

## FIVE MINUTE CEO/CIO BRIEFING ON WEB SECURITY

### SEVEN QUESTIONS YOU SHOULD BE ABLE TO ANSWER

*This briefing is designed to quickly and succinctly focus senior managers to the issues surrounding web security from a risk, cost and benefits impact.*

Copyright, 2001. [Guy Huntington, HVL](#).

Over the next few years, you'll be increasingly asked to approve significant expenditures relating to "web", "extranet", "internet", "access control", "intranet" or "application" security. These costs will be above and beyond what you've already spent on network security and Y2K.

Some of the requests will stem from your marketing initiatives providing goods and services in new ways by allowing your customers into your systems via web interfaces and the Internet. There are risks associated with this that need to be addressed.

Others will come from productivity and profitability initiatives you have underway by integrating your systems more closely with those of your business partners. These too carry increased risk as you effectively open up more of your internal systems to people not on your payroll.

Finally, others requests for expenditures will come from similar internal initiatives leveraging your intranet. Words such as "self-serve", "entitlement", "zero day start" and "single sign on" will appear in the proposals. This is a result of your managers seeking to achieve efficiencies, lower costs and improve quality by integrating internal systems, pushing decision making further down the ladder and automatically enabling users to do what they need to do without costly hoops and time consuming approvals to jump through.

Web security has many pitfalls; some that carry with it high risk and costs if you're not aware. There are seven questions you need to answer knowledgably to deal with this.

#### **QUESTION 1. IS THE SOLUTION A PROCESS OR A PRODUCT?**

Security is a process, only as good as it's weakest link. Especially for high-risk applications, solutions must involve mapping out the entire business process or processes in question from beginning to end. They can be complicated, often crossing over multiple departments, their systems and people. That means there's likely to be a lot of politics involved.

All too often, this will be boiled down into if you just had "vendor A's" product your problems would be solved. While it makes for a simple business case presentation, unfortunately nefarious or malicious people will go after the weakest link in the entire process be it the product, person or procedure. This renders your enterprise vulnerable and vaporizes the benefits the business case touted to solve. Simply put, the devil is in the details of the end-to-end processes.

### **QUESTION 2. IS THERE A RISK ASSESSMENT?**

In the general rush to address newfound security fears, the tendency is to provide a solution to perceived problems without identifying the true risk(s). Providing and managing access to some of your applications and systems may carry with it catastrophic results if broken into, while others may have risks that don't justify the expenditure to solve. You need a priority list of risks identifying which applications, processes, etc, need to be tackled first and the benefits associated with doing so.

### **QUESTION 3. WHAT'S THE IDENTITY MANAGEMENT PLAN?**

This is something that may not even make the radar screen of the proposal or presentation being given to you. The process of creating, managing, terminating and archiving the identity of your customer, business partner, employee or temporary contractor is the first stage of establishing trust. In the old days this was done by physically meeting someone. Today, you may never even see or meet the identity in question.

In larger companies, you can have more than 150 different identity repositories, each storing much of the same information over and over, differently. Thus Joe Smith may have separate identities for each system he interacts with, many often manually created and storing his identity information in ways other systems can't recognize.

Ask where something called "Lightweight Directory Access Protocol" (LDAP) directories fits into the solution? LDAP directories can provide a uniform way of taking the identity's basic information generated by a database and sharing this between applications internally or externally.

Other questions requiring answers are how much does it cost the enterprise to create and terminate identities? How long does it take to do so? How easy it is to interchange the identities with your own and your business partners' systems? What are the risks associated with not doing so?

For example, if you terminate Joe Smith, how long does it take until Joe is no longer entitled to all your applications, assets and buildings? What's the cost of not doing so? Is Joe still able to log onto your systems and use the cell phone, pager, credit card and laptop you gave him even though he was terminated a day, week or month ago?

### **QUESTION 4. WHAT'S THE AUTHENTICATION PLAN?**

The second stage of establishing trust is authentication. How do you know that the identity purporting to be John Smith really is him?

Words that may come at you will include "SSO" (Single Sign On), "PKI" (Public Key Infrastructure), digital certificates, smart cards, biometrics and tokens. Along with username and password, these are all ways of establishing the authenticity of the identity.

Beware of the overly simplified solution such as "Single Sign On". While you and your users may be frustrated by too many passwords and usernames to remember, going to the other extreme of using just one authentication mechanism for everything may not meet all your risk requirements.

Ask your managers if you can mix and match the authentication mechanism to the risk? For example, can you start with a single username and password and then use other forms of authentication such as digital certificates, biometrics, smart cards and tokens as the risk increases? Will the solution do this easily or require a lot of expensive rework and time?

Query your managers if the solution being presented will be compatible with “SAML” (Security Assertion Markup Language)? This is an emerging global standard to facilitate the exchange of authentication and authorization information between enterprises and systems.

### **QUESTION 5. WHAT’S THE AUTHORIZATION PLAN?**

This answers the question “Who gets access to what?” and is the next stage in the trust process. Whatever solution you’re being presented with, it needs to be very flexible to deal with many different situations as well as easy to understand and implement.

For example, after a successful authentication from your central web security system, you may want to pass the authorization ability to an application like SAP, PeopleSoft etc. and let them do their own authorization. In other situations, you may want to replace older authorization software and use a centralized solution in its place.

Many vendor systems look great on a brochure for authorization but are extremely complex, expensive and time consuming to implement and maintain. The method used to create the authorization policies and/or the rigidity of these systems may make it hard for say someone like the Help Desk in your organization to understand why you can’t get access to an application when you call in to complain. Furthermore, your IT department may have to bring in expensive consultants to customize and maintain your authorization solution.

As in authentication, ask your managers if the authorization component of your solution will support SAML? Increasingly down the road, you’re going to want to exchange portions of your authorization rules with other enterprises, such as your business partners, to cut down time and costs in handling authorization.

### **QUESTION 6. WHAT’S THE AUDITING PLAN?**

Part of the trust process is being able to ensure what purported to have happened actually occurred. Auditing is a critical component in achieving this. It can get quite complicated because many systems and standards are used in a business process.

For example in monitoring a service level agreement, you may have to reconcile audit files from your network, firewalls and the web security software. Has the solution you’re being presented with considered this? What standards are the files to? How hard is it to get at the data within the audit files and combine it with other audit files? Do you have the flexibility you need to heavily audit processes where there is higher risk and lightly audit others where the risk is low?

### QUESTION 7. HOW EASY IS IT TO IMPLEMENT, SCALE AND MAINTAIN THE SOLUTION?

Many companies have bought vendor web security solutions only to find that implementing, scaling and maintaining the product solution is expensive, complicated and time consuming. This is especially so with solutions using databases instead of LDAP directories and/or vendor products with unique coding.

How many independent checks have been made with other customers using the same solution? To what degree were the checks made? Can your own staff maintain the solution without a fleet of expensive consultants or long time frames? If you don't watch out you may be hit with a significant bill later to make the solution work, increase its coverage or even be forced to ditch it and start over. Caveat emptor.

### USEFUL REFERENCES

[Reducing Total Cost of Ownership in Web Security- Six Points to Saving Money \(pdf\)](#) or [\(html\)](#)

The second in a series of briefings on web security by Guy Huntington, HVL. This briefing is designed to quickly educate senior managers where to look for cost savings in web security deployments.

[Web Security PowerPoint Presentations \(www.hvl.net/ebusiness.htm\)](http://www.hvl.net/ebusiness.htm):

Put together by Guy Huntington, [HVL](#) and Derek Small, [Nulli Secundus](#) from their web security, directory and ERP experiences, these presentations cover general and specific issues in web security, identity management, single sign on, LDAP directories, PeopleSoft LDAP integrations and PeopleSoft Oblix integrations.

[“Secrets and Lies: Digital Security in a Networked World”](#):

Bruce Schneier, CTO of CounterPane and a noted cryptography expert wrote an excellent book covering the issues of digital security. It's a must read for IT managers.

[“SAML” \(Security Assertion Markup Language\)](#):

This is the emerging standard for authentication and authorization. It's being put together by OASIS, the Organization for the Advancement of Structured Information Standards. OASIS is a non-profit, international consortium that creates interoperable industry specifications based on public standards such as XML and SGML, as well as others that are related to structured information processing.

### ABOUT THE AUTHOR

Guy Huntington, President of [HVL](#), specializes in leading enterprise reengineering projects including B2B's, B2C's and intranet integrating web security and LDAP directory infrastructure into the many disparate systems within each enterprise including data warehouses, ERP's, etc. Guy has lead many projects over the years, authored numerous papers, online presentations, an electronic book and given many speeches on the use of the web in business. Guy can be contacted at 604-921-6797, [guy@hvl.net](mailto:guy@hvl.net) or [www.hvl.net](http://www.hvl.net).