

Protecting Customer Data at Rest and in Motion

Banks must be proactive about their security programs and overall defenses. They can start by making sure that their security program is in line with the strategies and goals of their business. Data breaches are constantly in the news, and the last thing that any bank wants is their good name associated with a data breach. Customer data is just too important - the bank's management team must do everything that they can to protect it because of the trust relationship with the customers.

Some of the technologies that banks are using more frequently now to protect data are encryption and strong virtual private networks (VPNs). Encryption should be a priority for any portable devices (laptops, flash drives, backup tapes, etc.) to protect data, and well-designed VPNs can help to shield data in motion.

It is important to remember, however, that technology and infrastructure can be well protected, but employees are only human and will make mistakes. It is imperative to have good policies and procedures in place, and augment them with security awareness training. Training must be ongoing and include a combination of classroom and computer-based training. Posters, giveaways, contests are ways of making awareness more fun. The goal is to make the users a key part of the protection strategy. Another critical area of exposure is the data entrusted to business partners. Vendors should be contractually bound to comply with your security policies. Data security includes not only securing the technology, but the critical information assets of the bank, whether stored on computers, media, paper, or at contracted parties.

At Reclamere, we help protect customer data through the entire life cycle. Up front, we can help with data breach risk assessments: identify what information assets are critical to the bank, where and how data is stored and handled, and how best to protect it. Building risk methodology into the security program is the key to ensure that critical data is not lost, stolen or altered. When you take a holistic view of the information flow from start to finish, it clarifies the points of protection. As part of our assessments, Reclamere helps identify threats with vulnerability assessments and other testing. Reclamere also can help with policy development, awareness program assistance, and Computer Incident Response Planning. The service is more preventive than a vulnerability assessment or a penetration test, which focus on the security of the technology.

Other Reclamere areas of expertise are data recovery and e-forensics. We work closely with banks to assist them with their overall backup and disaster planning efforts. For e-forensics, our experts can help to obtain, secure, and analyze electronic evidence that will stand up in court. We will negotiate with attorneys to ensure compliance with e-discovery requirements. Finally, at the end of the data life cycle, Reclamere is a recognized leader in certified - secure and environmentally sound - digital data and technology recycling and retirement.



Kevin Doyle
Manager

Kevin Doyle, Security Audit & Assessment Manager at Reclamere, has over eleven years of experience in Information Security. He holds the CISSP, ISSMP, and CISM certifications. He worked at the Pennsylvania State Employees Credit Union in Harrisburg, Pennsylvania for nearly twenty-four years as Internal Audit Manager, Compliance Officer, and Information Security Manager. He recently left PSECU and accepted a position at Reclamere in Tyrone, Pennsylvania. In his new position, he is managing Reclamere's Data Breach Risk Assessment and Auditing services. He has spoken previously at the Credit Union Information Security conference, the RSA Security Conference, and the Canadian National Payments Association conference.

