team lead and two personnel, who monitor alerts, check employee logs, and provide critical insights on system capabilities and demands in accordance with the company's evolving security needs.

He smiled as he acknowledged the fact that his work, and that of his team, is never truly finished. Within their purview are roughly 1400 employees and a global network of 5,000 insurance agents.

> **"It's a battle of good versus evil taking place on a daily basis."**

It's important to note that effective training against phishing is only one method of dealing with the threats inherent to the insurance industry; adding to that are many other efforts put forth to protect data and systems. It just so happens that phishing remains one of the most most prevalent and devastating methods of attack for companies like Ayalon Insurance.

THE CHALLENGE: TRAINING FOR THE MOMENT OF TRUTH

"In the past year, we've come to understand that it really doesn't matter how many technology tools or system safeguards we have in place to defend ourselves; identifying a threat will ultimately fall upon a human being's shoulders, every time," Ahuvia explained.

"The firewall and antivirus blocking software we've put in place will work, of course," he added. "Eventually, however, if a hacker wants to find a way in, then he or she can by baiting our personnel in ways that unknowingly grant access to these criminals."

Ahuvia underscored the employees' critical role on the company's frontlines of defense.

"We need our employees to understand that they play a very significant part in this effort. They need to comprehend that in everything they do—in all work-related actions they take—they must bear in mind that a pervasive threat exists. Someone always wants to harm the company."

The threat could be as innocuous as an employee receiving a routine-looking email with what appears to be an official payment request; if he or she doesn't think twice, it could set off a chain of events that puts resources and data into the wrong hands.

"Because email is so important for everyone's work—it truly is the main tool for communication in our company—the possibility that you could receive a fraudulent email and act upon it is very real," Ahuvia said. "We want to find ways to make our employees even more aware of this threat, not only so that they're vigilant, but so they know how to deal with it."

"If a hacker wants to find a way in, then he or she can by baiting our personnel in ways that unknowingly grant access to these criminals."

When they began seeking a solution a year and a half ago, Ahuvia and his team evaluated a number of companies.

CybeReady stood out for several reasons, he said.

“First, they proposed a fully managed service; this meant that they’re handling everything in terms of running the simulations to generating reports. That level of attention isn’t something that any of their competitors offered.”

Ahuvia felt that the CybeReady team’s approach to training also offered a much more holistic solution that would actually change employees’ behaviors for the long term.

“CybeReady seemed to truly understand that in the end, this is a business threat; not a technological one,” Ahuvia said.

“Other company representatives we spoke with explained to us how they deal with the threat technologically, yet the real problem of learning and awareness involves the weaknesses inherent to the human mind. We are not machines; if something looks intriguing and feel safe, we respond accordingly. Especially in work environments, employees tend to feel as if they’re being looked after—so what could be the harm in trusting an email that looks extremely legitimate?”

Secondly, Ahuvia noted that while others offered sophisticated or smart tools, in the end they were just tools. "The CybeReady team possesses knowledge of what factors actually tempt people to take action."

Timing is another critical component that sets CybeReady apart from other phishing training services.

"If everyone in the company or even a specific division receives the same email at 8am, they know it's a phishing scam (or a training exercise)," Ahuvia explained.

"CybeReady cleverly intersperses its phishing campaigns, targeting smaller populations within the company at varying times of day and days of the week."

Last, but certainly not least, is the quality of education itself. "Another great advantage, from my perspective, is the ability to clearly and concisely explain to the untrained user what phishing entails," Ahuvia said. "CybeReady explains very well what the person did wrong via a learning page that appears when an employee clicks on a simulation."

THE RESULTS: BUILDING A STRONGER CHAIN

Once Ayalon Insurance began working with CybeReady, it was clear to Ahuvia that his staff were being tested using a very sophisticated, covert approach.

"They're doing an excellent job sending emails that are very hard to resist clicking on," he said. The results speak for themselves.

"CybeReady's learning pages are very effective," Ahuvia noted. "By the statistics, we can see that people are paying attention; they're reading the material. As for their performance in the simulations, it's definitely improving over time. We can see very clearly that people are much less likely now to click on a phishing scam than they were before we began working with CybeReady. In fact, we can see that those who used to click on almost every phishing email they received have done a complete 180—they don't click anything now."

The reaction of Ayalon Insurance's staff to the phishing campaigns surprised Ahuvia.

"Honestly, I thought they might be a bit angry if we succeeded—if they clicked on a simulation and we caught them doing something 'wrong'," he said. "You know, along the lines of 'what is this, surveillance?' But they like it. We're getting emails from people saying that this was a great simulation; I fell for it, but it was a good one! The engagement level is remarkable."

When a real threat arrives, Ahuvia knows that Ayalon Insurance employees are now better equipped to handle it.

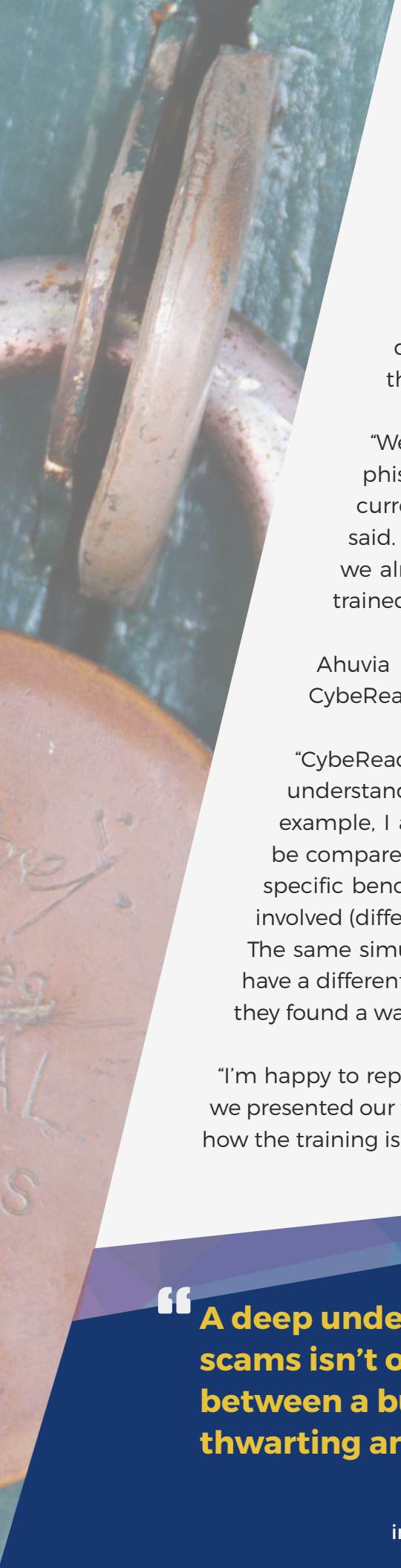
"We received a very vicious email, which came through all our defenses right into the mailboxes of hundreds of employees," he said. "It took us three to four hours to understand the magnitude of this threat and to locate and delete all of the emails—so we didn't have time to send a companywide announcement, which may have been more confusing than helpful. You can't announce until you know it's one person or one thousand who received it."

"We later understood that if someone clicked on the attachment, it would've been very bad. Yet nobody clicked. Not one! And we had many employees calling our security team to notify us of the suspicious email. It made it clear to us that CybeReady's efforts were a success."

> **"[We] firmly believe that CybeReady's approach to timing is paying off at Ayalon Insurance."**

Ahuvia firmly believes that CybeReady's approach to timing is paying off at Ayalon Insurance.

"Because the simulations are spread throughout the year, spanning different times of day, our staff doesn't get inundated," Ahuvia explained. "Even better, the simulations arrive when they're not suspecting it. Employees don't see it coming, and they're caught off-guard. Then, whenever a learning page pops up, they're reminded of what to look for; but it doesn't interfere with their day-to-day work."



THE ROAD AHEAD: OPERATING WITH A BIG ADVANTAGE

In cyber security, staying on top of the latest trends means having a distinct advantage over hackers. A deep understanding of the most recent phishing scams isn't only helpful; it could mean the difference between a business being vulnerable or successfully thwarting an attack.

"We've found that the CybeReady team is very knowledgeable about phishing scams happening all around the world; they're bringing current practices to us before they're arriving in our inboxes," Ahuvia said. "When we hear of an attack that happens, we want to know that we already simulated it here and that people are not only aware, but trained to handle it."

Ahuvia values honesty as well as flexibility in business transactions. CybeReady's team apparently possess both.

"CybeReady's expert team is a very honest and accommodating. They understand our needs and are flexible with our requests," he said. "For example, I asked them for a benchmark regarding our performance might be compared with other companies. They worked to create a legitimate and specific benchmark, which is not a straightforward task with all the variables involved (different simulations sent at various times, in different languages, etc.) The same simulation can be deployed at one company earlier in the year and have a different score than if it appears later in the year in another company. Yet they found a way to control for these items."

"I'm happy to report that we scored very well on the benchmark—so much so that we presented our findings to Ayalon Insurance's management team to demonstrate how the training is working. Our efforts are getting results."

"A deep understanding of the most recent phishing scams isn't only helpful; it could mean the difference between a business being vulnerable or successfully thwarting an attack."