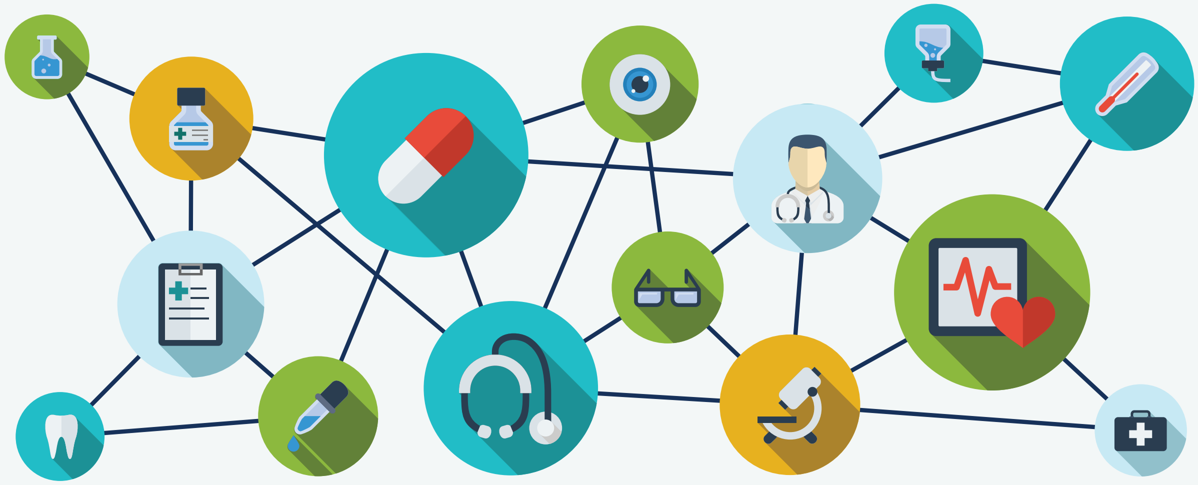
CYBEREADY
THE HUMAN READINESS COMPANY

CLALIT MEDICAL SERVICES - ENSURING HEALTHY SECURITY AWARENESS TOGETHER



כללית מעל 100 שנה
הכי טובה למשפחה

Access to sensitive information has made the healthcare industry a preferred target for hackers. Training employees effectively against phishing methods remains the strongest line of defense.

www.cybeready.com

About Clalit and CISO Itzik Kochav

Clalit Healthcare Services is the largest provider of healthcare services in Israel and is the second largest HMO in the world.
Its network consists of 14 hospitals, 10,350 community clinics and five sister companies, including dental clinics, medical device manufacturers, medical archive facilities, insurance companies and private clinical services. It also has over 50,000 employees, with about 7,800 doctors and 15,000 nurses. The rest of the staff is made up of other medical and administrative professionals.

The CISO, Itzik Kochav, has been working in information security for almost 45 years. As a highly seasoned professional, security awareness is a top priority for him and this concern is felt throughout his organization.

Itzik Kochav
CISO, Clalit Healthcare Services

The Challenge:

> **“Clalit needed a solution that could address effectively the unique training requirements of each community without creating much organizational noise”**

It’s well known that the healthcare sector faces more cyber threats than any other industry today and one of the main entry points for attackers is via phishing emails. When health professionals click malicious links in emails, they put the data, and moreover, the lives, of their patients at risk. Attacks to the healthcare system can cause operational downtime, a situation that is simply intolerable when surgeries and treatments are on the line.

Kochav and his team looked for a viable and scalable solution to tackle the phishing awareness problem for years. And with so many different communities of professionals within the HMO, it was clear that certain groups were far better at identifying phishing threats than were others. Thus they needed a solution that could provide the right learning experience and train each group according to its needs.

Another issue they needed to correct was that in conducting phishing simulations in the past, they encountered a great deal of negative buzz amongst employees. There was a palpable feeling of cynicism towards efforts to enhance awareness and this negativity was one of their biggest concerns.

Because of their deep commitment to changing the risky behaviors of employees across the HMO, Kochav and his team set out to find a solution that could address effectively the unique training requirements of each community without creating much organizational noise.

LOOKING FOR SOLUTIONS

Over the years, the team tried to educate and raise awareness among the different communities using various methods of interactive presentations and training simulations, all of which failed to achieve the required results. With employee behavior unchanged, they turned to outside phishing awareness providers. “None offered much in terms of flexibility and were unable to address the needs of such diverse groups. The solutions we tried took a lot of time to deploy and created that negative buzz that we knew we had to avoid”, explains Kochav. In the end, although they deployed simulation drills in the past, they were unable to see any tangible changes in employee behavior and results didn’t meet their expectations.

> **“The solutions we tried before took a lot of time to deploy and created that negative buzz that we knew we had to avoid”**

THE CHANGE TO CYBEREADY

In mid-2017, they found and implemented CybeReady across the organization. Despite Clalit’s magnitude, deployment was simple and straightforward. “All throughout the setup and deployment process, the team at CybeReady was attentive, yet highly methodical regarding their unique approach to employee awareness. It was clear that they really care about creating a dynamic solution that takes the organization itself into account,” says Kochav.

According to Kochav, one of the most valuable aspects of the CybeReady solution is the fact that although there is continuous Phishing practice running across the organization almost every day, there is lack of organizational noise created by its readiness Solution. Other systems they had tried in the past created a negative attitude towards awareness, which led to an employee resistance to change. “The CybeReady approach is so subtle that employees don’t even realize they are learning and changing their behavioral patterns”, explains Kochav. Campaigns run continually, training over 50,000 employees, and yet employees don’t feel the system is intrusive or disruptive at all.

> **“The CybeReady approach is so subtle that employees don’t even realize they are learning and changing their behavioral patterns”**

MEASURABLE RESULTS AND ACTIONABLE INSIGHTS

After just a short period, Kochav began to see a tangible change in employee habits. “Even my most unaware groups started exhibiting a greater level of awareness after a short time. These are employees who, in the past, expressed frustration with awareness training methods and moreover, those methods never bore any fruit. With CybeReady, we began to see positive change after the first two campaigns.”

What’s more, they have gained precise understanding into what each group needs to increase their awareness levels. Using CybeReady’s unique dashboard, They can see, for example, that the more vulnerable groups need more targeted tactics to improve their performance, while other groups can do with less. Using these metrics, the platform can detect, analyze and adapt automatically to target training methods specifically for each group.

Using CybeReady’s unique dashboard, they can see that the more vulnerable groups need more targeted tactics.

Another aspect of the CybeReady approach is that it allows them to properly target specific awareness issues. Via the CybeReady dashboard, Kochav can generate many different reports, sorting by role, location, previous awareness levels, etc. The reports provide the team with a comprehensive view of the organizational risk, with the ability to granularly drill down from large departments to small teams, while remaining compliant with local and national privacy regulations. It allows them to communicate the awareness levels of each unit or teams and make them focus on improving security.

> All I need is 10 minutes a month. The rest happens by itself

EASE OF DEPLOYMENT:

In charge of managing the platform is Hagar Reshef-Freid. "All I need is 10 minutes a month. The rest happens by itself", she says of the platform. With just a pithy time investment, she manages and monitors campaigns and progress, while the adaptive automatic process runs continuously, training their employees seamlessly. After each campaign, she gets the results as well as the system's suggestion for the next stage. All she has to do is approve the new suggested simulation plan and then it is automatically set into action.

The solution allows Kochav, Reshef-Freid and the rest of their team to focus on other critical security issues, while knowing that the awareness training aspect is being taken care of. "The deployment was quiet and smooth. It was up and running in a few days. Most of all, we haven't gotten any bad feedback from employees, like we did all the previous times we ran drills in the organization. With little effort on our part and just as little noise, the platform has become part of our daily routine in a very natural way," says Kochav.

THE RESULT:

Thus far, the results have been impressive; the security culture has changed dramatically and now everyone is on board with training efforts, regardless of their professional community belonging. "Now they send me apology emails and say "I clicked a link I shouldn't have. I'm sorry and I'll try to do better." Kochav also mentioned receiving feedback from employees "indicating that they came across emails that made them think twice before clicking. Before implementing CybeReady, this would have never occurred – they just didn't care enough", explains Kochav. In fact, the solution has made such an impact on the security culture that several of the HMO's hospitals have even made a competition out of it, to see which one can achieve the best awareness results.

> With little effort on our part and just as little noise, the platform has become part of our daily routine in a very natural way

> The results have been impressive. The Security culture has changed dramatically and now everyone is on board with training efforts,

EXPERIENCE WITH CYBEREADY:

As an added plus, Kochav says the CybeReady team was, and continues to be, incredibly supportive. “They came and immediately knew what needed to be done to raise awareness and change employee behavior. And now, think about the size and the diversity of our organization — and the fact that the program was deployed with such efficiency across such a large organization— and they were still able to get the best results, without additional effort on our part. To me, that’s amazing.” As with any new platform, during the first few weeks after setup, there were some aspects that needed fine tuning, but Kochav attests that the CybeReady team was always happy and eager to help.

Positive Security Culture, Positive Results

The word Kochav feels best sums up Clalit’s experience is “positivity”. The platform is transforming behaviors and their security culture in a fully positive way, all without shaming, or creating a bad vibe.

It’s clear to Kochav that CybeReady is truly invested in helping each organization transform their awareness level — and they have the tools and the drive to help them achieve their goals. As Kochav says, “CybeReady is a critical part of our tactical plan for 2018.”

> **“The fact that the program was deployed with such efficiency across such a large organization — and they were still able to get the best results, without additional effort on our part. To me, that’s amazing”**