CREDIT UNION tech-talk
LEADERS FORUM
SPECIAL ROUNDTABLE SECTION
Technology News for Credit Unions Since 1988 www.cunews.com

Meeting the Challenges of Attacks, Breaches & Compliance

Information security attacks are increasingly perpetrated by organized entities that ironically operate using the sound business axiom of cost / benefit analysis. Being astute profiteers, they look for the greatest return on their investments and prefer targets that provide the highest payoff with the least effort. This means they will regularly exploit the path of least resistance and will simply move on if the effort does not help their bottomline. This could mean attempting to exploit an easier target or it could entail finding an easier path at a previously targeted organization.

Due to the fact that all credit unions have limited resources, it is vitally important to understand the sources of the organization's greatest risks and vulnerabilities. To maintain the effectiveness of these controls and recognize the paths of least resistance in an evolving threat environment, it is important to regularly assess the controls from all typical attack vectors. Limited penetration testing tends to focus remediation efforts on the areas tested, even if these are not in fact the elements posing the greatest risk to the organization. Comprehensive Penetration Testing from all attack vectors provides the credit union with a thorough understanding of its relative risks and the nature of its most impactful vulnerabilities, whether they are due to people, processes, or technology. This clarity provides the credit union the confidence that its mitigation efforts and resources can be applied in the manner best suited to mitigate organizational risk and thereby less likely to fall prey to a criminal attack.

Effective Information Security Programs manage the risk of data breaches through the distinct but related efforts of prevention and containment. While it is impossible to eliminate the possibility of breaches, prevention strategies can reduce the likelihood of a breach while containment strategies can minimize the impact to the institution. Info@Risk's controls testing and program development services assist clients in identifying the assets in need of protection, the controls best-suited to protect them against extant threats, and whether control deployments are effective against attacks from all attack vectors. Additionally, Info@Risk assists in developing and refining the organizational policies and procedures needed to sustain the Information Security Program and manage information security risks and incidents. Through the assistance of Info@Risk's services, our clients develop the policies and procedures suited to manage their information security risks and learn whether those policies and procedures are effectively practiced at the credit union.

The difficulty many technologists confront in credit unions and other organizations is building the awareness that information security is an organizational effort requiring the active participation of all employees. All too often, an effective technological control is defeated or circumvented by an employee error or a compromise through a physical or social engineering vulnerability. Building organizational awareness of information security requires comprehensive and clear reporting and documentation of risk management processes and procedures, while avoiding unfortunate "knee-jerk" reactions from those less aware of the threat-filled risk environment confronted every day. Info@Risk's thoroughly documented reports and executive presentations place the credit union's information security risks in clear context, enabling effective risk-based decisions for the whole organization to thereby build organizational awareness and participation in risk management efforts.

The first essential element in effective risk management is to clearly and comprehensively identify the assets whose loss or compromise would most significantly impact the credit union and all the places or processes that access or store such assets. Controls implementation should be guided by this risk assessment and apply mitigation resources commensurate with the risk. To effectively maintain the effectiveness of these controls in an evolving threat environment, it is important to regularly assess the controls from all typical attack vectors.

David Trepp
President & CEO

Info@Risk

Contact Info
www.infoatrisk.com
Phone: 877.328.7475

David Trepp, President and CEO of Info@Risk, has been a technology entrepreneur since 1989. David first led the growth of InfoGroup Northwest (now Presidio) from four employees to the largest independent information systems integrator in the Pacific Northwest. Leveraging his unique experience building information systems, David launched Info@Risk in January 1998, with the single purpose of assessing clients' information system security. Since then, he has led over 500 information security assessment engagements for satisfied customers across all major industries throughout the United States. David was awarded the U.S. Army Achievement Medal in 1982 and graduated with a B.A., Magna C. Laude and Phi Beta Kappa from the University of New Hampshire and holds a M.S. from the University of Oregon.