PLANNING ASSUMPTION

March 15, 2001

Optimal Extranet Security: A Methodology

Steve Hunt

Contributing Analyst: Philip Rosch

Giga Position

One of the great challenges for large, distributed organizations is the rapid creation of practical and enforceable, risk-based security policies for extranets. Various business units, with degrees of sovereignty, often create their own ad hoc policies, leaving the company with limited means to coordinate security.

A methodology for promoting and enforcing an extranet security policy across business unit and organizational boundaries will require three phases: the questionnaire, the implementation and the review. The first phase entails asking business units and partners to respond to questions regarding levels of risk. The second phase applies corresponding protection levels to the actual application servers, firewalls, Web servers and other elements of the architecture. The third provides a method of oversight and measurement.

By following these three phases, an organization may roll out a broad and diverse extranet with consistent and appropriate levels of risk protection.

Proof/Notes

A secure extranet is achievable with modest effort and cost. The chief requirements are not time or money, but coordination, education and communication. By working together, business unit managers, IT staff, risk managers, auditors and security managers may all contribute their parts to an overall security architecture. If these players do not coordinate their communication, the simple building of an adequate policy will be costly and perhaps impossible. Furthermore, a comprehensive security implementation will be out of the question.

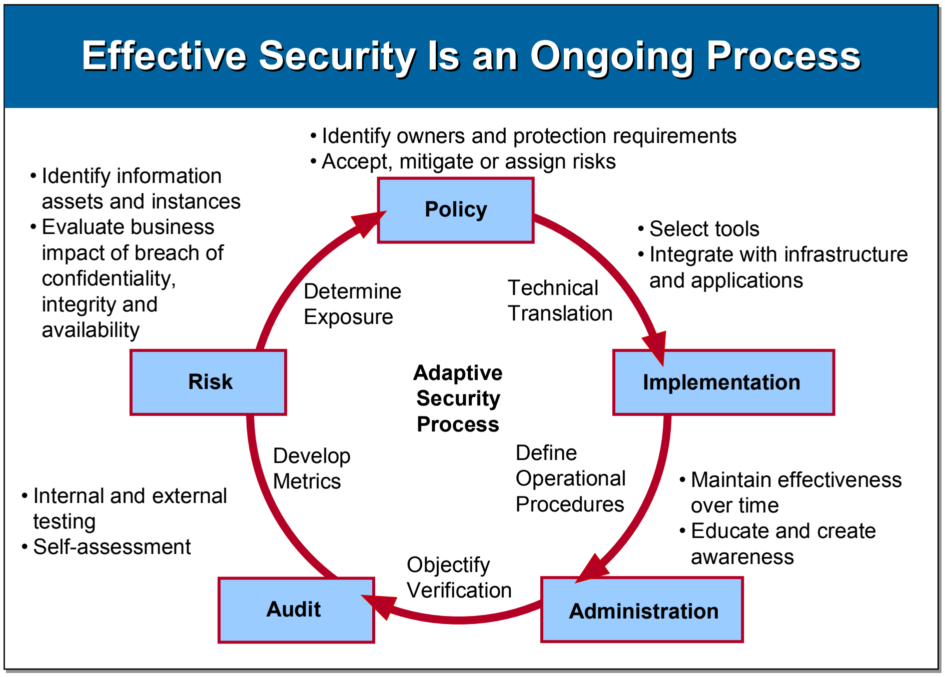
Someone, maybe a business unit manger or security manager, will be tasked with mitigating risk in any extranet initiative. Therefore, setting up a Web-based application, a document delivery service or a data warehouse will commonly include a few security-like measures, but no overall view of risk management.

Having said that, it is important to note that any methodology, such as this one, can only be incomplete. This methodology must be customized and expanded to meet business and technical requirements that are not expressly detailed in these pages.

Building and implementing a security posture is more art than science. Security, quantified as risk, has not only technical and business impact, but is largely emotional as well. Owners of data and business initiatives may not be able to tell you how much security they need, but they certainly can tell you how little they can live with. So intuitive, gut responses to a simple questionnaire will indicate a reasonably accurate level of risk tolerance.

The Questionnaire

Giga's concept of the four categories of security, known as the "four As," incorporates all elements of a security posture. A questionnaire designed to surface business requirements around these categories — authentication, authorization, administration and audit — may therefore be a creative approach to risk assessment and improved communication with the business units (see Figure 1).



Effective Security Is an Ongoing Process

- Identify owners and protection requirements
- Accept, mitigate or assign risks

Policy

- Select tools
- Integrate with infrastructure and applications

Technical Translation

Implementation

Define Operational Procedures

- Maintain effectiveness over time
- Educate and create awareness

Administration

Objectify Verification

Audit

- Internal and external testing
- Self-assessment

Develop Metrics

Risk

- Identify information assets and instances
- Evaluate business impact of breach of confidentiality, integrity and availability

Determine Exposure

Adaptive Security Process

Source: Giga Information Group Figure 1

Every business unit manager or application owner should be presented with a series of questions — perhaps as few as two or three, or up to dozens per category — depending on the technical savvy of the participants. The responses will be tallied and scored as to a level of risk. Those risk levels will then be applied to the development of policies leading to the implementation of the next phase.

Include questions that indicate the level of confidence the application owner needs. Beginning with authentication, the respondent should consider the degree of confidence required that the human being accessing the system truly is who he or she claims to be. While it may seem obvious that all users should be properly identified, there are levels. For example, a low-risk application may be protected by passwords. And while a password may be shared — and identity thereby compromised — the risk is low and tolerable. A better example may be online purchasing. Identity is commonly not required at all — only a credit card number is. That is because the identity of the human being at the end of the transaction is nearly irrelevant, as long as the credit card number is valid. Each of the four categories may be approached in this way.

The wording of the questions should follow the culture and conventions of your own company; yet, the simpler and clearer the wording of the questions, the more accurate the responses. Ranking responses along a simple five-point scale is the easiest for the respondent and the most effective for scoring risk levels later. Therefore, questions should be posed in the format: “On a scale of one to five, with five being the highest...“ Of course, include as many questions as required.

Authentication — Who Are You?
To what extent do you have physical control over the end user‘s system (laptop, PC, terminal, personal digital assistant (PDA), etc.) used to access your application?
To what extent can you maintain and configure software on the end user‘s system?
To what extent do you have legal or corporate influence over the end user? (The point of this question is to determine whether end users are under a legally binding contract, or corporate human resources policies; in short, can you fire or sue them?)

These previous three questions are directed at determining the minimal level of control over the user. As control of a user increases, so do the options of authentication types. For example, an employee using a corporate PC may be obligated to use special client software or to follow rigorous password policies. Selected business partners who are named and under contractual obligations may similarly be obligated to use software for registering and authenticating, but managing those nonemployees remotely will prove to be more difficult. Additionally, as control decreases, the ability to distribute and manage physical tokens or certificates will be compromised.

To what extent should an end user NOT be allowed to share authentication credentials (with a colleague, secretary, officemate, etc.)?
Questions along these lines indicate the degree to which the authentication method must be tied to the individual. As scores for this question increase, so does the requirement for nonrepudiation (see Glossary). For example, a user who must not be allowed to share credentials must, therefore, be obligated in some way to use a token or password that may not be shared. Biometric authentication is the type that is most binding to an individual (see Table 1).

Table 1: Authentication Types and Their Appropriate Uses

Authentication Type	Appropriate User Population
Passwords	Any user population
Passwords with single sign-on	Employees or extranet partners and customers with previously existing profiles
Digital certificates	Employees, plus a limited number of extranet partners and customers with previously existing profiles. Limited value when used exclusive of another authentication type.
Personal identification number (PIN) tokens	Employees, plus a very limited number of high-value customers and partners
Smart cards	Employees, plus a very limited number of high-value customers and partners
Biometrics	A subset of employees; must be used in conjunction with another authentication type listed here.

Source: Giga Information Group

Authorization — What May You Do?

Assuming any transaction may be viewed or intercepted by an unauthorized user, how much risk to the company does any single transaction represent?
This question, and any like it, drives toward a requirement for encryption of data in transit. Low scores would permit the transaction — such as a viewing of the corporate home page — to be performed in the clear. Higher scores indicate the need for deployments of Secure Sockets Layer (SSL) or virtual private networks (VPNs).

Assuming an unauthorized user may alter words, graphics, links or numbers on a Web site, how much risk to the company could a small, unauthorized change make?
Here we are getting at the sensitivity of content served over the network. Nearly all data on a Web server is at some risk of unauthorized modification. Hackers make headlines every month by successfully altering content on Web pages. As risk of such a hack increases, so does the need for Web content protection measures.

Assuming an unauthorized user may be able to execute commands, or make changes to the Web server itself, how much risk to the company could that represent?
Again, as risk of hacking the operating system increases, so does the requirement for system hardening.

Administration — How Do We Manage It All?

To what extent is the user population made up of multiple legal or corporate entities?
The point here is if the end users work for different business partner companies, then a single administrator will have greater difficulty managing the addition, suspension or deletion of user IDs. The higher the score, the greater the need for a distributed and coordinated administration model (see IdeaByte, Extranet Partners — Good Fences Make Good Neighbors, Philip Rosch).

Within your own corporation, are there fewer or more groups who are affected by adding or removing users from your system?
Again, higher scores on the questionnaire indicate a greater need for coordinated and swiftly executed administration.

Are their few or many variations to the access privileges of the users?
The more complex the privileges, the greater the need for role-based administration (see glossary).

Audit — What Happened?
How important is it to know whether a malicious or anomalous event has occurred in your system?
For some systems, the data is of such low value, or relative insignificance, that an unauthorized usage is not urgently important. But for most systems, unauthorized access or modification could lead to embarrassment and damage of the company's reputation.

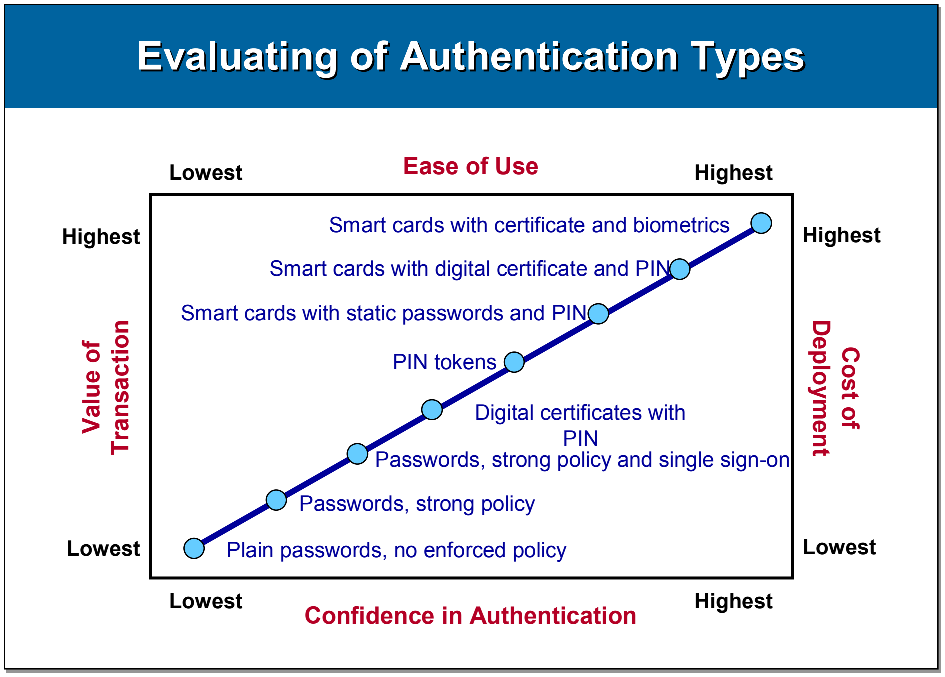
How important is it to see trends such as usage errors, failed log-in attempts, general user behavior, etc.?
Most business managers will be concerned with usage trends.

How important is it to respond to a malicious or anomalous event very quickly?
Incident response can range from logging an event in a report, to breaking a logical connection, to involving law enforcement for criminal offenses.

To what extent do you need to anticipate malicious usage?
Anticipating malicious usage properly requires a complete, formal risk analysis by a competent security auditor. A vulnerability assessment using scanning software or by hiring an outside firm is a somewhat useful endeavor.

The Implementation

Authentication
Passwords are the easiest authentication type to use and deploy. In most cases, however, they are also the most vulnerable to compromise. Users, when left to their own devices, tend to make passwords very easy to remember — and therefore, to guess (see Figure 2). Typically, users also write down their numerous passwords in an accessible place near the computer (see Planning Assumption, The Whys and Means of Online Authentication, Andrew Bartels).



Source: Giga Information Group

Figure 2

Obligating a user to conform to a password policy lowers the risks of password abuse and compromise. Adding a number or two, and a special character, and mixing upper and lower case letters are good examples of policies that reduce the "guessability" (see IdeaByte, Good Password Policies, Steve Hunt).

Single sign-on technologies also decrease the risks associated with passwords. If users only have to remember one password, then they are much less likely to write it down and more likely to make it a good one. Combining single sign-on with a good password policy makes for the optimal use of passwords. Leading vendors for single sign-on for browser-based extranet users include **Netegrity** and **Securant Technologies**.

Tokens, digital certificates, biometrics and smart cards are authentication types of increasing degrees of risk mitigation and deployment complications (see Table 2) (click here to see Table 2). Each type requires an authentication infrastructure consisting of methods of registering users, suspending and revoking user privileges and sharing credentials across target applications. So, consider whether multiple authentication types will be used across the extranet and then select an infrastructure vendor that can streamline the process for them all.

Authorization

Securing the Session

Some transactions may be made in the clear, with no additional access controls. Many informational Web sites deliver content that does not include private or sensitive information. Some other transactions include data that is valuable only for a few seconds, in which case, the need for session security is minimal. For confidence that data is secure for at least a few minutes, or perhaps hours, a standard implementation of 48-bit SSL, available from your Web server provider, is satisfactory (see Table 3). Standard SSL necessitates a certificate on the host Web server only. A stronger way to implement SSL is by distributing digital certificates to all users, thereby establishing mutually authenticated SSL. Conversely, altering human resources information or making a modest-value financial transaction calls for 128-bit SSL.

Table 3: Suitability of Security Methods

Security Method	Suitability
Clear text	Suitable for low-risk, public information
48-bit SSL	Suitable for private information of modest value, such as billing data, human resources changes, etc.
128-bit SSL	Financial transactions, health-care data, some human resources data, contracts and legal documents
Mutually authenticated high-bit SSL	Moderate-to-high valued data shared between two parties with some frequency
Site-to-site VPNs	Recommended for high-value transfers of data between corporate business partners. Note that these VPNs do not secure data within the respective local networks.
Point-to-point VPNs	Recommended for very sensitive data that should never be unencrypted during transit, including financial or health-care transactions, some legal documents, sensitive product plans and drawings, etc.

Source: Giga Information Group

Protecting Content

Web applications suffer from native vulnerabilities. That is, the natures of Web protocols (HTTP) and the browser languages (HTML, CGI, Java) combine to open several undesirable avenues for unauthorized access. Developing application code with access control in mind is helpful, but not complete. The integrity of data being viewed on a Web site can only be guaranteed with a proxy. **Sanctum** makes AppShield, a useful proxy designed to eliminate all common Web content hacks. Other vendors in this category include **Gilian**, **ClickNet** (now **Entercept Security Technologies**) and **Qiave** (acquired by **WatchGuard** in 2000). Qiave is a handy method for limiting data to a read-only designation. Gilian and ClickNet have deficiencies that exclude them from Giga's recommendations.

Hardening the Operating System

Beyond protecting content, hardening an operating system eliminates unnecessary risks related to violation of the underlying operating system, or using operating system commands to foil the security of an application. For example, hackers may install Trojan horse software and launch attacks on the network and data while hidden under the covers of an off-the-shelf operating system. Qiave and ClickNet sell limited products designed to ease or streamline the hardening of an application server, but they are recommended only in very specific conditions.

Giga recommends using hardening and isolation/insulation techniques designed for each specific application server, for best results. Contact Giga for more information on the methodology of hardening the systems your company uses.

Protecting the Link to the Back Office

At some point during a standard Web-based transaction, there may be a call to a back-office system — perhaps a database, the mainframe or another application server. That connection might cross a network boundary: for example, from the demilitarized zone (DMZ) (see Glossary) to the trusted network or local area network (LAN) (see Glossary). In that case, some intermediary authorization measure should be installed. For most links to the back office, the most efficient and effective is **Whale Communications**' e-Gap (see Planning Assumption, Securing the Extranet Web Application, Steve Hunt).

Administration

Security staff and business managers alike will benefit from the deployment of a coordinated administration console like **BMC**'s Control-SA or **Systor**'s SAM. **Access360** is struggling to make a name for itself with an intense marketing effort, while the functionality is inferior to the other two products. Products in this category ease administration and make it more efficient. Adding a user profile one time will trigger the automatic publication of that profile to all required systems: e-mail, Unix servers, **Lotus** Notes, **Oracle**, mainframes, etc. Similarly, user suspensions, ID revocations and modifications are equally automated. Unfortunately, these are elaborate and high-priced systems. Only corporations very serious about increasing efficiency and security will invest in a leading product of this type.

For most Web-based extranet applications, on the other hand, there is a lighter point solution. Netegrity and Securant Technologies, listed above as single sign-on vendors, provide adequate privilege management to browser-based users. For this limited population of external users, these products are recommended. All of these products support role-based administration (see Glossary).

Audit

Nearly every system connected to your network produces a native event log. **Hewlett-Packard** (HP) Openview, **Computer Associates**‘ (CA) Unicenter TNG, **Tivoli** and BMC have event management consoles that may collect many of these events and produce customized reports. However, none of these products is easy to customize for security use. Therefore, we recommend security-specific log collectors from **e-Security**, **Raytheon**, **Internet Security Systems** (ISS) and **Consul Risk Management**.

But herein lies the catch. To collect audit logs assumes you know what to do with them. Most audit events are very granular and detailed — not something that a casual viewer would interpret accurately. So, auditing requires not only a way of consolidating logs and filtering up the important events, but also assigning skilled engineers to review the logs and respond to malicious or anomalous events decisively — an expensive and difficult strategy.

Of course, these collected logs could simply be stored away on tape until a security or performance event makes it necessary to review the previous days or weeks of data. And that is an acceptable approach, assuming the risk of more frequent threats is not great. But consider that if the data is worth archiving at all, it is worth a cursory pass with an audit tool.

You may find, however, that the only way to ensure the confidentiality, integrity and availability of your systems is to monitor the logs more actively and constantly. If that is the case, then hire, train and fund a monitoring and response team (Giga can provide instruction) or seek an outsourcer to do part of the task.

Counterpane, **Telenisus**, **Riptech**, ISS and dozens of other firms offer variations on the theme of managed security monitoring and incident response. Bear in mind that it is not recommended (and, arguably, impossible) to fully outsource security monitoring and response (see Planning Assumption, Outsourcing Security Is a Reasonable Option in Certain Situations, Steve Hunt).

One more option lies under the heading of audit: proactive vulnerability assessments. Giga recommends that vulnerability assessments be run with great caution. Usually such a scan uses software that searches a network segment for points where security may be breached. These scans can be very disruptive of the network performance and may actually damage systems and production software. Moreover, if an outside firm runs the scan, the price can be exceptionally expensive, with very little return on the investment. That is, 80 percent of the lengthy report these scans present you with consists of nothing more complex than the exposure of bad passwords, system patches that are out of date, ports and services enabled that shouldn‘t be and unauthorized modems. The remaining 20 percent are often esoteric and of low relative risk to your network or are very expensive to remedy. In any case, a coherent security posture will properly mitigate all relevant risks without the cost or damage of a vulnerability assessment.

If you still prefer to know what vulnerabilities are out there, then you are advised to scan and assess only segments of the network at a time. Do it with the full awareness of network administrators, system engineers, auditors, business managers and security staff. Scans should be scheduled during anticipated times of decreased network activity.

The Review

So, how will you know if the extranet security architecture is doing what you expect? Review it periodically. Engage your own risk management team to devise a customized method of collecting reports on the authentication, authorization, administration and audit features of the architecture. In any case, the review will have the following basic components:

- Baseline metrics (where you started)
- Aggregated ongoing operational metrics (trends compared to plans)
- Gaps (areas where behavior modification is necessary)
- Service-level metrics (as articulated in the extranet contracts)
- Emerging business requirements

The objective is continually to reduce the gap between policy and actual practice.

Alternative View

Two trends may detract from the recommendations in this Planning Assumption: the growth of outsourced security services and the consolidation of application servers with security features. It is possible that consulting firms and security specialty firms of several types may develop “packaged“ proposals for extranet security incorporating all of the facets discussed here. The provider would integrate all of the technologies, manage them externally, administer users and their privileges and respond to all security and performance incidents. In fact, one vendor, **Aventail**, is already marketing such a system, and **Commerce One** is shipping with Netegrity‘s Siteminder bundled and integrated.

Additionally, extranet application servers from **SAP**, **BEA**, **IBM** and others will continue to partner with security technology companies or integrate authentication, authorization, administration and audit functionality into their servers. At some point, these servers may be self-contained secure extranets in and of themselves.

Findings & Recommendations

The creation of policies is only the start of the battle. Planning the implementation and deploying the rules and technologies can be a long and tedious effort. The degree to which an organization coordinates these tasks among senior executives, business managers, IT staff and security managers will dictate the success and ease of the project. Treat the rollout of an extranet security architecture the way you would treat any important project: with sufficiently empowered and financed project managers, with approval from all business managers who are impacted and with realistic deadlines.

That coordination and empowerment will happen along the way, as IT staff and business managers work together to develop and respond to the questionnaire. When IT staff collects the questionnaire responses, they can extrapolate the appropriate security technologies, as discussed. Then, after calculating the costs of purchasing deploying and maintaining those technologies, the business managers have an opportunity to revisit their requirements in light of the expense. In this way, true understanding and collaboration grows between all parties. Most of the suggested questions in the questionnaire are directed to the business manager or data owner. However, security managers, risk managers and auditors should increase or decrease the overall scores relative to proper risk management and cost effectiveness (see Planning Assumption, Establishing a Framework for Risk Management, Jon Erickson and Chip Gliedman).

Authentication: Your organization will likely maintain several authentication types concurrently. Seek the processes or technologies that permit you to enroll, suspend or delete users regardless of the authentication type used by a particular user. Take care to match the quality of the authentication type with the risk involved in the transactions.

Authorization: Extranets serve data to a wide variety of business partners — nonemployees. For that reason, authorization rules must be flexible and even somewhat “open.” You cannot restrict your business partners solely to applications and data resident in the DMZ. You must make connections to the trusted, internal LAN. When doing so, put primary security measures in place to secure the data. Securing access to the network or to application servers is secondary to protecting the data itself.

Administration: The goal is not to centralize administration, but to coordinate it. In a large, distributed organization, there will be many user populations that will require specialized administrators who understand the special needs of that group. Similarly, all the target platforms in use around the company have system administrators who cannot be replaced. Therefore, by coordinating all user and system administrators, a company has a chance actually to manage it all. The key will be migrating to role-based administration, and implementing the policies, processes and technologies that enable it.

Audit: Outside security assessments have a place, but don’t forget the people side of the equation. Errors or mischief inside the network or issues around the potential for social engineering as a result of an ineffective awareness program must be considered — not only for your company, but for your extranet partners as well. In any scenario, incident response is assumed. Have in place a well-thought out press response plan to hacking and fraud — witness the recent **Microsoft** fiasco which grew more from Microsoft’s poor response to the press than actual failures of their security architecture.

Finally, secure extranet policies should be organic, growing out of effective risk assessment, the business culture and requirements, using language and ideas familiar to employees. Develop the policy with a grass-roots movement. Get senior and mid-level managers involved all around the organization. They will respond to the questionnaire and end up thinking clearly about the risks of their particular applications or business. That is why Giga cannot write all of the questions for you. However, if your organization absolutely needs outside help, contact Giga for further specific assistance, or consider a security policy vendor like **PentaSafe**. PentaSafe’s VigilEnt Policy Center offers companies an alternative to entirely homegrown policies. Built on the seminal work of Charles Cresson Wood, PentaSafe’s solution walks you through the construction, distribution and education related to security policies.

References

Related Giga Research

Planning Assumption, The Whys and Means of Online Authentication, Andrew Bartels

Planning Assumption, Recommendations for Secure E-Business, Steve Hunt

Planning Assumption, Authentication Is the First Step Toward Secure E-Business, Steve Hunt

Planning Assumption, Securing the Extranet Web Application, Steve Hunt

Planning Assumption, Securing the Extranet Web Application, Steve Hunt

Planning Assumption, Outsourcing Security Is a Reasonable Option in Certain Situations, Steve Hunt

Planning Assumption, Establishing a Framework for Risk Management, Jon Erickson and Chip Gliedman

IdeaByte, The Four A’s of Secure E-Business, Steve Hunt

IdeaByte, Extranet Partners — Good Fences Make Good Neighbors, Phil Rosch

IdeaByte, Good Password Policies, Steve Hunt

Relevant Links and Other Sources

Sources for more information on building and deploying security policies include the following:

Information Systems Security Association, www.issa.org

System Administration, Networking and Security (SANS) Institute, www.sans.org

Colorado Swimming, www.csi.org

SecurityFocus, www.securityfocus.com

Vendors mentioned in this Planning Assumption include the following:

Access360, www.access360.com

ActivCard, www.activcard.com

Aventail, www.aventail.com

Baltimore Technologies, www.baltimoretechnologies.com

BEA Systems, www.bea.com

BMC Software, www.bmc.com

ClickNet (Entercept Security Technologies), www.clicknet.com

Commerce One, www.commerceone.com

Computer Associates, www.ca.com

CONSUL Risk Management, www.consul.com

Counterpane Internet Security, www.counterpane.com

Datakey, www.datakey.com

e-Security, www.esecurityinc.com

Gilian Technologies, www.gilian.com

Hewlett-Packard, www.hp.com

IBM, www.ibm.com

Internet Security Systems (ISS), www.iss.net

Netegrity, www.netegrity.com

PentaSafe Security Technologies, www.pentasafe.com

Riptech, www.riptech.com

RSA Security, www.rsasecurity.com

Sanctum, www.sanctuminc.com

SAP, www.sap.com

Securant Technologies, www.securant.com

Silent Runner (Raytheon), www.silentrunner.com

Systor AG, www.systor.com

Telenisus, www.telenisus.com

Tivoli Systems, www.tivoli.com

VeriSign, www.verisign.com

WatchGuard, www.watchguard.com

Whale Communications, www.whalecommunications.com

Glossary

Administration — The process of managing a variety of users and user groups and their privileges on a variety of target applications and resources. Also, the process of managing administration and authorization.

Audit — Either an accumulated log of events or the process of managing those logs.

Authentication — Answering the question "Who are you?" The process of determining the relative identity of a user in a specific context. Passwords and user IDs are the most common online authentication type.

Authorization — Answering the question "What may you do?" The process of determining the limits of authorized access to a particular resource, such as a file, server or network.

DMZ — Demilitarized zone. A networking expression denoting a segregated, semitrusted network where semitrusted external users may be granted limited access.

Extranet — The system of external connections permitting business partners, distributors, suppliers and customers to access some LAN and DMZ resources.

LAN — Local area network, the private network of a company.

Nonrepudiation — The attribute of authentication that guarantees the authenticity of a signature.

PIN — Personal identification number, essentially just a four-digit numeric password.

Role-based administration — The administration of users based on their roles. A role is a profile of a user, taking into account all of that user's functions in an organization. For example, one user's role may be administrative assistant, allowing access to e-mail and the basic network, while another user may have the role of vice president, granting access to e-mail, the network, the mainframe, some discrete applications and a financial database.

Table 2: Authentication Infrastructures

Vendor	Product	Infrastructure	Authentication types supported
ActivCard	Tokens, smart cards	The most versatile infrastructure, supporting many smart cards, password policies, certificates	Passwords, certificates, tokens, smart cards
Vasco	Tokens	Manages its own tokens	Tokens
RSA Security	Tokens, certificates, smart cards	Manages its own tokens and cards, but open to other certificates	Passwords, tokens, certificates, smart cards
Securant	Privilege management software	Manages all password policies and certificates	Passwords, tokens, certificates
Netegrity	Privilege management software	Manages all password policies and certificates	Passwords, tokens, certificates
Datakey	Smart cards	Manages its own smart cards and passwords	Smart cards
Entrust	Privilege management software and digital	Full public key infrastructure (PKI), manages certificates and passwords	Passwords, certificates, smart cards

	certificates		
VeriSign	Certificates and management software	Full PKI, manages certificates only	Certificates
Baltimore Technologies	Certificates and management software	Full PKI, manages certificates only	Certificates
Secure Computing	Tokens	Manages its own tokens and passwords	Passwords, tokens

Source: Giga Information Group

Note on Table 2: Certificates refers to x.509 v3 digital certificates. This is a sampling of leading vendors and is not exhaustive. Biometrics vendors are usually quite proprietary. The vendors listed may be able to customize support of biometric devices.