

Realtime  
publishers

"Leading the Conversation"

# The Essentials Series

## Messaging and Web Security Volume III

*by Dan Sullivan*

---

Article 1: TJX Data Breach Revisited .....	1
Highlights of TJX Data Breach and Subsequent Publicity .....	1
Lessons Learned.....	2
Article 2: DNS Poisoning: New Techniques .....	3
Traditional DNS Corruption Techniques.....	3
New Type of DNS Attack.....	4
Article 3: End User Security: The Weakest Link?.....	6
Lack of Understanding of Security Risks .....	6
Lack of Compliance with Security Policies.....	7
Insufficient Security Tools for End User Activities .....	8
Article 4: 5 Steps to Getting Started with Data Loss Prevention.....	9
Step 1: Develop a Data Classification Scheme.....	10
Step 2: Identify Threats to Various Data Classes .....	11
Step 3: Define Tolerance for Various Risks .....	11
Step 4: Conduct a Gap Analysis Between Existing Risks and Tolerance for Those Risks	12
Step 5: Close the Gaps between Unacceptable Risks and Current Means for Mitigating Those Risks.....	12
Article 5: Third-Party Database Tools.....	13
Auditing and Monitoring .....	14
Vulnerability Scanning .....	15
Intrusion Prevention.....	15
Summary .....	15
Article 6: Where to Spend Your Security Budget Part 1: Identifying Priorities .....	16
Step 1: Gather Risk Assessment Data.....	17
Step 2: Identify and Classify Information Assets .....	18
Step 3: Determine Business Impact .....	19

---

## Article 1: TJX Data Breach Revisited

If one had to pick a top security story of 2007, it would have to be the TJX data breach. That incident walks away with top honors for a couple of reasons. First, it was the largest data breach in history. Early estimates in March 2007 placed the number of compromised customer records at [45.6 million](#), but that number grew to 94 million records, as reported by [CNET](#) in January 2008. The second reason this breach is so notable is that it seemed to stay in the news because of slowly revealed bits of additional, sometimes contradictory, information.

At this point, perhaps the best that can come from this incident is that it becomes a case study in how to reduce the adverse impact of a data breach. To that end, this article will first recap some of the major points of the TJX data breach story and then summarize lessons learned.

### Highlights of TJX Data Breach and Subsequent Publicity

When we look at the TJX data breach case study, we can see two failures: failure to protect customer information and failure to properly respond to the breach. Here are some highlights of the protracted story: In mid-January 2007, TJX announces a data breach in a press release that includes a statement that the company had worked with security consultants to put a security plan in place after the fact. The press release included the following [statement](#):

With the help of leading computer security experts, TJX has significantly strengthened the security of its computer systems. While no computer security can completely guarantee the safety of data, these experts have confirmed that the containment plan adopted by TJX is appropriate to prevent future intrusions and to protect the safety of card, debit card and other customer transactions in its stores.

This, of course, raises questions as to why such a plan was not in place before the incident.

Several days after the initial announcement, the Massachusetts Bankers Association was notifying members that TJX may have kept unnecessary data about customers in violation of credit card industry [rules](#).

Within a few weeks of the announcement from TJX, banks and retailers began reporting incidents of fraud related to the TJX breach. These include companies in the U.S. and Canada. In addition, 60 banks in Massachusetts alone began issuing new credit cards to potential [victims](#). In March 2007, the company increased the estimated number of victims and added that attackers may have compromised the company's encryption software. Also by this time, shareholder and victim lawsuits had begun to be [filed](#). By August, TJX had incurred \$118 million in charges related to the incident according to their [quarterly report](#).

By the fall of 2007, TJX was trying to put the breach behind them and move on with a class action settlement, but a federal judge had found some of the settlement [wanting](#). Attorneys General in 10 states also opposed portions of the proposed [settlement](#). Even in early 2008, we probably have not heard the last of this incident; we will probably hear of lawsuits from consumers and banks well into this year.

---

## Lessons Learned

We can learn a number of principles from the TJX incident:

- Security matters—IT professionals know this and some executives and managers know it as well. If this understanding breaks down somewhere along the line, the consequences can be severe.
- Security policies and procedures must be in place now, not just after a breach. Closing the proverbial barn door at TJX did not halt the subsequent raft of bad press, damage to brand, and lawsuits.
- It is sometimes difficult to estimate the full extent of a breach. Post-breach forensic investigations can be slowed and hampered by poor monitoring and audit trails. This point argues for well-designed plans to prepare for breaches before they occur.
- Data breaches can reveal non-compliance and other operational problems. In the TJX case, the retailer may have been keeping more data on consumers than allowed under industry rules. This could lead to penalties in addition to the direct consequences of a breach.
- Data breaches are expensive. TJX incurred \$118 million in initial expenses and court cases are still proceeding. It is difficult to estimate the damage to brand reputation and lost revenues due to the publicity surrounding this incident. It is difficult to imagine how implementing proper safeguards could have cost more.

The data breach at TJX was unfortunate and its ripple effects spread to banks and customers. By its own admission, the company had improved its network and system security after the breach, which can lead one to ask why those improvements were not put in place prior to the breach. The answer could relate to expected cost/benefit tradeoffs or to lack of awareness about the full scope of the threat. Regardless of the reason, companies that maintain large databases of financial transaction and customer data will no longer be able to claim ignorance of the potential risks.

---

## Article 2: DNS Poisoning: New Techniques

Trust was implicit in many of the Internet protocols when they were first developed. The basic email protocol, Simple Mail Transfer Protocol (SMTP), for example, has no mechanism to ensure that the sender listed in the header is actually the person or agent who sent the message. Spammers can exploit this implicit trust in the protocol to spoof the sender's identity. Trust was also implicit in the Domain Name Service (DNS). The basic protocol does not require verification of a DNS server, and even if it did, weaknesses on the client side yield opportunity for malicious attacks. This article will examine some of the well-known and emerging techniques for compromising DNS and offer suggestions on reducing the risk of DNS poisoning.

### Traditional DNS Corruption Techniques

DNS works by taking requests from clients to map domain names into IP addresses. For example, the domain realtimepublishers.com maps to the IP address 70.86.192.100. The domain name is easy for humans to read and use while the numeric IP address is more efficient for routing, so we routinely map between the two. A problem arises when we can no longer trust the mapping from domain names to IP addresses. This can happen in several ways.

First, the DNS server used by a client may have been compromised and malicious data is placed in the DNS database. For example, an attacker may change the IP address associated with a bank to point to a server controlled by the attacker. This could occur if the DNS server is running a version of DNS software with vulnerabilities that are exploited by the attacker.

A second method of attack is to change locally cached domain name mappings. Clients may maintain a host file with domain names and IP addresses of local network or frequently used domains. For example, a local network may have several servers that are not accessible from the Internet and are not registered in public DNS servers. The network administrator may create a host file with mappings for each local server and distribute those to all clients. When the user makes a request of a server (for example, browse a directory on a local server), a lookup is done on the host file of the local client; if the server name is found, the corresponding IP address is returned. This process can also be used to save the time required to make a DNS query. Although the host file clearly has advantages, it can be exploited in an attack.

---

Malware writers have sometimes corrupted host files to prevent detection of their malicious code. When a Trojan or virus infects a device, it may edit the host file to add entries with bogus IP addresses for the update sites of major antivirus vendors. In this way, when the antivirus software on the device tries to connect to the vendor's site to download updates and new signatures, it will be redirected to an attacker-controlled site instead, leaving the client unable to detect the recently installed malware.

Keeping DNS server software up to date is one way to reduce the chances of poisoning the DNS cache. This is an important responsibility of ISPs and others who run DNS servers to reduce the chances of successful DNS attacks. End users should also keep their operating systems (OSs) up to date, install and keep up to date antivirus software, and just as importantly, not use privileged accounts for everyday tasks. A non-privileged user will not have the ability to edit the host file and therefore could block unauthorized changes to that file unless the attacker has some way of elevating privileges.

## New Type of DNS Attack

A new type of DNS attack has been discovered by researchers at Google and Georgia Tech. The scheme exploits DNS servers that have been configured to respond to requests from any client. (These are known as open recursive DNS servers.) The problem with such a configuration is that, if these servers are compromised, they can be used to redirect users to malicious Web sites. Here are the steps in the process.

1. The attacker sets up a malicious Web site. This may be for phishing or for distributing malware.
2. The attacker compromises an open recursive DNS server and plants false information. For example, the mapping from a bank's domain to IP address is changed so that the mapping directs clients to the malicious site.
3. The attacker, through a Trojan or other method, changes the DNS registry information for a client. For example, if a client normally uses their ISP DNS server, the registry setting is changed to direct DNS requests to the compromised DNS server set up in step 2.
4. A user, working with a compromised client, browses to a bank site (for example, [www.myexamplebank.com](http://www.myexamplebank.com)). The browser initiates a DNS request, which is sent to the compromised open recursive DNS server. The compromised server returns the IP address to the malicious site.
5. The user receives the content from the malicious site that presumably looks identical to the legitimate bank site.
6. The attacker harvests usernames, passwords, account numbers, or other identifying information.

---

This type of attack is successful because there is a breakdown in several stages of the DNS service:

- DNS servers have to accept requests from anyone. This allows a client device to be redirected without triggering any notice; the DNS server willingly provides an IP address.
- The DNS server data is updated in an unauthorized manner.
- The client device's registry is changed in an unauthorized way.

Typical anti-phishing techniques depend on checking URLs for signs of phishing, such as similar-looking URLs. Those techniques will not work with this type of attack because the anti-phishing program is analyzing a legitimate URL; the problem does not manifest itself until later in the process.

To minimize the risk of this type of attack, we can adopt a number of strategies:

- Properly patch and configure DNS servers to reduce the ability of attackers to compromise the DNS server.
- Do not configure a DNS server as an open recursive server.
- Keep antivirus software up to date to detect Trojans that may change client registry settings.
- Use OSs that are more difficult to compromise; Vista, for example, prompts users before executing programs to reduce the chance of a malicious program from running without users' knowledge.

These are short-term solutions to this threat; a more secure, less trusting model of domain name resolution is required to further reduce the emergence of similar threats to DNS.

---

## Article 3: End User Security: The Weakest Link?

Security applications are essential to protecting an organization's assets, but they are not all that is needed. A company can install and manage the best antivirus solutions, firewalls, intrusion prevention systems, and content filters while monitoring and auditing systems according to best practices. What is the weakest link in the proverbial security chain? It's none of these applications—it is the end user. Content filters can detect documents that should not be emailed from an organization, but they cannot prevent someone from printing a confidential document and removing it from the building. Antivirus systems on the network cannot protect a user working on a home computer riddled with malware. Data loss prevention tools will not stop a laptop with unencrypted data from being stolen. The problem in all these cases is not the technology but the end user.

The end user as the weakest link stems from three fundamental problems:

- Lack of understanding of security risks
- Lack of compliance with security policies
- Insufficient security tools for end user activities

To improve information security, sometimes we need to spend more time and resources with people and less with technology.

### Lack of Understanding of Security Risks

A lack of understanding of security risks stems from the complexity of the risks and insufficient training. IT professionals might get frustrated with user behaviors that clearly put assets at risk, such as using easily guessed passwords or copying sensitive information to unencrypted devices. No one expects an average user to understand how buffer overflows can be exploited or how signature-based virus detection works, but they should understand basic practices that reduce the chance of compromise.

Users in many companies can equally well argue that they could not possibly know that a trusted Web site could be used for drive-by malware downloads or that they should not disclose a password to a purported service desk technician who calls claiming to be fixing a network problem. These kinds of situations can spiral down into little more than finger pointing about who is to blame when a breach occurs. Rather than waiting for that, IT professionals can actively engage their colleagues to help maintain a secure environment.

---


IT departments should provide basic security awareness training. This should cover the need for security measures as well as some very basic security practices:

- The proper use of passwords and authentication devices
- Acceptable and unacceptable uses of computing and network resources
- Restrictions on transferring information from the network to outside devices, such as personal USB drives, cell phones, or home computers
- Tips on how to avoid social engineering attacks

This kind of training should be provided with some repetition. Although having a new employee view a security awareness video and sign off on understanding its content might be good enough for the legal department, it is not sufficient to actually achieve its goal. Employees can forget and circumstances can change, especially with the dynamic nature of computer security threats.

## Lack of Compliance with Security Policies

Security policies should be in place that define acceptable use of IT resources. At a minimum, policies should cover email use, authentication, network security, laptop and mobile device use, and information sharing outside the organization.

 For a list of commonly used policies and starter templates for policies, see the SANS Institute's Security Policy Project at <http://www.sans.org/resources/policies/>.

Simply defining policies and linking to them from an employee portal will not lead to compliance. First, such a practice may satisfy minimal legal requirement and legally shift some responsibility to employees, but it is not sufficient to ensure employees follow those policies. A study by the Ponemon Institute, reported in *ComputerWorld* (Source: Jaikumar Vijayan "Security Policies? Workers Ignore Them, Survey Says" *ComputerWorld*, Dec. 6, 2007), found significant lack of compliance, such as:

- More than 50% of respondents had copied confidential information to USB flash drives
- 46% of respondents admitted to sharing passwords with colleagues
- 33% of respondents admitted to emailing documents home in violation of policy
- 80% of IT professionals surveyed did not know whether turning off firewall settings violated a company policy

Part of the solution to such poor compliance rates is to improve the security awareness training as described earlier. Another part of the solution lies with the policies themselves.

---

When designing policies, it is important to keep in mind business as well as security requirements. The key is to balance the need for security with usability. There is no value in a policy that is so restrictive that a user cannot do her work. Also, the policy, and the procedures that follow from it, should be readily understood and implemented by users. Here are some principles to guide policy development:

- Policies should protect information and assets but also provide for the way employees work. For example, employees may need to transfer documents with USB drives; do not ban all USB drives but limit the type of content that may be copied (for example, word processing documents and spreadsheets may be copied, but database files may not). Also, use encrypted USB drives only.
- Policies should define what should be done as well as what cannot be done. For example, in addition to stating that work documents may not be copied to a non-company-provided PC, like a home computer, also state that laptops will be provided to employees that need access to work material outside of the office.
- Policies should direct IT to provide sufficient support and tools to accommodate users with varying levels of technical skill. If all documents on laptops should be encrypted, then provide full disk encryption such as Vista's BitLocker or McAfee Endpoint Encryption; do not expect users to create and manage encrypted files or folders manually.

The last principle begins to address the third factor at work in the problem of end user security: insufficient tools for end user activities.

## **Insufficient Security Tools for End User Activities**

The last problem is that even if users are aware of security threats and abide by policies, they may still do things that can compromise their systems or lead to data loss. They could, for example

- Visit a trusted site that has been compromised and now pushes drive-by download malware
- Open a legitimate-looking link in an email that leads to a phishing site
- Have a laptop containing confidential information stolen

In each case, there is no intentionally risky behavior, but the user still becomes the victim of an attack or a criminal's theft. For these times, automation is the best defense. Content filters that scan network traffic may be able to detect and block malware from compromised Web sites. Email filtering and spam detection software may be able to identify phishing links that look legitimate but use homographic attacks to dupe humans. Full disk encryption will not prevent loss of laptops but it will at least protect the information on them.

End users can become the weakest link in an information security plan; however, that need not be the case. Proper training, pragmatic policies, and effective countermeasures are the key to avoiding to strengthening the weakest link.

---

## Article 4: 5 Steps to Getting Started with Data Loss Prevention

Lost and leaked data from stolen laptops, compromised networks, and malware-infected client devices are timely topics in the IT press these days. Of course, this news is going to generate interest in data loss prevention techniques, but where does one begin? At first glance, someone might be tempted to rush out and buy software or hardware from a data loss prevention vendor, install it, and be done. Check that one off the list. Unfortunately, that kind of thinking puts the proverbial cart before the horse.

Planning is crucial to any security program, and data loss prevention is no different. Putting software, hardware, and procedures in place without understanding the specific details of an organization's requirements is like playing the lottery. Yes, you might hit it right on, but chances are not in your favor. A rational, methodical approach is needed to understand the nature of data loss risks and ways of mitigating those risks. One way to approach the problem of getting started with data loss prevention is to follow these five steps:

1. Develop a data classification scheme
2. Identify threats to various data classes identified in Step 1
3. Define tolerance for various risks
4. Conduct a gap analysis between existing risks and tolerance for those risks
5. Close the gaps between unacceptable risks and current means for mitigating those risks

An approach such as this provides organizations with information about their own needs and weaknesses. These should be the driver behind the choice for data loss protection methods rather than blanket application of a generic solution.

---

## Step 1: Develop a Data Classification Scheme

Data classification schemes are a means for distinguishing the value of different kinds of information and their value to an organization. Not all information is created equal; at one end of the spectrum, the distribution of intellectual property must be limited to preserve its value; at the other end of the spectrum, public sales information is ideally spread as far as possible.

A typical data classification scheme for commercial enterprises uses four categories:

- Public
- Sensitive
- Private
- Confidential

Public information can be shared outside the enterprise with no impact on the organization. This kind of information needs little protection from disclosure. (The integrity of the information must still be protected; for example, a public Web site should still have access controls to prevent an attacker from defacing a company's Web site.)

Sensitive information should not be publically available but if it were leaked would not cause serious damage to the organization. Project plans, common business contracts such as leases, delivery schedules, and such might provide small bits of information that competitors could piece together to formulate an understanding of operations and strategies, so this sensitive information warrants more protection against disclosure than public information. Although the loss of sensitive information may cause some harm, the loss of private or confidential information is much more likely to result in damage.

Private information is data about customers, employees, clients, and others that is held in trust by an organization. The disclosure of credit card data, Social Security numbers, and similar breaches are examples of private information loss. Damages may result from brand damage (for example, if a department store has a large public breach, shoppers may turn to competitors) or from fines and other penalties for violating privacy regulations.

Confidential information is restricted because its disclosure could adversely impact the business. Trade secret, contract negotiation, and strategic planning information are examples of confidential information that warrant more protection than sensitive or public information.

With a classification scheme such as this in place, all information managed by an enterprise should be categorized into one of the categories. This can be a time-consuming task and the boundaries may not always be simple; for example, a quarterly earnings report can be sensitive or confidential one day and then public information the next.

---

## Step 2: Identify Threats to Various Data Classes

The second step in the data loss prevention process is identifying the types of threats to sensitive, private, and confidential data and the likelihood of their occurrence. The types of data loss threats may apply to all kinds of data, including:

- Loss due to hardware theft, such as laptop theft
- Loss due to malware-infected client devices copying data to an outside device
- Loss due to hardware failure, fire, flood, or other natural disaster
- Loss due to employees copying information to unmanaged devices
- Loss due to a compromised network that allows attackers to monitor and steal data

Once the types of threats are identified, it is important to assess their likelihood. For example, the chances of a client device becoming infected with malware are relatively high unless antivirus measures are in place. The chance of laptop theft may be high for some users, such as sales staff or other mobile workers, but much less for others. Likelihood estimates should be made for each type of threat but also broken down according to user roles or organizational structures to provide a more fine grained assessment of risks.

## Step 3: Define Tolerance for Various Risks

The previous step produces a set of threats categorized by role and/or organization structure. The next step is to assign a risk tolerance category to each. This can be as simple as deciding some risks are acceptable and some are unacceptable; the unacceptable risks will then be transferred, by purchasing insurance, or mitigating measures will be put in place.

Unacceptable risks will probably include high-likelihood threats to confidential and private information. Insurance may be an option in some cases but mitigation strategies are more likely to be used. Insurance is more appropriate for disaster recovery types of risks. Acceptable risks may be those involving sensitive and public information on low or moderately low likelihood threats.

The goal of this step is to identify the top priority risks based on threats to different kinds of information and their likelihood. Once you have a reasonable ordered list of information assets and the threats to them, one can begin the gap analysis.

---

## **Step 4: Conduct a Gap Analysis Between Existing Risks and Tolerance for Those Risks**

Companies and organizations probably already have some security measures in place to protect information. Clients and servers may be running antivirus software, firewalls define network perimeters, and some end user security awareness training is in place. At this step, the goal is to align the risk tolerance profile with the current security measures in place and identify risks that are not properly addressed.

For example, one may determine that there is a moderately high risk of an employee copying confidential information to a USB flash drive and losing or giving that information to a competitor. Access controls may be in place to limit the number of employees that have access to that information and so it reduces the risk but not enough. In that case, additional measures, such as host-based content filters or blocks on USB drives may be needed.

The goal of this step is to produce a list of additional measures that are needed to align the security measures in place with the risk tolerance of the organization.

## **Step 5: Close the Gaps between Unacceptable Risks and Current Means for Mitigating Those Risks**

The final step in the process is putting measures in place to mitigate risks. This is the point where one can invest in network filters, full disk encryption, and other data loss prevention technologies and know that they are applying them in a rational manner. In any but the most ideal circumstances, there will be budget, staff, and time constraints that limit how much can be done. Again, this five-step procedure helps to identify the most likely threats to the most important information and so allows organizations to target those first.

---

## Article 5: Third-Party Database Tools

Relational database management systems (RDBMS) such as Oracle, IBM DB2, Microsoft SQL Server, and Sybase are relatively self-contained applications. Within core functionality and add-on modules, they contain authentication, authorization, auditing, reporting, encryption, and other mechanisms needed to secure enterprise data. Yet, even with this broad array of features, there is room for third-party tools to complement what is provided by database vendors.

One may wonder, why if so much is already built-in to an RDBMS, would there be a need for third-party tools. There are several reasons:

- **Separation of duties**—Database administrators have traditionally had full reign over database systems, although this is starting to change. Oracle, for example, now provides means to limit the scope of DBAs' abilities to manipulate the database. Even with these enhanced features, an organization might want a separate role, independent of RDBMS management, to be responsible for monitoring and auditing database activities. An administrator of a third-party tool can meet that need without necessarily having the same kinds of privileged access to a database as a DBA would have.
- **Improved performance**—Adding features to a database application can slow response time. For example, if additional monitoring procedures are triggered on a database insert, update, or delete, the cumulative effect can degrade the responsiveness of the application. A third-party tool that monitors database network traffic may be able to provide the same type of auditing but do so outside the database and thus relieve the RDBMS of the additional burden.
- **Need for specialized security measures**—Databases are designed to store and manage data; intrusion prevention systems (IPSs) are designed to detect anomalous patterns of activity indicative of an attack. These are not the same kinds of activities and there are sound reasons to take a “best of breed” approach to multi-layered defenses: use RDBMS for data management and IPS for intrusion prevention.
- **User identification**—A database user may have a network or server authentication but use a shared pool of database connections. How is one to track who is using which pooled resource when? Some third-party tools provide this capability.

---

These are just some of the reasons a separate tool may be required to meet the full range of functional and non-functional requirements for database applications. There are certainly cases in which an RDBMS or a third-party tool may be used to meet the same requirement and then it comes down to questions of quality, reliability, maintainability, scalability, time to deployment, and of course, cost. In broad terms, there are three areas in which third-party tools may have a role in enterprise databases:

- Auditing and monitoring
- Vulnerability scanning
- Intrusion prevention

Tools may fall into individual categories or provide features across these categories.

## Auditing and Monitoring

Auditing and monitoring is required by regulations such as the Sarbanes-Oxley Act (SOX), but implementing the required levels of auditing may be difficult or costly in legacy systems. For example, if one is required to record the date and time of a change and the identity of the person making the change and this function is not already built-in to a database application, the changes could be difficult.

Adding auditing within a database application could require changes to the database schema as well as to the applications that use the database. In the worst case scenario, every table in a database would have to be modified to add columns to record the timestamp of the change and the user identifier of the person making the change. This, of course, assumes you have access to the database schema and application code, which is not always the case. It also assumes the database application is tracking the identity of the person or other application making the change. For performance reasons, application designers often create a pool of shared database connections that are used by different users at different times. Unless the user identifier is passed through the database connection to the database code, there is no way of knowing which user made the change. This would require additional code changes to the application as well as the database code.

In-line auditing tools can monitor user activity and correlate application network traffic with traffic on pooled connections to associate network identifiers to the use of shared connection pools. Tools from Sentrigo ([www.sentrigo.com](http://www.sentrigo.com)) and Imperva ([www.imperva.com](http://www.imperva.com)) have examples of this type of functionality. This kind of monitoring alleviates the need to make changes to code and does not add load on the database server because the tools can run on separate servers.

---

## Vulnerability Scanning

RDBMS are complex systems with an array of modules and components. Even for seasoned veterans accustomed to working with these systems, there may be parts of the RDBMS that are poorly understood and therefore difficult to protect. Each time an additional component is added to a database server, there is a potential to introduce new vulnerabilities. For example, one may find that the addition of an XML or geo-spatial mechanism to a database server introduces a buffer overflow vulnerability because of a programming flaw in the mechanism's API. Database administrators who manage large installations with multiple servers with varying configurations cannot be expected to manually track all components across all instances and know all vulnerabilities.

Vulnerability scanning tools can automate the detection, and in some cases correction of, known vulnerabilities. The NGSSQuirreL Database Assessment Security Suite from Next Generation Security Software ([www.ngssoftware.com](http://www.ngssoftware.com)), for example, is designed for specific database products and allows DBAs to identify vulnerabilities, assess the risk, and in some cases fix the vulnerability.

## Intrusion Prevention

Another area in which third-party tools can help with database security is with intrusion prevention. With these monitoring tools, anomalous activity can be detected and sessions terminated. Or, in the case of Sentrigo Hedgehog, the sessions can be allowed to continue but subsequent actions are blocked. When considering an intrusion prevention tool for databases, factor in the need for reporting and notification. One may, for example, want to be notified of some types of suspicious activity but allow it to continue as long as it does not cross a set threshold.

## Summary

RDBMS are complex, multi-function applications, but they are not a one-stop shop for data protection needs. There are times when third-party tools can provide a better solution to a particular problem (for example, logging events inline rather than changing application code to log record updates) or can provide a service not offered by an RDBMS, such as intrusion prevention.

---

## Article 6: Where to Spend Your Security Budget Part 1: Identifying Priorities

The trade press and even mass media routinely run stories on data breaches, lost laptops, virus infections, leaked corporate documents, and emerging security threats. With so many potential threats to information assets, it can be difficult to determine the best way to allocate limited resources to protect those assets. This article is the first in a series on security budgeting that will try to shed some light on the process.

Security professionals are the first to note that there are no silver bullets when it comes to protecting assets, and the same can be said for security budgeting. The most rational spending plan for one company may be inappropriate for another. There are however, procedures that many organizations can follow to help them improve the way they allocate security budgets.

In this article, we examine three steps to identifying security priorities:

- Gathering risk assessment data
- Identifying and classifying information assets
- Determining the business impact of security threats

The process begins by casting a relatively wide net to collect as much information as possible and ends by consolidating that information into a focused set of categories that link assessments of risk to business operations and functions.

---

## Step 1: Gather Risk Assessment Data

The first step requires gathering information about risks. The goal of this step is to document and understand the kinds of threats that an organization faces. There are many sources for this type of information:

- General security information available from trade journals, security blogs, vendor security bulletins, trade conferences, professional organizations, and security researchers. These sources can provide readily accessible and low-cost access to information about continuing and emerging threats, such as malware, phishing scams, botnets, application vulnerabilities, and so on.
- Past internal studies, including risk assessment studies, audits, and incident reviews. These sources are particularly useful at identifying areas of weakness in the past that may possibly continue into the present.
- Business strategy documents. These are important for understanding critical business plans and the operational components they depend on. For example, if strategic initiative depends upon supply chain partners having access to the organization's enterprise resource planning system, any threats to that system—from malware attack to service disruption due to natural disaster—should be documented.
- An assessment of IT staff skills and end user training. This is an area that is easily overlooked; humans are often a weak link in the best-laid security plans. The problem is not that employees will intentionally subvert the company or willfully violate policies, but unintentional violations of rules and poor information security practices can quickly undermine the most sophisticated technical countermeasures in place.
- An assessment of the quality of IT governance in an organization. Think in terms of process maturity models in this area. Does your organization respond in an ad hoc fashion to security threats and incidents or do you have policies and procedures in place? Are metrics calculated to measure the state of security management? Do IT executives report to management on the state of information security? The objective of this exercise is to understand how effective policies and procedures will be in the long term. Writing policies is easy; monitoring and enforcing them is more difficult. A governance mechanism should be in place to ensure policies and procedures are enforced.


At the end of this step, one should have an assessment of external and internal threats and weaknesses that can disrupt business operations.

---

## Step 2: Identify and Classify Information Assets

The second step to identifying budget priorities is to understand what assets need protection. This includes both information and tangible assets.

Information in an organization should be categorized by the level of protection that it requires. For example, public information can be disclosed with causing any harm to an organization while confidential data about customers, clients, or patients should not be disclosed outside the group of users who require that information to do their jobs or to the owners or designated recipients of that information. Private information of a company, such as trade secrets and intellectual property, warrants protection by virtue of the value of the information. Regulations may also specify that some kinds of information need particular levels of protection. For example, the financial performance data of a publicly traded company may be governed by regulations dictating how and when it is released to the public.

 For more information about how to categorize and protect data, see “5 Steps to Getting Started with Data Loss Prevention” at <http://www.realtime-websecurity.com/ESMWSv3.asp>.

Tangible assets are the servers, desktop devices, mobile devices, and other hardware that constitute the IT infrastructure of a business or organization. These should be classified according to their importance to the day-to-day operations of a business. For example, if a sales person’s laptop is lost and it contains no confidential or private information, the loss is limited to the hardware replacement cost. If private information is on the device but is strongly encrypted, that may be a low risk incident as well. If, however, an email server is compromised and streams of email conversations may be copied to attacker-controlled servers, a great deal of private information may be compromised. For each tangible asset or class of assets, one should determine the potential losses (relatively, precise quantified measures are not required at this point) if that device were compromised. Once information and tangible assets are categorized according to their value and function, you can move to the next step of determining the business impact of an incident.

---

### Step 3: Determine Business Impact

The final step in this phase of prioritizing a security budget is to determine the business impact of particular risks to assets. As noted, there is no need for precise quantitative measures at this point. It is sufficient to categorize as follows:

- Risks should be grouped according to likelihood. A grouping of high, moderate, and low likelihoods is sufficient. For example, the chances of a malware infection on a laptop without antivirus protection is high; the chances of a database breach through a SQL injection attack may be high if the application code has never been tested or reviewed but moderate if it has.
- Categorize how critical an asset is to the business in the same scheme: high, moderate, and low. The loss of a mission-critical server should, of course, be ranked as high while the loss of a desktop workstation used by one employee is likely to be ranked as low.

Next, calculate the business impact according to the following matrix, where the intersection of likelihood and criticality indicates the level of business impact:

	Likelihood		
Criticality	Low	Moderate	High
Low	Low	Low	Moderate
Moderate	Low	Moderate	High
High	Moderate	High	High

Risks apply to information and tangible assets. The highest impact risks are clearly the first priority for budgeting and the low impact risks are the least important.

## **Copyright Statement**

© 2008 Realtimerepublishers.com, Inc. All rights reserved. This site contains materials that have been created, developed, or commissioned by, and published with the permission of, Realtimerepublishers.com, Inc. (the "Materials") and this site and any such Materials are protected by international copyright and trademark laws.

THE MATERIALS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. The Materials are subject to change without notice and do not represent a commitment on the part of Realtimerepublishers.com, Inc or its web site sponsors. In no event shall Realtimerepublishers.com, Inc. or its web site sponsors be held liable for technical or editorial errors or omissions contained in the Materials, including without limitation, for any direct, indirect, incidental, special, exemplary or consequential damages whatsoever resulting from the use of any information contained in the Materials.

The Materials (including but not limited to the text, images, audio, and/or video) may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, in whole or in part, except that one copy may be downloaded for your personal, non-commercial use on a single computer. In connection with such use, you may not modify or obscure any copyright or other proprietary notice.

The Materials may contain trademarks, services marks and logos that are the property of third parties. You are not permitted to use these trademarks, services marks or logos without prior written consent of such third parties.

Realtimerepublishers.com and the Realtimerepublishers logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners.

If you have any questions about these terms, or if you would like information about licensing materials from Realtimerepublishers.com, please contact us via e-mail at [info@realtimerepublishers.com](mailto:info@realtimerepublishers.com).