

Addressing the Big 3: Compliance, Fraud & Cyber Security

Compliance can be one of the biggest challenges for credit unions of any size. The rules introduced by the Gramm-Leach-Bliley Act have added another layer of compliance requirements to an already complex operating environment. In addition, the constant release of new information security guidance from the FFIEC and the NCUA matches the constant march of new technologies being introduced to credit union information technology systems. Keeping track of the specifics of each new guidance or regulation can be daunting, and the purposeful vagueness of many regulations leaves them open to differing interpretations for each examiner and credit union. The entire process can seem like a moving target. As one of two firms in the nation that performs exams under contract with the NCUA, TrustCC is in a unique position to evaluate compliance for our clients and make recommendations that will best align with examiner expectations.

To help with NCUA examinations, we comb through all of the credit union's documentation and help them to understand where we see weaknesses – our goal is make the examination process as painless as possible. We are also constantly reviewing FFIEC and other agency alerts and creating new materials to support compliance by our clients. Then we take it a step further and help them prepare for their next audit with specific recommendations and action items that will greatly assist them when the examiners arrive. At TrustCC, we have developed a highly innovative modular approach to IT auditing that covers all of the bases: GLBA compliance, BCP, vendor management, risk assessments, incident response, physical security and more.

To combat fraud, we recommend regular audits of employee accounts, especially super user accounts (administrator, root, etc). Credit unions normally have excellent controls on physical money movement, but digital money movement is somewhat more difficult to monitor. For instance, we recommend dual controls when it comes to wire and ACH transfers, but we sometimes see back office staff with the rights to singlehandedly create, approve and send ACH transfers. These users are prime targets for attackers utilizing social engineering tactics, and successful breaches often contribute to account takeovers and fraud. TrustCC provides in-depth security awareness training to credit union employees which helps them spot fraud, protect member information, and recognize common attack techniques. We can customize a training approach for management, your Board or a sub-Committee, your IT folks or all employees.

As more and more members turn to online and mobile banking and more employees work remotely, cyber security issues are only going to increase. In fact, at 63% of the networks we test, TrustCC was able to successfully penetrate the network and obtain internal sessions. From these sessions TrustCC almost always finds misconfigured systems and exploitable vulnerabilities that lead to compromised data and escalated access privileges. After identifying these vulnerabilities and risks, TrustCC security experts deliver detailed recommendations that the credit union's senior management can use to make important decisions on how to prioritize and remediate those risks.

TrustCC's proven strategy combines the most technical penetration testing available with comprehensive security assessment techniques and broad IT audit procedures. TrustCC maintains a laser-like focus on helping our credit union clients retain the trust of their members, and this proven by the fact that over the past 13 years we've performed over 1600 IT audits and security assessments for about 400 financial institutions.

Andy Robbins and Brandon Henry Security Experts & Certified Ethical Hackers



Andy Robbins brings a creative and tenacious style to demonstrating network vulnerabilities for CUs. After a successful stint at an IT managed services provider, Andy has been delivering operationally feasible remediation strategies to CU after exposing their typically unseen vulnerabilities for the past two years.



Brandon Henry has participated in hundreds of security assessments for financial institutions. His deliberate and goal-oriented style has been used to safely demonstrate vulnerabilities on CU networks in a way that delivers impactful value without impacting business operations. Brandon also develops TrustCC's vulnerability scanning analysis software, which takes the often-times chaotic raw output from popular tools and produces reports that influence intelligent remediation strategies.

Contact Info

www.trustcc.com