BEAUCERON SECURITY

www.beauceronsecurity.com

FINANCIAL INSTITUTION CASE STUDY

Results

1. Increased phishing report rate **from 30% to as high as 51%** in the first six months.
2. Reduced click rates from 22% to currently averaging **less than 4%**.
3. Automation provided substantial reduction of resource hours (roughly **2.0 FTE**) which allowed the department to deliver additional services to the business lines and increase the value of security within the organization.
4. Ability to answer regulatory requirements through **reporting functionality** in real time within one platform.
5. **Ability to integrate** with additional data analytics and visualization tools via API such as Tableau.
6. The team could **focus on providing industry-relevant content** and tools designed to empower frontline employees to better serve the institution's clients and answer cybersecurity concerns with confidence.

Protecting a global financial institution

As a global financial institution with billions of dollars in assets under management, the client was intimately familiar with the need for a robust security awareness practice and, therefore, had an established program already in place. Their challenge was the ability to quickly demonstrate compliance and a consistent positive change in behaviour over time.

With ever-changing regulatory requirements, the financial institution needed a high degree of configuration in their program. The institution wanted to exceed compliance requirements and drive an industry leading approach to not just make people aware, but to motivate their organization to care about security. This required being able to quickly deploy new training in response to intelligence, incidents and changes in policies, standards and tools.

Challenges

- Demonstrating continuous improvement, delivering a consistent global program without adding any new full-time positions.
- Freeing up staff time from tactical tasks to strategic content and campaign development and execution.
- Demonstrating that regulatory requirements have been met; at a moment’s notice leveraging out-of-the-box and custom reports.
- Integrating enterprise systems for identity, email threat analysis, mobile enterprise application and more.
- Finding a technology partner who would drive innovation in automation, analytics and behaviour change using a data-driven, scientific approach.

Company overview

- Among the largest banks in North America
- Serving 16 million+ clients globally.
- 100,000 employees worldwide, including multiple subsidiaries.
- Dedicated global cybersecurity team distributed across multiple locations.
- Several major IT programs and initiatives to enable digital transformation and security.
- Well-established cybersecurity awareness program, with click rate and report rate targets.

Key features deployed

- **Individual employee dashboard** highlighting their personal security score, which in effect is their personal resiliency score.
- **Custom workflows** that allow for role-based courses to be deployed to different employee groups in an automated fashion.
- **Automated, randomized and targeted phishing** campaigns with automated remedial interventions.
- Customizable **Chat Bot** delivering instant answers to the users' pressing cybersecurity questions, eliminating the need to search for answers through the intranet.
- **Reporting** functionality to pull and manage all compliance requirements required by financial regulators.
- Automated and manual **reward and incident reporting** to reinforce positive behaviour.
- **Multi-channel phishing** reporting tools including Outlook button, email forwarding and integration with mobile device management (MDM) platform.

Key decision factors

- Market-leading **automation** designed to provide cost savings over time.
- **Rigorous security controls** for the platform with data storage controlled to specific locations.
- **Tight integration** with Microsoft Office365 for user provisioning, single–sign-on and advanced integrations.
- **Comprehensive platform customization** to mirror corporate branding and provide relevant user messaging.
- The ability to **host content from any provider** under one platform with reporting and tracking capabilities.
- Ability to **easily pull reports** to satisfy governance and regulatory requirements.

Building on an established cyber awareness program

As the company evolves their security awareness program with a focus on behaviour science, the goal will be to leverage the built-in capabilities of the platform to deliver more innovative awareness content, program results analysis and engagement with their community.

New integrations with in-house custom-built email security analysis tools will provide new ways to understand real phishing threats that are reported. In addition, integrations with in-house data reporting and learning and performance management tools will continue to build value for the business.

Leveraging the Beauceron platform, the cybersecurity awareness team is able to build a living lab of experiments and data that can be used for continuous feedback and improvement of the awareness program tactics and results.

> ”The tool has more than paid for itself in the reduction of resource hours and the multiple tools it has displaced, plus allows people to do the jobs they are supposed to be doing, instead of running all the functionality in the background and aggregating the data.”
>
> **Senior Manager Awareness & Education,**
> **Global Cyber Security**