

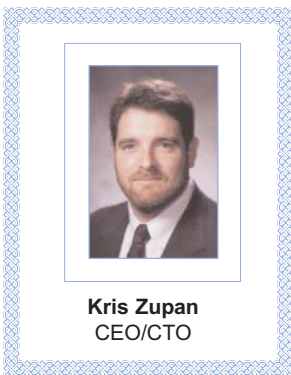
Pay Now or Pay Later: Obtaining ROI from Security Solutions

There usually is no hard and fast ROI on security solutions, because many of them are based on meeting regulations. In this sense, compliance “sells” security and the fact that you are mitigating serious risks naturally offers a great deal of value. Another way to look at it is to ask what are the forensic costs of investigating a data breach if one were to occur? Or what is the cost to the credit union to sustain damage to their brand and reputation?

While the focus a few years ago was on GLB compliance, there is a shift in interest now to the VISA and MasterCard security programs and a big emphasis on disclosures. Every credit union should be familiar with and adhere to the PCI Data Security Standards that the associations have worked together to establish for the protection of cardholder data. Protecting member data has never been more important than right now, and disclosure laws like the California Security Breach Information Act (SB 1386) are gaining in popularity and will ensure that everyone is made aware of security lapses.

One area that is of growing concern among auditors and security personnel is remote vendor access. Virtually every credit union relies on multiple vendors to assist them with maintaining their IT infrastructure. Of course a Virtual Private Network (VPN) is almost always employed, but that merely encrypts the communications link and does nothing to adequately control and monitor the vendor’s access to the credit union’s network. The auditors are starting to call for more scrutiny on what these third parties are doing when they working on the credit union’s systems.

To address this problem, we have developed a unique solution: eGuardPost™. This is the only solution on the market that delivers a simple way to add granular controls to remote system level access to vendors, consultants, outsourcing partners, or telecommuting employees. By establishing a front end proxy server, remote users can be completely controlled and thwarted from uploading any malware onto your internal network. Not only can you define the systems, IDs and protocols that they can access, but you can record their every move for playback at later time. These keystroke logging and session recording capabilities make event reconstruction a very simple process.



Kris Zupan
CEO/CTO

eGuardPost™ runs on top of our Password Auto Repository™ purpose built hardened appliance. When implemented together, they provide an unparalleled level of secure internal and external access for administrators and vendors alike. While we have gained a tremendous reputation for the development of these powerful, innovative and one-of-a-kind security solutions, it is important to remember that we also protect credit unions 24x7x365 via our managed security services division.



Kris Zupan is CEO/CTO of e-DMZ Security and a CISSP. A seasoned veteran in the field of distributed security, Kris Zupan built and managed one of the largest Firewall and UNIX Security deployments while in tenure with a Fortune 10 Financial Services Organization. The UNIX Security Model he established there earned laudatory comments from Regulatory Agencies. Zupan founded e-DMZ Security on his visionary concept of Co-Managed Security Services, building on his extensive experience in providing the highest level of security for practical, 'real-world' applications. He has presented on the topic of UNIX Security and is active on various product advisory boards for security companies.