Becoming a Secure eBusiness: Avoiding Common Security Pitfalls

Introduction: Addressing Security for eBusiness

In this new era of eBusiness, the race is on for companies to roll out their high value business to business applications onto the Internet. However, due to the special security demands of the Internet, two eBusiness trends are emerging: Some companies are reluctant to deploy online their core legacy resources—such as mainframe systems and applications—that are needed for eBusiness. They are not confident about security and don't believe a good solution exists. Organizations have spent years developing internal security to protect their valuable information assets running on legacy systems and fear that they won't be able to reproduce that proven security in the eBusiness environment.

Other companies are rushing into eBusiness with faulty security implementations. A major contributing factor to flawed security is the relatively small number of experienced security experts knowledgeable about Internet security issues and technologies. Additional contributing factors are lack of awareness of the risks involved and the gap between legacy technology and Internet security technology. The result is an unsound, hole-patching approach that fails to address the enterprise's need for "360-degree" eBusiness security.

This paper identifies common eBusiness security pitfalls and explains the implications of each. It also presents a practical approach to address these pitfalls and to implement a comprehensive solution for eBusiness security all the way from the browser to the core business resources and applications at the heart of eBusiness. Such a solution would take advantage of PKI technology and leverage the security already built into the organization's mainframe systems.

Such a solution is the first step towards ubiqitous eBusiness security for the future. eBusiness systems must be protected by an integrated security platform intelligently designed to leverage the existing infrastructure and security intelligence of the corporation. This platform must extend across heterogeneous environments both inside and outside the organization.

The Mainframes Behind eBusiness

eBusiness is indeed emerging as the next great business opportunity. Organizations are staking their claims in a market that will be measured not in billions but trillions of dollars, according to leading industry analysts. Virtually all major eBusiness initiatives have one critical aspect in common--accessing and utilizing the organization's core back-end resources, typically mainframe systems, as a central part of the operating plan. For example:

- Brokerage firms are moving high net worth portfolio management services to the web.
- Banks are engaging in both consumer and corporate banking over the Internet.
- Manufacturers, distributors and retailers are turning to the Internet to streamline their supply chains, reduce inventory and cut costs.
- Health organizations are using the Internet to facilitate the delivery of healthcare to patients and to expedite cumbersome third-party billing and payment.
- Insurance firms are giving agents access to critical internal rating data over the web.
- Businesses of all types are using the Internet to process orders, service customers, and collaborate with a variety of partners.

When implementing eBusiness initiatives, companies must pay close attention not only to where their business data is going—to the Web and then to a global population of client browsers; but also to where their data lives—on the mainframe. And, they must keep this architectural picture in mind as they begin to extend their business to cross-enterprise partners who also have mainframes. According to Jim Hurly, Managing Director for Information Security at the Aberdeen Group, "The mainframe platform remains the center of computing's gravity and should benefit from e-commerce. On average, 75% of mission-critical data is still on mainframes." Even with e-commerce applications, he continues, the mainframe continues to play a central role, providing the critical enterprise data and applications behind the web systems.

These are the systems that process transactions, handle critical customer and corporate data, and manage logistics and the supply chain. Long protected by powerful mainframe security applications such as RACF, web-based eBusiness now exposes these systems to new Internet security threats.

Security for the organization's critical mainframe systems was never designed with the Internet in mind. Rather, the security was designed for a closed, well-defined, and tightly controlled environment. Key characteristics of such environments include a known and relatively trusted user population, a well-defined set of applications, and firm connectivity boundaries.

With eBusiness and the Internet, however, security considerations for the mainframe shift dramatically. The walls of the data center have been breached. Portions of the network are no longer under the control of the organization, and there are an undeterminable number of physical and logical access points. The relatively trusted user base is now extended to include less trusted external partners and customers as well as the completely unknown public at large. The challenge: how to tap web opportunities without putting valuable data and critical mainframe systems at risk.

Security Implications of Disparate eBusiness Agendas

Compounding the security challenge are the disparate array of perspectives involved in the eBusiness process. As a whole, organizations understand the opportunities presented by the Internet, appreciate the imperative to deploy eBusiness applications as quickly as possible and recognize the security concerns over the valuable mainframe data being exposed to the web. However, while everybody recognizes the need for security, a variety of agendas can come into play even among people working in the same organization, such as:

- "Get the eBusiness initiative up and running on the Internet as quickly as possible. Security is a concern but don't bog down the project with added security measures."
- "Get the web front end of the eBusiness project ready; secure the web server and application server; remain uninvolved in back end security issues."
- "Balance the logistics of running both the web site and conventional systems. Keep the amount of extra work, including security, to a minimum."
- "Don't move too quickly and thereby create unjustified security risks. Work through every security consideration carefully and deliberately even at the risk of delaying the project or increasing system administration workloads."
- "Guard the valuable corporate resources in mainframe data and applications. Don't jeopardize that asset by opening it to the web without ensuring that it will receive the same level of protection it currently experiences."

This mixed bag of agendas can lead to a situation where the desire for quick eBusiness rollout combines with lack of awareness of security pitfalls to result in exposure to avoidable eBusiness risks.

The first step in correcting the situation is to become more aware of the most common eBusiness security pitfalls. Armed with this awareness, organizations can avert risk and propel eBusiness securely forward.

Common eBusiness Security Pitfalls

Security failures typically come about not because of some obscure flaw or exotic bug, but rather because the organization tripped over one of the following five common pitfalls. These are:

1. Trusting the web server, a notoriously vulnerable device
2. Disconnected logins; i.e., lack of end-to-end user authentication
3. Implementing SSL from the browser to the web server only, not end-to-end
4. Using client-side digital certificates for security from the browser to the web server only, not end-to-end
5. Lack of expertise in security

Pitfall #1. Trusting the Web Server

The web server is at the heart of Internet connectivity and, in it's proper role, the web server serves several purposes. It formats information in a standardized HTML format that is universally readable by all browsers. It is a facilitator of connections between the outside world (i.e., the browser) and internal systems such as legacy databases and mainframes. It is a purveyor of static and dynamic information.

However, it is crucial to remember that the web server should not be relied upon to fulfill any role related to security. The web server is designed to be accessible to anyone on the Internet, and it is the most available and most vulnerable point of contact in an Internet connection. Yet, many organizations currently face the following web server-related security shortcomings trusting the Web Server.

1. **ID/password login credentials hard-coded in web applications or stored in a lookup table on the web server.** Often, web applications—particularly client/server applications that have been migrated to the web—have within them a hard-coded ID/password for the application and/or for the users to log in to the back end. Or, the web server stores lookup tables containing the login credentials of every user, which are used by the web application to log users in to the back end. This is done simply as a shortcut to make things easier for the administrators and users.

   Whether the credentials are stored on the web server in a clear or encrypted fashion, this scenario presents an easily exploited vulnerability. It is relatively easy for a hacker to access a lookup table stored on a web server, or to get a copy of the application off the web server and to extract the ID/password.

2. **Trusting the web server for processing transactions and/or storing data.** The web server is the most vulnerable point of attack. It is therefore not the place to process transactions or store sensitive data, even temporarily.

3. **Exposing back-end systems directly to the Internet by natively web-enabling them; i.e., placing the web server directly on the back end.** This exposes the back end to Internet-based/Internet-style attacks. (Such attacks used to be reserved for the web server alone.)

In addition, this removes a level of protection behind the web server. Traditionally, the web server is on a physically separate machine from the back end. A filtering firewall or router guards access to the web server from outside, allowing individuals access to the web server. Then, a second filtering firewall or router behind the web server provides a second barrier, allowing only the web server to access the back end. If the web server is physically placed on the back end, there is no second filtering point. Whoever accesses the web server may gain access to the back end.

4. **"Golden" logins (trusted logins) from the web server to the back end.** The Internet environment currently facilitates secure user login from the browser to the web server. The user's unique login credential, which can be an ID/password or a certificate, logs them in such a way that the web server can specifically authenticate them. This is a good thing.

   The problem is that the same user most likely does not have an individualized, unique login from the web server to the back end. Rather, the web server itself completes the connection to the back end using its own Web server login. The web server login has "golden" privileges to access and manipulate any information at the back end. Such a login is known as a golden login, also called a trusted login.

   A hacker who compromises the web server can find the golden login credential, log in to the back end, and take advantage of the golden login privileges to wreak havoc on the system.

   And, such a system depends on the web application's security features to maintain a granular audit log. Since only the web server, and never the user, logs in to the back end, there is no back-end mechanism for maintaining a granular audit trail of user activities. While the web application may be programmed to maintain an audit log, there are dangers inherent in depending on web application developers—rather than security specialists—for granular auditability, an essential security requirement.

Pitfall #2. Disconnected Login: Lack of End-to-End User Authentication

A disconnected login occurs when the browser logs in to the web server or to a middle-tier server and then the web server/middle-tier server logs in to the back end. Example of this are password lists on the web server, web application authentication servers and web-enabled single-sign-on servers. This presents a lack of trusted, end-to-end user authentication. The user never actually logs in to the back end. When the client logs in to the web server, and the web server completes the connection by logging in to the back end, the web server essentially becomes the user's proxy. There is no way to know if the legitimate user is performing the transactions or by someone who has compromised the web server. In addition, if the browser's login credentials are stored even temporarily on the web server, they are vulnerable to being compromised.

Note: In the eBusiness environment, web application authentication servers provide an important level of access control and personalization to the user experience. For example, they are used to return personalized pages to users that access an eCommerce site, or to authorize access to member pages for such applications as online consumer banking. However, end-to-end user authentication from the browser to the back-end system—an essential security element for high value business-to-business transactions—is not provided by web application/ middle-tier authentication servers.

Pitfall #3. SSL from the Browser to the Web Server Only: Data Communications Flowing in the Clear Within the Corporate Network

SSL, Secure Sockets Layer, is the encryption-based security protocol implemented in every web browser. SSL establishes an encrypted channel for secure data transfer over the web. While organizations are usually careful to establish such an encrypted channel for information that travels outside the corporate network over the web, it is surprisingly common for passwords and data travelling across the corporate intranet behind the firewall to travel in the clear, unencrypted.

Security planners must recognize that internal networks are no longer as private as they once were. Today many non-employees, consultants, contractors, partners, and associates of all sorts will have access to the corporate network behind the firewall. It is not difficult for any of these users to run one of the widely available, easy-to-use sniffers to intercept traffic on the private corporate network and capture unencrypted information, particularly passwords.

In addition to the straightforward security problems presented by this situation, there are also legal implications. For example, clear data flowing within an organization can violate privacy-oriented regulatory requirements. And, information illicitly gained can cause serious damages and breaches of confidentiality for which the organization may be liable. The data might also be used competitively or in other ways harmful to the company, which may experience losses without ever actually realizing how the losses occurred.

Pitfall #4. Client-Side Digital Certificates from the Browser to the Web Server Only

The digital certificate-based security of PKI is rapidly becoming accepted as a standard for eBusiness security. Corporations are enthusiastically investing in PKI and rolling out client-side digital certificates (and rightfully so), but often with the incorrect assumption that it will provide a comprehensive eBusiness security solution.

It is essential to understand that the functionality of client-side PKI is not integrated with back-end corporate resources, such as mainframes. In fact, PKI security currently extends only from the browser to the web server, leaving the information to travel unprotected by PKI from the web server to the back-end host. To remedy this dangerous situation, PKI requires enablers to fully integrate it with back-end resources and applications. Until PKI is extended to the back end, most of the weaknesses discussed in this paper remain uncorrected, yet the company may have a false sense of security based on its mistaken assumption about PKI and client-side digital certificates.

Pitfall #5. Security Implemented by Non-Security Experts

In fact, eBusiness security is complex and difficult to implement well, which is why the above organizations so readily get caught in the above pitfalls. Security matters belong in the hands of experienced security and risk management specialists. This is illustrated in the following true, instructive anecdote:

Two developers needed a way to allow a web application to log in to a back end database. The easiest way was to hard code the ID/password directly into the application. Since the user was never supposed to see the code but only the resulting HTML, the developers thought it was safe to place the login credential directly into the code. However, a bug in the web server allowed the users to view the code by just typing in a few question marks at the end of the

URL, giving them a text display of the login ID and password to the back end system. While the bug in the web server was partially responsible for this problem, an experienced security specialist would have anticipated the potential danger in placing the ID/password in the code under any circumstances.

A Practical Approach to eBusiness Security

A practical approach to eBusiness security starts by reconciling the disparate business and security agendas within an organization. Managers must agree on the balance between speed, cost, effort, and security. This will include consideration of the size of the specific eBusiness opportunity and the specific assets at risk, as well as an assessment of potential threats based on whether the initiative is intended for an intranet, extranet, or the public Internet.

Managers must then review their eBusiness efforts in light of the security pitfalls described above. Where they have encountered a security pitfall, they must correct the problem. If they can't tell, they need to bring in someone with specific experience and expertise in Internet security.

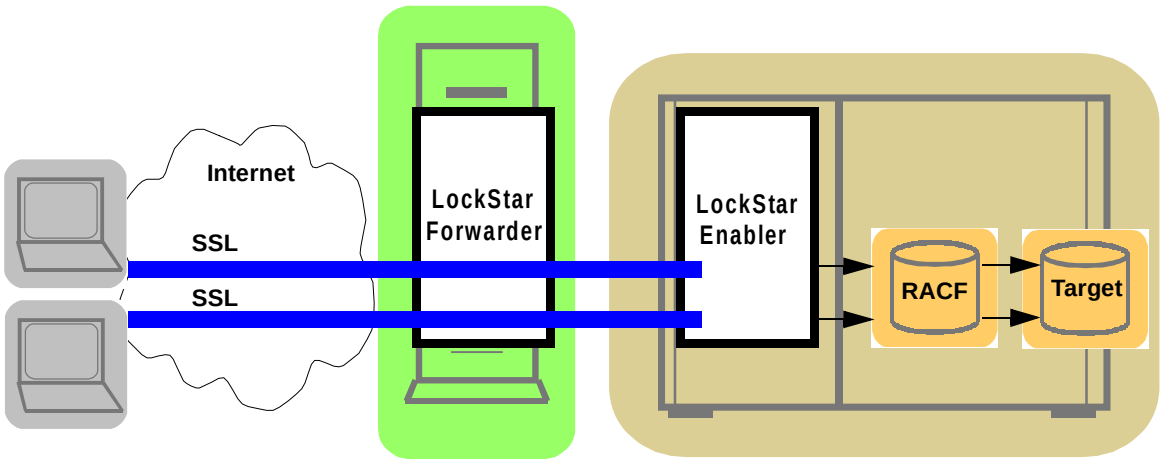
Finally, organizations need to extend whatever eBusiness security approach they choose all the way to their mainframes and other back-end systems. To do this, organizations need to leverage the intelligence built into their existing back-end security systems, through such processes as mapping digital certificates to RACF, a proven mainframe security application.

Lockstar Recommended eBusiness Security Steps

Lockstar, which is experienced with both mainframe and Internet security, recommends a five-phase strategy for eBusiness security to help you steer clear of the pitfalls described above.

1. **Take increased security precautions at the web server.** Fully implement all security options available through the web server and check to ensure that you have avoided the pitfalls described above.
2. **Establish end-to-end user authentication.** Set up an end-to-end user authentication mechanism that reaches from the web browser to the mainframe or other back end resource. This avoids the problems associated with golden logins, disconnected authentication, and over-reliance on second-tier security.
3. **Establish an end-to-end encrypted data channel.** Ensure privacy by protecting data in transport. Use encryption from browser to host, to ensure that critical or confidential data is not exposed as it travels over internal or external networks.
4. **Implement PKI security end-to-end.** Seek out proven PKI enablers to deploy PKI all the way from the browser to the back end, integrating it with existing security systems, such as RACF on a mainframe.
5. **Turn to security specialists, such as LockStar.** By adopting solutions designed by professionals with proven security expertise, your organization can be sure that all known risks taken into consideration and that security has been implemented in the most effective manner possible. The LockStar solution is illustrated in Figure 1.

Figure 1 LockStar architecture



Tier 1: Clients with standard browsers login with certificates or ID/passwords

Tier 2: Each browser has a secure SSL connection to the back end through the LockStar Forwarder on the web server

Tier 3: LockStar Enabler on the back end validates and maps individual logins to native access controls

Conclusion: Start Securing eBusiness Now

Obviously, security as an afterthought will not work for eBusiness. The time to start planning eBusiness security is as soon as you begin developing your eBusiness strategy. The most effective security is designed into the eBusiness solution from the outset.

Begin your eBusiness security planning by familiarizing yourself with likely security threats and common security pitfalls. In general, you will want to review and, where appropriate, tighten existing security policies and procedures. Educate both users and the technical staff to the eBusiness security threat and enforce practices to mitigate that threat.

Look beyond the common web security solutions, which typically stop at the web server. Instead, implement an end-to-end solution extending beyond the web server to encompass your valuable back-end information assets. A partner like Lockstar will bring eBusiness and mainframe security experience as well as technical solutions designed to leverage the existing infrastructure and security intelligence of the corporation to implement a secure, end-to-end eBusiness environment.

Finally, consider that the security solutions put in place today will become your foundation for addressing the growing eBusiness security needs of the future. Companies such as LockStar are developing platforms to extend integrated security across the heterogeneous eBusiness environments of the future, both inside and outside the organization.