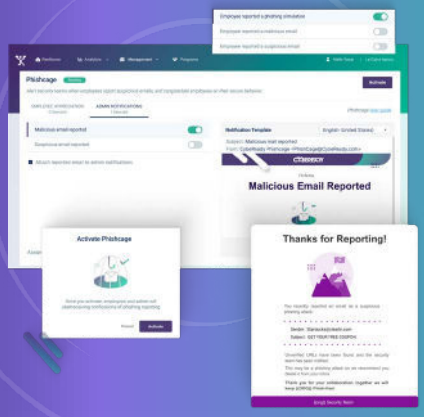
ERICSSON CYBEREADY

Building Cybersecurity Readiness: Ericsson's Employee Training Journey

www.cybeready.com



The Industry Challenge

According to Checkpoint, the telecommunications sector has long been a high-value target for cybercriminals. The communications industry saw a *51% rise in the number of attacks in 2021*[1] making it the third most vulnerable sector. The telecom infrastructure is used to transmit and store large amounts of sensitive information making it a lucrative target for bad actors.

The telecom industry is particularly vulnerable to cyber-attacks. The telecommunications infrastructure that has found widespread adoption makes the industry a lucrative target for cybercriminals. After all, a successful attack on the telecommunications network can potentially expose information to millions of customers.

Why is the telecommunication sector vulnerable to attacks?

Both telecommunications threats and cyber risks for the telecom industry are increasing. The major reasons why the telecommunications sector is a lucrative target for cyber-attacks are as below.

1

Legacy technology

The telecommunications sector still uses legacy technology which makes it vulnerable to IP-based threats. The adoption and transition from legacy systems are slow, leaving companies with vulnerable old-school systems.

2

Interconnected networks

The telecom industry has interconnected networks. There is also tons of customer data and sensitive information. The combination of these two factors means that cybercriminals can cause maximum damage through minimum effort.

3

Sensitive information

Telecom providers store a lot of information including financial information such as credit card information, social security numbers, contact details, etc. which are particularly useful for bad actors to sell on the dark web.

4

Increasing threat surface

The threat surface continues to increase as we move towards advanced technology such as 5G.

5

Lack of awareness

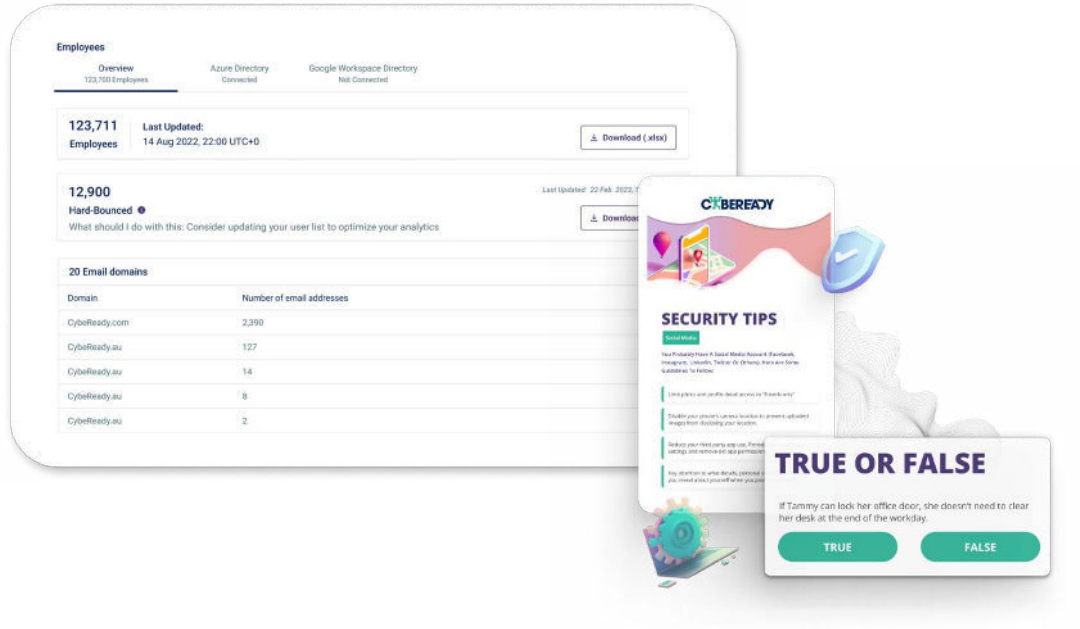
Lack of technical knowledge and awareness within the team is one of the major challenges. Poor password hygiene and data sharing often invite risks that could easily be avoided through proper education.

Just like in other sectors, a main threat to the telecommunications sector comes from their own employees.

[1] https://blog.checkpoint.com/security/check-point-research-cyber-attacks-increased-50-year-over-year/

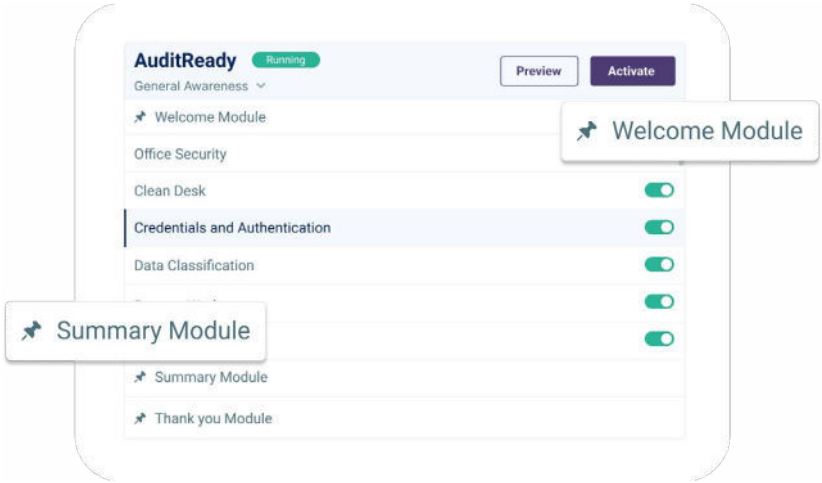
The company

Telefonaktiebolaget LM Ericsson, commonly known as **Ericsson**, is a Swedish multinational networking and telecommunications company headquartered in Stockholm. The company sells infrastructure, software, and services in information and communications technology for telecommunications service providers and enterprises, including, among others, 3G, 4G, and 5G equipment, Internet Protocol (IP), and optical transport systems. The company employs around 100,000 people and operates in more than 180 countries.

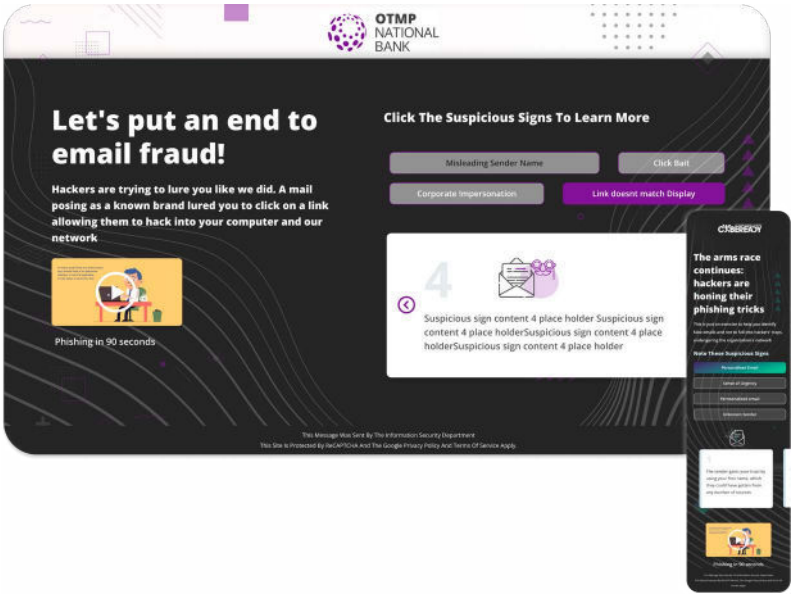


The Cybersecurity Challenge: Training 130,000 Employees - Globally

The Security team at Ericsson was faced with the challenge of training a large, distributed workforce. Ericsson's employees are spread out over multiple geo-locations in more than 50 countries and 30 languages as well as multiple business units (over 20). The Security Awareness team was challenged with the need to grant each unit some autonomy, and access to the training data, progress, and management while keeping a centralized control center for the entire workforce training.



In addition, following Ericsson's experience with other security awareness training solutions, the team was looking for a way to eliminate the challenges that come from automated clicks. Auto-clicks are a common issue when bots (utilized by other email security systems) generate "fack click" as part of the ongoing efforts to sample and test all company emails. When those auto-clicks are generated on phishing training emails, they may impact the training results and show that employees have clicked on emails even when they didn't - which results in blaming employees as well as not getting a realistic view of the training progress.



Ericsson's team values security awareness training and sees it as a significant component of the company's cybersecurity suite. The Awareness team has prioritized this effort and understands the need for effective training that actually changes employee behavior and builds a positive cybersecurity culture. Before learning about CybeReady's Readiness program, the team was using another security awareness vendor's solution.

With the previous vendor, the Awareness team at Ericsson found themselves spending tedious hours planning training campaigns and sending phishing simulations to employees, creating reports, and trying to measure progress. They were putting in a lot of time and manual effort that consumed expensive IT resources without yielding measurable results.

The Solution: An Employee Readiness Program that runs out-of-the-box

At the beginning of 2022, Ericsson's Awareness Lead met with CybeReady and decided to start a two-month POC to evaluate the solution.

The first thing that stood out in CybeReady's solution was the fact they help security teams go beyond awareness and build employees' Readiness for cyberattacks. They liked the methodology that trains employees continuously, via short, positive, in-the-moment training sessions. In addition, the fact that each employee receives localized translated content (in 4 languages), made a big difference in engaging employees across the 50 countries Ericsson covers.

Ericsson's team appreciated CybeReady's ESP (Elastic Security Program) capability which trains the different business units according to their needs. This allows each local security officer visibility of the global training as well as the specific progress achieved by their local organization. CybeReady's ESP provides flexibility and supports organizational changes (closing of BUs and opening new ones) - easily. It allows the team to centrally manage Ericsson's distributed workforce and grant business units control without compromising the quality of training.

CybeReady's advanced technology also helped Ericsson identify and eliminate the automated clicks challenge. It cleans out the data: proactively with two layers - with screen controllers that run in the background as well as the monthly review and additional clean up of the data. All this is not being done for Ericsson, as opposed to previous solutions, where the team had to monitor and clean those auto-clicks out manually.

Most importantly, Ericsson's employee training effort started yielding measurable results quickly after switching to CybeReady. Ericsson reduced their click rate by half, across its extensive and diversified workforce.

High-risk groups decreased significantly

Erin Swoverland, Security Competence Manager at Ericsson, experienced the change across all organizational levels. She started seeing a real change in employee behavior.

"The best part of utilizing CybeReady is to see how our employees started taking an active role in defending the organization", she said. "Within 12 months of training, we're starting to see a real cybersecurity culture emerging and employees are not just aware but actually care about doing their part".

"The training methodology increased employee engagement, while the advanced automation allows us to train each employee in their language and locale and adapt the training to their performance continuously as if they were not one of 100,000 employees but an individual who receives a personalized training program. Additionally, the ESP has allowed our business units the autonomy they needed to run their own training, while we can keep the main control in our team's hand".

In conclusion, Erin shared: "Upgrading our security training program to CybeReady's solution was beneficial to our employees, our security team, and the entire organization. For the first time, we can present measurable results and see how employees improve and build cyber resilience without burdening our IT team whatsoever."