

Protecting Customer Data at Rest and in Motion

When considering data loss, most people think of hackers - criminals who, instead of breaking into a safe at a local bank to steal money, use a computer to break into a network to steal account information and eventually money. The threat from hackers is real. However, it's not as common as you might think. According to the Identity Theft Resource Center, hackers account for less than 12% of all data loss incidents.

While the threat from outside the organization is real, more records are compromised when data loss occurs at the hands of insiders – by a ratio of 10 to 1. The reasons are understandable but often ignored because many organizations have not established an effective balance between what information is needed by the employee (or partner, consultant, vendor, customer, etc.) to do their job and what information should be protected. Most organizations take the “ostrich” approach of sticking their heads in the sand and don't realize that it only takes one data breach to become public before all customer confidence is lost and customers take their business elsewhere.

Protecting customer data involves multiple layers of security practices and technologies. Both preventative and detective measures are needed. The solutions fall into three broad categories – (1) having a well thought-out security framework to address technical and non-technical solutions, (2) having a well structured network to segregate data from outsiders and even insiders, and (3) implementing technologies that effectively control access, protect data and monitor its use.

Documented security policies are fundamental in an effective security program. They provide a framework for implementing technical and nontechnical controls. There are several sources for best practices (e.g., NIST, ISO, COBIT, etc.). While policies are critical, equally as critical is raising security awareness through training and communication – the most important tool in preventing data loss by employees. A comprehensive policy framework enables banks to make informed decisions about which solutions best address their risks. While this sounds overwhelming, spending a few weeks to establish a policy framework can save millions of dollars resulting from a data loss.

Once the security framework is developed, organizations can focus on the technical solutions to (1) control access, (2) manage activities, and (3) monitor usage. Banks can best manage data through a well structured network that controls access to various applications, network zones, and/or devices through the use of passwords and biometric validation. Organizations that structure their networking around the data that is needed to perform a particular role can most effectively manage activities and ensure that all users have access to the data they need to serve customers. Conversely, employees cannot access data that may compromise the security of the organization. Finally, technology should be implemented to monitor usage and control how (encrypted nor not), where (what devices, locations, ports), and when (time of day or month) data can leave the network.

Technical solutions break down into access, data at rest, data in motion, and monitoring. Users need to be authenticated before getting access to customer data. This can involve two-factor (tokens, biometric) authentication. Devices can also be authenticated before getting network access. Encrypting customer data is also crucial. Whole drives, individual files, and database elements can be encrypted, making stolen data worthless. Encrypting data transmitted across internal networks or the Internet is also important to prevent “sniffing” or “man in the middle” attacks.

Finally, an exciting new technology, port protection, combines several defenses into a software client that plugs data leakage on PCs. These “port protectors” control which users can transfer data via USB ports, wireless networks, etc. and even enforce encryption policies. Unfortunately, no single technical solution can eliminate the risk of losing customer data. However, a comprehensive approach, incorporating technical and nontechnical measures, can reduce and manage your risk.



Keith Young
Practice Manager

Keith Young is ICS's Executive Practice Manager, leveraging his 10+ years as an information technology and security professional to lead a team of consultants to solve organizational, technical, and people-related challenges to deliver real world security solutions to federal, state, and commercial organizations. Mr Young's broad background includes experience as a consultant, IT manager, security engineer, researcher, and instructor working with credit unions, banks, and some of the largest financial services institutions in the world. Mr. Young is a Certified Information Systems Security Professional (CISSP) and holds a Master of Science degree in Industrial and Organizational Psychology from Auburn University.

