Addressing Insider Threats, Cyber Attacks & Data Security

Insider threats are not over-hyped. They remain among the biggest threats to a community bank's critical data and overall security. Traditionally, "north-south" perimeter-traversing data traffic is carefully monitored, while internal "east-west" data traffic is less closely scrutinized. In this paradigm, an attacker who gains access to the network may be able to laterally move around the network internally and look to elevate their credentials, disrupt operations, or pilfer data.

The majority of bank employees are trustworthy and want to do the right thing, but they can still jeopardize the bank's security posture by their actions, especially if they are unaware that those actions are dangerous. They may click on phishing emails, visit malicious websites, or bring in USB drives – there are numerous ways that employees can introduce threats into your network.

The fact of the matter is that breaches are pretty much inevitable, and unfortunately the average time it takes for a company to detect a breach in their network is over seven months. This statistic is a clear indicator that the vast majority of organizations aren't focused on detecting threats, and it is critical that your bank be able to detect a breach and respond quickly and appropriately.

With our all-in-one managed security solution, we not only detect breaches within your network much more quickly (from months down to minutes), but our team of highly skilled security analysts and engineers will take steps to mitigate the issue entirely. We closely monitor activities at both the perimeter and within the credit union's internal network.

The first step that we take is to establish a baseline of your network. This allows us to then spot both upticks and downticks in activities that signal a breach is in progress, or has already occurred. In addition to our sophisticated detection tools, we extract the bank's log files to our state-of-the-art Security Operations Centers where we can granularly analyze them and respond quickly.

We have assembled a team of highly talented professionals in the fields of Information Assurance and Network Security. We use tens of thousands of threat resources to help us keep track of the ever-increasing number of cyber-attacks.

Our security program approach is based on four key capability areas which, when taken in aggregate, comprise a fully-functioning, mature security program capable of meeting FDIC regulations as well as actually protecting the bank's information and members. 1) Prevention through defense in depth; 2) Detection through constant vigilance and our sophisticated suite of tools; 3) Containment through secure network architecture; and 4) Eradication to act swiftly, remove the threat, and use the incident as a basis of knowledge to evolve the prevention, detection, and containment strategies accordingly.

When it comes to data security, encryption is is important, but we always recommend a full data classification survey and business impact analysis first. Information gained during this critical step will help ensure the bank is right-sizing its data protection strategies, and neither over-spending, nor under-protecting. Granular access controls are also required, facilitating the core security concept of least privilege access for all employees, contractors and vendors. Additionally, device hardening, configuration management, and multi-factor authentication are part of the equation.

The TruShield team, which has secured some of the most sensitive data and systems in the world, including top-secret government and military networks, and banks of all sizes, is ready to handle your security needs so that your bank can focus on what you do best – provide great service to your customers.

Paul Caiazzo
Co-founder and
Chief Security Architect

trushield

Contact Info
www.trushieldinc.com
877.583.2841

Paul Caiazzo is Co-founder and Chief Security Architect at TruShield responsible for developing corporate strategy and leading the technical product and service development efforts of the company. He holds CISSP, CISA, and CEH certifications, and has many years of experience solving complex cyber security challenges within the Federal government. Paul is responsible for architecting security operations centers around the globe, as well as helping domestic and international clients develop practical threat detection and mitigation strategies. In addition to his position at TruShield, Paul currently serves as Cyber Security Advisor to the Science and Technology Policy Center for Development.