

Securing the Credit Union from the Inside to the Outside

It's often assumed that breaches always come from the outside. That's not always true. Threats from the inside usually involve sensitive information jumping the credit union's walls. Yes, it can be deliberate, such as when an employee downloads valuable files or data (innocently or otherwise) onto a laptop, jump drive or other device. But more often than not, sensitive data and information move outside unintentionally.

At Diebold, we deliver end-to-end logical security to protect credit unions from ever-evolving threats to their data assets. We work with end users to identify the areas within their credit union that are most vulnerable and develop the solutions that will mitigate threats and stop breaches. Our solutions include custom network, hardware and end user support services designed to protect organizations' information-related assets, as well as the networks on which those assets reside. Diebold also provides identity, credential and access management solutions, providing credit unions the ability to identify, authenticate and manage the individuals who enter facilities, access physical property and leverage logical assets.

A credit union's reputation depends upon the protection of their assets. And we know those assets aren't as easy to define as they used to be. Whether they're physical, logical, tangible or intangible assets, our charge is to help you preserve them. Diebold Security exists to protect your credit union from criminal activity and critical loss, while enabling you to do business in a secure, efficient environment. Our solutions are custom designed to help you secure your business, improve your workflow and increase your return on investment.

When you work with Diebold, you become part of a global team focused on making your business more secure and more efficient. Diebold Security is part of Diebold, Incorporated, a global leader in integrated self-service delivery and security systems and services. The Diebold team includes more than 16,000 associates with representation in nearly 90 countries worldwide. As a security integrator, Diebold strives to deliver innovation in converging and connecting systems—both legacy equipment and today's newest technologies—to enable optimum security, interoperability, efficiency and return on investment.

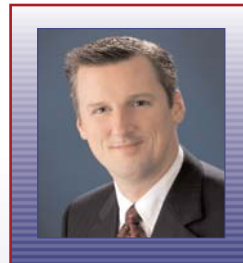
The only security integrator in the world with a 150-year history in physical security, Diebold complements that skill set with a deep understanding of logical security tools. Through the expert application of advanced technology, Diebold's security professionals can solve the most challenging security issues. Our holistic approach helps end users build security programs that protect their five key assets: 1) Facilities; 2) Staff; 3) Networks/data; 4) Equipment; and 5) Members.

To enable the protection of those assets, Diebold serves as a consultant to end users to help them:

- Identify areas of their organization that are most vulnerable
- Assess and prioritize which real-world threats would have the most significant impact on their physical and critical information assets and determine the likelihood of each risk occurring within the organization
- Develop a holistic security strategy designed to integrate physical and logical tools to protect the organization's assets
- Deploy efficient solutions and mitigation strategies that will keep assets safe and demonstrate an ongoing commitment to reducing risk
- Manage and monitor the overall maintenance of the security program
- Integrate, manage and monitor physical and logical security operations

With a deep understanding of your specific environments and security objectives, Diebold builds custom solutions that meet your unique needs. Those solutions come in the form of powerful and seamless end-to-end systems that incorporate a variety of security tools, including alarms and access control, credential management, video, barrier equipment, safes and vaults, logical security systems and more.

B. Scott Harroff Chief Information Security Architect



Scott Harroff is responsible for leading Diebold's logical security initiatives, ensuring that products and services are consistent in their information security architectures and that they meet the necessary logical security standards. He also is responsible for identifying digital security solutions and partners that complement Diebold's physical security solutions and expand the company's offerings in the logical security space.

Prior to his current role, Harroff served as information security officer. He was responsible for the protection of networks, systems and information assets in an increasingly complex environment. He was also responsible for developing and deploying a global security architecture that can effectively support business growth and ensure secure communications for Diebold associates, customers, suppliers and other stakeholders.

Prior to his current role, Harroff served as information security officer. He was responsible for the protection of networks, systems and information assets in an increasingly complex environment. He was also responsible for developing and deploying a global security architecture that can effectively support business growth and ensure secure communications for Diebold associates, customers, suppliers and other stakeholders.

Contact Info

www.diebold.com