CrossCountry Consulting

A Better Experience

Cybersecurity in Financial Institutions

CrossCountry Consulting

Enduring Cybersecurity Challenges in an Increasingly Digital Landscape

Financial Institutions (FIs) are perpetual cyber-attack targets, desired both for monetary assets and their trusted customer data, such as personally identifiable information, bank account numbers, etc. Due an accelerated digital transformation during the COVID-19 pandemic, FIs strove to innovate customer interaction while shifting to a remote workforce, greatly expanding their attack surface. Challenges facing FIs are compounded by the need to keep pace with complex and evolving cyber and privacy related regulatory compliance efforts.

KEY CONSIDERATIONS

HOW WE CAN HELP

CEO — How can I ensure that what we're doing is protecting our assets?

CFO — How can I make sure we're investing cyber resources in the right areas?

CISO — How can I make sure we're appropriately assessing cyber risk?

Threat Intelligence & Modeling

- Perform comprehensive threat assessments based on open-source intelligence and FI expertise to inform the organization of its unique threat landscape and drive prioritization of cybersecurity strategy
- Generate tailored threat models to inform risk and strategy decisions and resource allocation

Offensive Security Testing

- Execute an attack simulation by emulating a specific threat actor and carrying out its likely objective
- Test ability to detect an adversary before the attacker gains control
- Perform penetration testing to find exploitable security deficiencies
- Identify vulnerabilities within a network and provide remediation prioritization using vulnerability scanning tools and techniques

Strategy & Transformation

- Create and transform risk management programs to align to industry frameworks and address cybersecurity regulation
- Advise on information security strategy to reduce risk and provide roadmaps to meet cybersecurity objectives
- Identify current cybersecurity maturity and threat landscape, and level of protection needed to meet regulatory requirements

OUR EXPERIENCE

Case Study: Offensive Security Testing & Cybersecurity Framework Assessment

CrossCountry performed a scenario-based attack simulation and an assessment of a bank's cybersecurity framework and roadmap. The goal was to demonstrate that additional budget was needed to uplift its cybersecurity program, as well as verify that the roadmap addressed relevant cyber risks.

Offensive Security Testing – Red Teaming

Our Approach

We simulated a targeted cyber-attack that emulated a malicious insider's attempt to access customer information and banking data.

Impact

We demonstrated that an adversary could obtain: customer SSNs; debit card information; bank account numbers and transactions; and 81% of employee passwords. The client learned its security controls did not detect the emulated attacker activity and that controls must be fine-tuned to provide better visibility into malicious activity. Our team identified areas of security deficiencies to identify and classify security risks, improve resiliency to attacks, and inform the cyber roadmap to prioritize future investments.

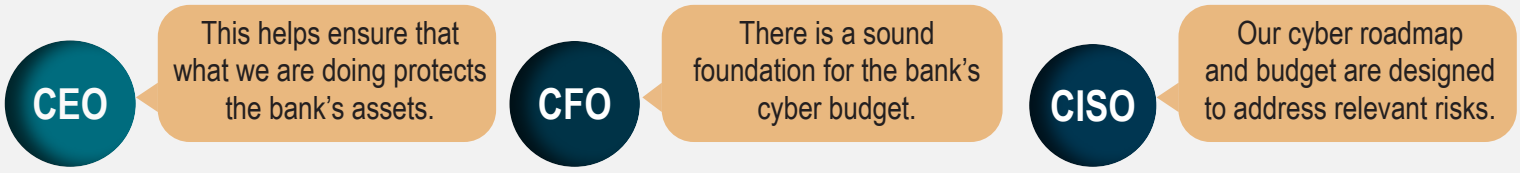
Cybersecurity Framework & Roadmap Assessment

Our Approach

Our cyber framework assessment approach was customized to the bank's specific regulatory environment, threat landscape, and strategic needs, and was based on best practices, such as Financial Services Sector Coordinating Council (FSSCC), NIST, and NYDFS frameworks and regulatory guidance.

Impact

Leveraging the FSSCC cybersecurity profile, which integrates commonly used frameworks and regulatory guidance, we enabled the security team to enhance their cybersecurity roadmap and budget to prioritize efforts to address the most significant risks.



ACKNOWLEDGMENTS

"CrossCountry has proven to be an excellent partner for our strategic security initiatives."

- Mark Fitzgerald, Chief Information Security Officer

Investors Bank

"CrossCountry's Cyber & Privacy team has been an invaluable business partner as we've scaled and matured a world class cybersecurity program. Through our partnership, we have enhanced the capabilities across many of our top cyber risk initiatives to build a holistic cybersecurity program."

- Michele Valdez, Chief Information Security Officer

OneMain Financial

Contact Us

CAMERON OVER, Partner
cover@CrossCountry-Consulting.com
703.899.6486

STEPHANIE MENDOLIA, Director
smendolia@CrossCountry-Consulting.com
757.593.3350

ERIC EAMES, Associate Director
eeames@CrossCountry-Consulting.com
703.786.3697

CROSSCOUNTRY CONSULTING

Inc.5000 HONOR ROLL 2020
5X HONOREE

glassdoor
2021 BEST PLACES TO WORK