IRONSCALES
SAFER TOGETHER

SRC CYBER SOLUTIONS LLP
CYBER RISK SOLUTIONS

Case Study

Chelsea Football Club

Challenges

- Well-known brand in the public eye
- An uptick in phishing attempts on European football clubs
- A busy internal team

Solution

- Self-learning, AI-driven phishing protection from IRONSCALES
- Regular phishing simulation and training
- The IRONSCALES mobile app

Results

- Total remediated emails in the past year – 102,618
- Analyst hours saved in the past year – 513 hours and 54 minutes (data is based on the average of 33 minutes that it takes an analyst to resolve a phishing attack based on the Osterman Research, 2020)
- A noticeable improvement in employee phishing awareness

> "The mobile app is a key benefit from my side. A few times now I've received alerts in the evening as hackers are targeting our C-Suite or Executives. With the app, I can remediate these threats in minutes from wherever I am, without having to log on to my computer."

MATTHEW GREEN, INFORMATION SECURITY ANALYST AT CHELSEA FC

Company Intro

Chelsea Football Club (FC) is an English professional football club based in London. Founded over 100 years ago, the club competes in the Premier League – the top division of English football – and is one of the most recognizable and successful clubs globally. The club's backend operates like any other company, with a core staff of around 800 individuals spread across departments including Operations, Marketing, HR, and IT.

The Problem

As a high-profile sports team with millions of worldwide fans and publicly recognizable players and staff, Chelsea Football Club is constantly in the spotlight. And data leaks to the press often target sports clubs, like the Football Leaks case which saw confidential financial transactions between European professional footballers and clubs published between 2015 and 2019. Chelsea FC knew that keeping their data safe was a top priority; research by the UK's National Cyber Security Centre (NCSC) in 2020 found that at least 70 percent of sports institutions in the UK suffer a cyber incident every 12 months, which is more than double the average for businesses.

As the main internal communication tool for most organizations, email is particularly susceptible to being compromised by hackers. In 2020, a Premier League football club narrowly avoided losing £1 million when their email account was targeted by hackers during a transfer window, mirroring a successful phishing scam against Italian club Lazio in 2018, which lost them €2 million. With the escalation in email-based attacks, the Chelsea FC security team recognized that email was a key risk vector when it came to securing data.

> One of the good things about the IRONSCALES training and simulation features is the analytics. We never name and shame, but we can now see which departments will need more training over time and which departments already have a solid base of phishing knowledge."

MATTHEW GREEN,
INFORMATION SECURITY
ANALYST AT CHELSEA FC

Beyond their existing email management and monitoring system, the team had no dedicated anti-phishing solutions implemented and no system for user training and phishing awareness. Chelsea FC had found that the built-in email filtering solution provided by Microsoft Office 365 was cumbersome to use, with no ability to be used while on the go for email mitigation. Chelsea FC's internal team cover information security responsibilities like policy creation, performing security procedures, and network monitoring, but as a small and agile team, they required further external solutions to be able to boost their email security capabilities.

The Solution

The Chelsea FC security team was looking for something easy to manage for their busy team. As email security responsibilities at the time of implementation were spread between the IT infrastructure team and senior engineers, the organization was looking for a solution that would save time, ideally using automation to remove the burden of identification and mitigation from the staff. The team also recognized the importance of user education in their anti-phishing strategy and were therefore looking for a platform that could address their training needs and educate users across the business.

After being recommended the IRONSCALES solution by their security partner, the team quickly found that its self-learning, AI-driven phishing protection and simple usability was the best tool for supporting both their email security needs and their busy internal team. After conducting a short Proof of Concept within the IT department, Chelsea FC's security team found the implementation process very easy, with IRONSCALES integrating directly into the Office 365 inboxes of their 800 users. From there, the solution started inspecting emails for phishing automatically. The internal security team also found IRONSCALES' ongoing support particularly beneficial throughout the implementation process and beyond.

Outcomes

IRONSCALES' powerful combination of machine and human intelligence has helped Chelsea FC resolve over 2000 incidents since starting to actively use the solution in 2019. Of these incidents, 572 were phishing, 693 were spam, and 313 were deemed safe. One of the key benefits for the Chelsea FC security team has been the ease of use and management; the solution began using AI to detect and remove threats from inboxes immediately after implementation. The handy IRONSCALES phishing button has made reporting intuitive for the busy team at Chelsea FC, and even when employees don't report directly through the IRONSCALES button they're often raising it through the service desk, showing a marked improvement in general awareness.

"I would definitely recommend IRONSCALES to others. It's a great software that has helped us drastically improve our employees' awareness of what to look for to spot phishing."

MATTHEW GREEN,
INFORMATION SECURITY
ANALYST AT CHELSEA FC

The Chelsea FC team is also benefitting from IRONSCALES' mobile app, which allows them to immediately triage notifications from users directly from their phone, whether they're at work, at home, or on the go. When working from home was mandated in 2020 due to the COVID-19 pandemic lockdown, the team saw increased attempts to spoof Directors and PAs targeting home workers. However, using the IRONSCALES mobile app has made it easier for members of the internal security team to keep mailboxes clear of malicious emails at any time of day and from any location, throughout the remote working transition.

The Chelsea FC security team has also been able to run various phishing simulation campaigns, with both email security and awareness training integrated into IRONSCALES' single offering. Launching simulations one department at a time, the Chelsea team has been able to establish the phishing knowledge of each area of the business. After starting with basic campaigns, the internal team is now working on making each simulation more difficult than the last. By running simulations continuously and building on their employees' knowledge tactically, Chelsea FC has seen a 'definite improvement, in general phishing awareness and a noticeable uptake in reporting.

By using the IRONSCALES solution, Chelsea FC joins a global threat intelligence-sharing community, with every IRONSCALES customer helping to warn the wider community about newly discovered threats anonymously. Being a part of the community means that Chelsea FC is not only able to anticipate threats from around the globe before they hit, but is also helping other organizations do the same, contributing to the wider defense against email-based attacks.

Looking Ahead

Chelsea FC is continuing to run detailed phishing simulations, intending to test based on the vulnerabilities they identify within each department of their business. By running these simulations strategically and beginning to personalize them based on department, the internal team can more accurately quantify their cybersecurity posture and minimize clicks on malicious links across the entire organization.

ABOUT SRC CYBER SOLUTIONS LLP

At SRC Cyber Solutions LLP, we provide Next Generation, Automated and User-Friendly solutions in partnership with AUTOMOX for Patch and Endpoint Management, IRONSCALES for Comprehensive Email Security and Anti-Phishing Protection, THREATX for WAAP (WAF++) with an Attack-Centric approach for Web Application and API protection and Project Ares for Online Gamified Simulation-based Cyber Security Training.

www.srccybersolutions.com | +91 120 232 0960 / 1 | sales@srccybersolutions.com

IRONSCALES
SAFER TOGETHER

SRC CYBER SOLUTIONS LLP
CYBER RISK SOLUTIONS