

## Protecting Customer Data at Rest and in Motion

In today's ever-changing world of information technology, new threats emerge every day. For years there have been the staple threats such as viruses and Trojans. While emphasis on the risks of external technical threats still exists, the threat of disclosure of non-public customer information by "insiders" is one of the biggest and often overlooked security issues facing banks today.

Also, gone are the days of hacking for fame ? now it's all about fortune. In today's world, information is currency. Invariably, wherever information exists that can easily be converted to money, attackers will go. Current statistics support this trend:

- " Identity Theft is at an all time high and continues to rise year after year.
- " Breaches occurring from "insiders" continue to rise. Fifty-one % of insider breaches come from IT Administrators.
- " Organized crime rings are arranging for customers to be hired at financial institutions in order to steal information.
- " As stated in a recent Verizon Security Report, 39% of security breaches come from business partners.
- " Phishing continues to be a huge problem for banks, and this trend will continue as long as consumers continue to fall victim to these attacks.
- " Trojans that steal log-in credentials to online accounts are on the rise.

There is a security issue with mobile account services that causes concern for consumers. Mobile devices, after all, are portable, and that makes them much more prone to being lost or stolen. Banks need to make sure that they have all means of security in place when offering this service to customers, so that the convenience is worth the risk.

There is no "silver bullet" to securing the information assets of a bank. There are multiple processes and multi-layered approaches to guard critical data and repel malicious attacks from both the outside and inside an institution's network. 24x7x365 real time managed services, correlation, and monitoring of the Internet, firewalls, servers, and other critical components help protect customer information in the most effective manner. Never depend on just one layer of monitoring.

Clear policies and procedures are also important to implement and enforce. Important security related projects include the ID Theft Prevention Policy, Risk Assessment documentation, and security awareness training for employees (at different levels) complement a strong real time security monitoring program and can be very effective tactics to help protect confidential customer data from getting into the wrong hands.

Gladiator understands that information security is a process, not a "product." We offer Enterprise Information Security Solutions products and services in 5 key areas:

- " CoreDEFENSE Managed Services that includes Firewall Monitoring and Management Services; Network Intrusion Prevention Services; Server Intrusion Prevention Services and Event Log Analysis; Comprehensive Reports; Performance Monitoring & Patch Management Services)
- " eShield (email filtering and encryption)
- " IT Regulatory Compliance (ITRC) Policy Products/Services:
  - Network/Internet Systems & Security Manual
  - Information Security Program
  - ID Theft Prevention Policy
  - Remote Deposit Capture Policy
  - Compliance Services Package and custom Policies/Procedures
  - eSAT (electronic Security Awareness training)
- " Consulting Services such as Vulnerability Assessments, Penetration tests, Security Assessments and ITRC Consulting Services
- " ISO Training

These services provide a solid and dependable set of integrated solutions to help banks protect their customers' information and their reputation.



**Danny Johnston**  
Group President

**Danny Johnston** is group president of Gladiator Technology, a ProfitStars Solution. Danny oversees the strategic direction, financial management, and marketing efforts for Gladiator Technology. With an impressive 30 years of business experience in the financial services industry, Danny is skilled at helping customers make well-informed, solid technology decisions in defining financial institution network and Internet security requirements. He guides strategy implementations that better equip banks and credit unions with the proper resources to meet federal requirements and achieve maximum information security levels. A well-known expert in his field, Danny is a sought-after speaker on topics regarding information security, risk assessments, and financial regulatory expectations.