BEAUCERON SECURITY

FIRST COMMUNITY BANK SINCE 1916 AND TRUST

COMMUNITY BANKS CASE STUDY

FIRST COMMUNITY BANK AND TRUST

Results

1. **100%** of staff reported feeling they **knew more about cybersecurity** from this experience.
2. **100%** of staff have **completed onboarding** training.
3. Achieved a **click-rate under 1%** in Year 1.
4. Achieved a **report-rate of 55.9%** in Year 1.

Protecting Community Banks

Financial Institutions have long been a preferred target for cybercriminals.

This poses a particular threat to community banks, who must have world-class approaches to cybersecurity to combat worldwide threats. Community banks also understand how important their relationships are with their customers and how much their clients rely on secure, trusted services.

Customers trust community banks with their financial needs and a great deal of personal identifiable information including government ID, contact information and more. For these reasons and more, banks are 300 times more likely to be targeted by cybercriminals who look for weaknesses in a bank's systems and infrastructure [1].

Protecting clients' confidential information such as loan information, credit and debit card numbers as well as other financial information that is tied to a customer's personal, identifiable information is a top priority for community bank leaders.

Compliance Requirements

Banks play a vital role in our economy and government regulators keep a close eye on their compliance with security standards and rules.

The financial sector is obligated to meet compliance requirements that help protect confidential data and reduce the chances of a cyber attack. If these requirements are not met, organizations can face hefty fines and penalties.

For instance, over the span of three months in 2020, the U.S. Office of the Comptroller of the Currency levied an estimated $625 million in fines on organizations that failed to meet compliance requirements [1].

The Role of Awareness

Robust security awareness including regular phishing simulation tests is a vital part of modern cybersecurity defenses and increasingly a point of interest for auditors and regulators. A world-class security awareness program is a must.

Challenges

- Provide a positive cybersecurity awareness experience for team members by reinforcing proactive behaviors like reporting phishing emails instead of deleting them.
- Encourage employees to engage in meaningful cybersecurity training.
- Spend less time in creating phishing simulations and assigning training to meet security priorities.
- Demonstrate that compliance requirements have been met by leveraging out-of-the-box and custom reports.

Company Overview

- Privately owned bank serving Beecher and Peotone, IL, and the surrounding communities for over 100 years.
- Member of the Independent Community Bankers Association (ICBA) and participant in the ICBA ThinkTECH Accelerator.
- Currently working with 12 fintech companies to drive a variety of digital transformation initiatives to meet the evolving needs of their customers.

Key Decision Factors

- Market leading **automation** designed to provide cost savings over time.
- Focus on **positive cybersecurity behavior** change and reinforcement.
- Ability to **easily pull reports** to satisfy governance and regulatory requirements.
- **Customizable** courses, workflows and the ability to control which educational elements team members can opt in to in order to focus on relevancy.
- Track the **phishing report rate** within the platform to measure the effectiveness of education by having team members demonstrate that they can spot potentially malicious emails and report them.

Key Features Deployed

- **Customized team member onboarding experience** to suit the bank's needs and reinforce other policies, behaviors and initiatives that FCBT has already undertaken with regards to cybersecurity.
- **Individual team member dashboard** highlighting their personal security score, which in effect is their personal resiliency score.
- **Phishing templates** sent via automated, randomized phishing engine.
- **Reporting functionality** to pull and manage all compliance requirements required by financial regulators.
- Automated and manual **reward and incident reporting** to reinforce positive behavior.
- **Multi-channel phishing reporting** tools including Outlook button and email forwarding.
- **Risk self-assessments** based on the NIST Framework and organizational Risk Advisor.

Resources

[1] Hartman Executive Advisors, "Cybersecurity Concerns for Community Banks and Credit Unions in 2021," 2021. [Online]. Available: https://hartmanadvisors.com/cybersecurity-concerns-for-community-banks-and-credit-unions-in-2021/. [Accessed 2022].

"Clearly, every community bank needs a robust solution in this space, but just having a solution versus having one that truly delivers is critical. Our experience with Beauceron Security has been excellent. Our employees are far more engaged in the process, and our first-year results are meaningfully better than anything we have achieved before as an organization. The solution is both simple to implement and cost-effective. It's a perfect place to start for a bank looking to embark on their fintech journey."

Greg Ohlendorf , President & CEO
First Community Bank and Trust