CASE **STUDY**

Topic: Information Security Training for Financial Industry

TERRANOVA

INTERNATIONAL BANK IMPROVES INFORMATION SECURITY TRAINING EFFECTIVENESS WITH TERRANOVA

Security is a critical concern for organizations today, especially those in the financial sector. According to PricewaterhouseCoopers, over the past year alone, 31 percent of global financial service companies have experienced numerous security incidents - with nearly 35 percent of respondents attributing the breaches to employee action.

A major global financing institute was challenged with how to strengthen its defense against the rapidly accumulating risks of cybersecurity and online fraud. Servicing a wide range of business sectors across more than 30 countries, the company needed a way to ensure that the users of its systems would not compromise its critical infrastructure. Complicating matters even further was its international scope and public funding and ownership, which meant it did not have a specific set of regulations or compliance standards to adhere to, thus limiting its guidance.

THE CHALLENGE

After conducting a risk analysis, the company determined the biggest threat to the bank's security came from internal users rather than external sources. Identifying approximately two dozen risks that users were responsible for, the client learned it needed to implement a training program that revolved around data leakage. It sought a solution that would provide user education and guidance on a range of topics, including email, cloud and mobile security, as well as best practices for sharing sensitive data and information.

The financial institute needed a solution that allowed it to not only deliver practical advice about information security specific to the organization, but to also simultaneously educate users who had no prior knowledge of the subject. Yet most of the vendor applications it looked at were limited in terms of customization and editing capabilities.

The company knew it needed a platform that would allow it to provide guidance and training to employees with varying levels or knowledge.

"Other organizations tend to have a base in which to work where people know information security and what the dangers are," *the company's chief information security officer explained.* ***"But we had to help our large user base understand information security - and that was a major challenge."***

Summary

Sector

Financial

Challenge

Deliver practical advice about information security specific to the organization, and simultaneously educate users who had no prior knowledge of the subject.

Solution

- Phishing simulations
- Customized security awareness campaign

Results

- 100% of users captured
- Increased reporting of phishing attempts

THE SOLUTION

Determination to achieve this goal was what led the bank's chief information security officer to Terranova Corporation due to its quality of materials, delivery mechanisms and feature customization.

Leveraging online and video content, the client was able to use its own materials and edit and tailor as much as it needed, ultimately enabling it to present its users with training modules that made the most sense.

Through the LMS, the company was able to deliver its users with a basic concept in a short animation, as well as integrate additional messaging and guidance details with interactive content. In addition, reinforcement mechanisms allowed the financial institution to emphasize the same points using various avenues.

Due to the vast number of users - and accompanying usernames and passwords - it was especially beneficial that the application offered a seamless and convenient experience, which was made possible through Terranova's Single Sign-On (SSO) capabilities.

"Of all the vendors we looked at, Terranova had the most flexibility and gave us the greatest choice in terms of what we could present to our users," *the company's chief information security officer said.*

THE RESULTS

The company used two main measurements to assess the effectiveness of the solution: social engineering and instant management. The bank ran a number of scenarios, which involved sending phishing emails, unsecure attachments, cold calling and more to identify whether users applied the guidance the training provided and, if not, the reasons behind the lack of improvement.

In addition, the financial institution collected and pooled data that offered insight on which incidents should not have occurred due to the provided training from various departments.

Each scenario was weighed based on a complexity scale of five to one. For the most complex, the goal was to achieve a successful identification rate of between 60 percent and 80 percent for the least complex.

Just six months into the product lifecycle, the financial institute hasn't made a request for a specific module that hasn't been completed - and it has seen significant rewards since implementing the LMS security awareness solution.

With a previous provider, it saw about a 60 percent uptake in its user base, but with Terranova's product, it has reached approximately 75 percent. Because the client is able to report monthly compliance, it is able to keep better track of which departments has completed the training. And for the first time in the bank's history, it has been able to write an internal training policy.

Due to the versatility of Terranova's solution, the financial institute has already realized profound improvements in the information security training and education of its users and will continue to release modules that help further fuel the success of its security measures.