Protect Your Knowledge Base: How to Put Together A Workable Security Plan

All men by nature desire knowledge.

Aristotle, c. 360 BC

Knowledge is power.

Francis Bacon, 1597

Knowledge must come through action.

Sophocles, c. 442 BC

Knowledge is one thing, virtue is another.

John Henry Cardinal Newman, 1873

History's most effective leaders have always understood the value of knowledge. In any competition, superior knowledge gives us a strategic edge, and allows us to make informed decisions when our opponents are just guessing. From grammar school through all ages and walks of life—in politics, war, business, sports and retirement — clear knowledge is the foundation of actions that result in success.

How often do we muse over the advantages we would gain if we could only be "a fly on the wall" in a certain place and time? How much cash might certain information be worth? And how far would our rivals go to get information about us? With the proliferation of knowledge on computers and laptops, corporate espionage is a much larger industry than you might think.

By early 2002, the street value of an executive's laptop computer — a grab bag of information about a given firm — was placed at $35,000. Multiply that by the number of laptops circulating in a large organization, then consider all the additional knowledge residing on desktop computers and networks, and it doesn't take long to see that even a small firm's knowledge base is an asset worth millions. In most cases, the organization's entire future hinges upon its secrecy.

Knowledge Up for Grabs

Whatever the industry, inside knowledge is in high demand. And it's readily available on company networks, laptop computers and in wireless communications.

- **In any industry**, rivals may seek information to (1) determine the competition's business strategy and key players, (2) undercut a competitive situation, (3) expose company secrets, or (4) coerce concessions.
- **In healthcare,** compromise of patient records can represent an invasion of personal privacy that may also impact insurability decisions and result in litigation. If negligent, the institution or practice may be exposed to criminal and civil prosecution.
- **In the insurance industry,** compromise of customer records can also represent an invasion of personal privacy that in turn may impact insurability decisions and result in litigation. If negligent, the firm may be exposed to criminal and civil prosecution.
- **In the financial services industry,** compromise of customer records can also result in invasion of personal privacy and fraud. If negligent, the firm will be responsible for fraudulent transactions, and may be exposed to criminal and civil prosecution.
- **In the telecommunications industry**, interception of customer communications or records can lead to fraudulent account usage, and expose the company to significant loss. The provider may also be liable for intrusions into the customer's privacy and any resulting losses.

Elements of a Comprehensive Security Solution

Because threats to information security vary from one field or discipline to the next, and may come from so many quarters, a one-size-fits-all answer often just isn't realistic. When you conduct a front-end evaluation of your own networks and business situation, you'll assess the kind of information you need to protect, and from whom you need to protect it.

You're likely to determine a need for some or all of the following forms of security:

- **Encryption.** By encrypting data on computers and in communications, you protect:
    - E-mail and other electronic messages and transactions from Interception, opening, and alteration by unauthorized persons.
    - Access to information on networks.
- **Secure Logon.** With secure logon, you require that persons who gain access to information identify themselves, usually with a personalized card or token and a secret password.
- **Remote Network Access Control.** Remote access control limits access to your network from off-site locations to those who submit correct identification.
- **Authentication/Non-Repudiation.** A function of "public key cryptography." authentication and non-repudiation assures that no party taking part in an electronic transaction can deny their involvement.

Critical Decisions for a Comprehensive Security Solution

After you've decided what information you need to protect, and determined the reasons you need to protect it, you'll want to review the capabilities and features you require to achieve the appropriate level of security.

To maximize your return on investment, you're likely to examine the following issues:

- **Cost Effectiveness.** To get the most "bang for your buck," you'll want to select a solution that can meet your needs without outstripping your future requirements.
- **Scalability.** As you grow, you'll need a system that can adapt to new and expanding requirements.
- **Flexibility.** You'll want to identify across-the-board solutions that are compatible with all of your current and anticipated applications, systems and hardware.

Solution Components

Individual Functions

Typically, to protect its data flow and knowledge base, organizations require a combination of solutions to perform some or all of the following functions:

- **Encrypt and Accelerate On-Line Transactions**
  For organizations that process customer transactions via the Internet, establishing a "Secure Sockets Layer" (SSL) connection accelerates processing on your server while strongly encrypting sensitive information.
- **Secure Logon**
  Secure logon identifies those who attempt to access your organization's computers.
- **Control Network Access**
  Network access control identifies those who attempt to gain access to your organization's internal networks.
- **Preclude Physical Tampering**
  Even if you protect your network from external attack, you remain vulnerable to physical tampering to obtain encryption keys. A fully secure network, then, also requires protection of its physical components.

Issue	Solution	Benefits
Transactions Encryption and Acceleration	 CryptoSwift PCI Cards	Encrypt and process more than 1,000 secure server transactions per second
	 NetSwift 2012 High Security Appliance	Additional encryption/acceleration performance. Operable where PCI slots are unavailable or unusable.
Secure Log-on	 iKey Smart Token	Token-and-PIN user authentication at Windows log-on and network access.
Preclude Physical Tampering	 CryptoSwift HSM	Erases critical information upon detection of tampering. Solid shell shelters the web site's digital credential and is inviolable without creating tamper evidence. Also accelerates server performance.
Higher-Assurance Authentication	 iKey 2032 Token	With the private key is sheltered in the device, provides on-board key generation and signing for fail-safe token-and-PIN user authentication. Tamper-evident option creates evidence to betray any physical intrusion attempt.

Rainbow Technologies' Solutions for Knowledge-Base Security

- **Implement extremely high assurance**
  If your network or computing requirements call for extremely high assurance in user identification, you'll want to consider a tamper-evident token that protects encryption keys.

In the remainder of this report, we'll examine practical components available today to build a total solution to protect your knowledge base.

SSL Encryption and Acceleration of Online Transactions

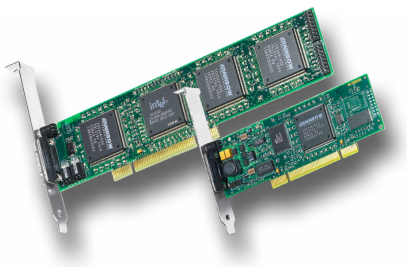
When you need to protect on-line financial transactions and transfers of critical information, a SSL is the most effective and comprehensive solution available.

CryptoSwift: Industry's Leading SSL Solutions

Although your choice will depend upon your network's configuration, Rainbow's CryptoSwift solutions offer the industry-leading SSL acceleration solutions in either form factor:

- CryptoSwift PCI-based accelerator boards for Web servers.
- Standalone acceleration appliances.

CryptoSwift has secured more transactions than any other SSL acceleration device in the world.



CryptoSwift PCI Cards

Rainbow PCI CryptoSwift cards are ideal for companies with intensive transaction processing and all Web-based server traffic.

With the ability to process up to 1000 secure transactions per second, Rainbow's CryptoSwift® eCommerce accelerator delivers the responsiveness that online customers demand.

At the same time, Rainbow's CryptoSwift eCommerce Accelerator frees up your servers, allowing them to process orders and transactions, increasing throughput and minimizing customer wait time. With CryptoSwift, it's cost effective to deploy security everywhere, and customers can take advantage of 24/7 online service without concern for loss of privacy.

SSL Acceleration Appliance

When PCI slots are unavailable or unusable, or additional performance is required, Rainbow's SSL acceleration appliance provides extremely wide-ranging processing power.

The Rainbow NetSwift2012 high-security appliance:

- Provides the fastest WTLS and SSL transaction performance available in a single unit
- Combines an integrated security acceleration and termination solution for mCommerce and eCommerce applications.
- Incorporates both the WTLS protocol for WAP gateways and high-speed SSL for Web servers in a single, plug-and-play security solution
- Can be installed and configured in minutes

Secure Windows 2000 Logon

Until the release of Windows 2000, Interactive Logon required the user to enter a username and password. In a real breakthrough for PC security, however, Windows 2000 allows user authentication through Rainbow's iKey USB tokens.

Before booting, Windows users insert an iKey token into a standard USB port, as though it were a key to unlock access to the PC. Then, instead of running the standard 'CTRL+ALT+DEL' attention sequence, Windows requests the user's PIN. Only after inserting the iKey and providing the correct PIN can the user access Windows.

The iKey stores the user's Public Key Infrastructure (PKI) credentials. Once successfully logged-on to their PC, authorized users can roam freely within the network from any workstation—a very flexible deployment of systems and users.

The Windows 2000 Active Directory supports PKI using "X.509" Digital Certificates. Both the iKey 1000 series and iKey 2032 can store these Certificates, which can be used for Secure Windows Logon, Secure Web Authentication/ Access and Secure eMail.

Preclude Physical Tampering

Even with networks protected from external attack, you remain vulnerable to physical tampering to obtain encryption keys. A fully secure network, then, also requires protection of its physical components.

HSM hardware stores a server's key within an enclosure that protects it from physical tampering. Encryption and decryption of sensitive information takes place inside the HSM, and all information is automatically erased if any physical tampering occurs.

CryptoSwift HSM

CryptoSwift HSM protects your critical electronic data like a safe protects your valuable belongings. The device is a PCI-based add-on card with a tamper resistant cover that prevents access to the sheltered circuitry. Should an intruder physically attack the HSM, its tamper active design immediately erases all sensitive data automatically.

In addition to data security, when installed in a Web server, CryptoSwift HSM accelerates the performance. It protects a Web site's digital credential by keeping the signature within the CryptoSwift HSM's security boundary.

For maximum performance and security, all digital signing and verification processes take place inside the HSM, and all keying material is encrypted before it leaves the HSM. With its tamper-active design, CryptoSwift HSM defeats physical attacks through detection and response. Token-and-PIN authentication takes place through a trusted channel via a standard USB port, with Rainbow Technologies' iKey device.

Higher Assurance Authentication

If your user authentication requirements call for extremely high assurance, Rainbow's iKey 2032 token supports on-board key generation and signing. As with the CryptoSwift HSM, the private key never leaves the iKey. For even greater security, a tamper-evident option (FIPS 140-1 Level 2 certification) is also available.

The iKey 2032 provides a reliable, robust security solution that is easy-to-use and administer, yet provides exceptional PKI-based security solutions for desktop applications for the Internet, eCommerce, extranets and corporate intranets.

By removing certificate storage and digital signature signing functions from the desktop and placing them within the token, the iKey 2032 significantly reduces the risk of internal or external security attacks. Through user-identification data contained in each device, network administrators can grant or deny access based on the user's authorization level.

The iKey 2032 supports enterprise, business-to-business and business-to-consumer applications built on all major PKI systems. It provides not only on-board cryptographic key generation, but also secure storage of key pairs and X.509 digital certificates.

Each token features 32K of memory to more easily store and manage digital certificates and digital signatures.

Putting It All Together

From so diverse a menu, you're bound to find just the right combination of solutions that protect your knowledge base. For example:

- **For tamper protection and desktop access control,** consider iKey for Windows 2000 logon and HSM for secure key storage.
- **For transaction security and tamper protection,** consider CryptoSwift PCI cards or NetSwift2012 for transaction protection, and CryptoSwift HSM for secure key storage.
- **For PKI and Higher Assurance functions,** consider iKey2032 for private key protection, and HSM for secure key storage.

Going Forward

We hope this report has helped you understand the need to protect your knowledge base, and the solutions readily available today. Rainbow Technologies and its Mykotronx and Spectria subsidiaries stand ready to lend their expertise in determining and implementing a fully-integrated solution, ensuring that your knowledge base is secure and accessible—no matter what your specific requirements.

There is nothing so captivating as new knowledge.

Peter Mere Latham, c. 1850