

# Risks to Database Security in 2012

## ABSTRACT

Application Security, Inc. (AppSec) publishes an annual update highlighting what we see as potential risks to sensitive information. Today's risk landscape is comprised of an assortment of old, new, and emerging risks and vulnerabilities. Some of the biggest risks today have not changed in the past 5+ years. And while many risks remain the same, they are very real and pose an increasing threat to sensitive information loss and associated breach costs. How organizations defend themselves and mitigate risk is as important today as it ever has been.

## DATABASE RISKS FOR 2012

Databases have become increasingly vulnerable to attack. Two factors have contributed significantly to this escalation: First, organizations are being asked to grant increased access to data stored in the database. This additional access dramatically increases the potential for theft and abuse. Those that require access to data include internal employees, auditors, contractors, subcontractors, and supply chain partners. Secondly, database attackers have changed. In the past, people hacked into networks to "prove they could." While those attacks were malicious, they seldom resulted in data theft. Now the motivation is financial and sometimes political or ideological. The attackers are organized, persistent, and are looking for information they can resell in the form of credit card numbers, Social Security Numbers, government secrets, Personally Identifiable Information (PII), and other proprietary information. This personally identifiable information, as well as intellectual property and government secrets, resides in the database.

Given these realities, organizations require a security strategy that eliminates vulnerabilities, locates sensitive data, identifies user access, monitors database activity, and mitigates risk at the database level. Historically, organizations focused efforts

on perimeter security and external attacks. They invested in firewalls, antivirus software, and secure router configurations. While these investments are necessary, they do little to stop a direct attack on the database. These attacks, if unchecked, can cripple an organization. Current research estimates that 509 million database records have been compromised between 2008 and 2010<sup>1</sup> and with the costs to clean up after a breach estimated at over \$214 per record.<sup>2</sup> Remediation cost for most breaches is in the multi-millions of dollars. In this environment, organizations must protect themselves against the most critical risks first, as well as focus on protecting their databases from new and emerging risks.

The following list highlights new and emerging security risks that IT professionals should factor into their database defense strategy for 2012:

1. **Unpatched Vulnerabilities**
2. **Advanced Persistent Threats**
3. **Misconfigurations**
4. **Insider Attacks**
5. **Insider Mistakes**
6. **Social Engineering**

Responsible firms must implement database security best practices to secure the infrastructure where the data resides. By addressing top risks, adhering to compliance regulations, and applying risk mitigation strategies, organizations should meet the requirements of the world's most regulated industries.

### 1. **Unpatched Vulnerabilities**

Databases continue to experience increasingly sophisticated methods of attack. Attacks have advanced from recognizable exploits to more subtle methods that defy traditional intrusion detection mechanisms. Exploit scripts are posted to the web within hours of database

1 Verizon 2010 Data Breach Report. A study conducted by the Verizon Risk Team in cooperation with the United States Secret Service. July 2009/July 2010

2 Ponemon Institute. Fifth Annual "US Cost of Data Breach Study – Benchmark Study of Companies." January 2010

patch releases. The availability of working exploit code, coupled with a 90+ day patch cycle (at most organizations) essentially leaves the keys to the database available for the taking. Discovering and patching these vulnerabilities in conjunction with auditing and monitoring known unpatched vulnerabilities protects the database from this risk.

## 2. Advanced Persistent Threats

Another risk gaining momentum is large, well-funded organizations making highly focused assaults on large stores of critical data. Known as Advanced Persistent Threats (APT), these attacks are relentless, defined, and perpetrated by skilled, motivated, organized, and well-funded groups. No longer interested in the occasional bits and bytes, organized criminals and state-sponsored cyber-professionals are targeting databases where they can harvest data in bulk. According to the FBI, online fraud and malware attacks are now focused on financial gain or political motivation, and increasingly involve organized crime or state-sponsored hackers. These attacks target large repositories of personal and financial information. Once stolen, these data records can be sold on the information black market or used and manipulated by other governments. With database attacks netting thousands or even millions of records, it's easy to see how this target has increased in popularity. By locking down database vulnerabilities and closely monitoring access to critical data stores, database professionals can discover these attacks in time to stop them.

## 3. Misconfigurations

Database misconfigurations provide weak access points for hackers to bypass authentication methods and gain access to sensitive information. These flaws become the main targets for criminals to launch certain types of attacks often with elevated privileges. Default settings may not have been properly re-set, unencrypted files may be accessible to non-privileged users, and unpatched flaws may lead to unauthorized access of sensitive data.

**Fix Default, Blank, and Weak Passwords** - Ensure that all databases have complex passwords and that default, blank, and weak passwords are eliminated. Make sure to use separate passwords for each instance and enforce and extend the same password policy that your organization is currently using to all network logins. If the database supports it, consider using network authentication, such as Active Directory, instead of username/password authentication.

**Encrypt Sensitive Data at Rest and In Motion** - Never store sensitive data in clear text in a table in the database where any member of a DBA/IT team can access that sensitive data. Ensure that the information is encrypted and not allowed to travel on the network. By locking down database vulnerabilities and closely monitoring access to critical data stores, database professionals can discover attacks in time to stop them. Defense against a SQL injection attack requires a multi-layered approach, and protective measures should be architected with an end-to-end view, meaning that both the web application and the database infrastructure are scoped into the solution.

## 4. Insider attacks

Forrester Research estimates that over 70% of all database attacks originate inside the breached organization. The current economic environment and the associated workforce reductions have created an increase in disgruntled employees—leading many to think insider attacks will increase in 2012. These insiders, motivated by anything from greed to revenge, and immune to the security provided by firewalls and intrusion prevention systems, represent a risk to the enterprise.

Common types of insider attacks include password guessing or theft, privilege escalation, data theft, malware deployment, and denial of service attacks. A recent, widely-publicized breach, attributed to an insider, was perpetrated by an employee who had made the decision to join another firm. Before departing the current employer, the employee accessed and stole over 25,000 proprietary documents. The attack progressed for months before it was discovered. This breach emphasizes the fact that firewalls and network security alone are not sufficient. It is crucial that an organization regularly conduct user rights reviews, assess vulnerabilities, and monitor privileged activity including that of trusted employees and partners.

Far too many people have access to data where there's no specific mandate or business directive requiring access privileges. Or, employees may have excessive privileges that can be used to gain unauthorized access to sensitive data. Essentially, the more conduits there are on a corporate network, the more opportunities there are to exploit those access points – and the more that organization risks external attacks.

In any organization, it's critical to know where the most sensitive data resides. The first step is to conduct a

comprehensive analysis of which users have access to each system, which data and functionality they can access, and verification that the level of access that has been granted is appropriate based on the user's business function. Forward-thinking organizations must proactively implement user entitlement best practices that ensure appropriate access and ownership rights are assigned to critical data. Failure to conduct a full user rights review increases an organization's risk of data access abuse and increases the risk of failing mandated compliance audits.

Establishing strong policy-based access and activity monitoring on critical systems forestalls an insider attack. Activity monitoring and auditing provides alerts on suspect activity allowing action to be taken in a timely manner. Database security solutions geared for the enterprise allow IT and security personnel to set different alert levels based on activity type. These alerts can be intelligently filtered and disseminated in a variety of formats and to defined groups or individuals based on pre-established policies.

#### 5. Insider Mistakes

Another potential risk to database security is the "unintentional authorized user attack" or insider mistake. The most common manifestations of this security incident type include the accidental deletion or exposure of data along with inadvertent, non-malicious security policy circumvention. The first risk occurs when an authorized user inadvertently accesses sensitive data and mistakenly modifies or deletes the information. The latter can occur accidentally when a user makes an unauthorized copy of sensitive information for the purpose of backup or "taking work home." Although not a malicious act, it clearly violates organizational security policies and results in data residing on a storage device which, if compromised, could lead to an unintentional security breach. The widely publicized stolen laptop is a common example of this type of risk.

Conducting regular user entitlement reviews provides auditors, IT advisors, and consultants with a detailed view of an organization's data ownership, access controls, and rights to sensitive information. This process allows organizations to establish and document compliance with the separation of duties controls required by industry and government regulations.

Monitoring Separation of Duties has become increasingly important. Not only are appropriate access rights a key security concern, but separation of duties controls are

also a fundamental principle of regulatory mandates including Sarbanes-Oxley (SOX), Gramm-Leach-Bliley (GLBA), FISMA, HIPAA, and PCI.

To ensure that these unintentional violations do not occur, organizations should extend the critical protections in place at the network and web application layer to the database. Regular database security assessments including audit and pen tests, and misconfiguration checks should be performed to minimize these risks. In addition, activity monitoring can be implemented to guarantee that sensitive data is not unwittingly downloaded or transferred.

#### 6. Social Engineering

In 2011, a number of severe attacks, such as the RSA breach, occurred when legitimate users unknowingly provided security keys to attackers as a result of sophisticated phishing techniques. The success of these new attacks implies that the trend will continue through 2012. In this scenario, users provide information to an attacker via a compromised website or through an email response to what appears to be a legitimate request. Employees should be informed about this type of illegitimate request and educated not to inappropriately respond. In addition, organizations can mitigate the effect of successful phishing attacks by detecting the

## 5 Key Steps to Database Security Process Control

In order to effectively secure their databases, organizations must address five critical requirements:

1. **Isolate Sensitive Databases:** Maintain an accurate inventory of all databases deployed across the enterprise and identify all sensitive data residing on those databases.
2. **Eliminate Vulnerabilities:** Identify and fix vulnerabilities that are exposing the database on a continual basis.
3. **Enforce Least Privileges:** Reset user access controls and privileges to allow access to only the minimum data required for employees to do their jobs.
4. **Monitor for Deviations:** Implement appropriate policies and monitor for any and all activity that deviates from normal and authorized activity.
5. **Respond to Suspicious Behavior:** Alert and respond to any abnormal or suspicious behavior in real-time to minimize risk of attack.

suspicious activity in a timely manner. Database activity monitoring and auditing minimize the impact of such an attack.

## SECURITY AS A PROCESS

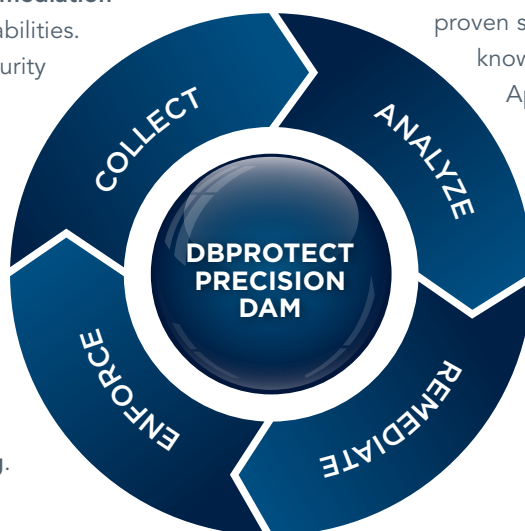
All too often, security solutions are deployed as a series of technologies chasing well-known risks rather than as a comprehensive approach to securing the enterprise. A systematic approach and living process, that can grow and change with an organization, is critical to effectively securing today's dynamic environment.

### DbProtect Enables Database Security Process Control - Collect, Analyze, Remediate, Enforce (CARE)

DbProtect's complete solution **collects** data detailing an organization's database ecosystem through an automated discovery process. DbProtect then **analyzes** the data to highlight areas where risks reside and where database security process improvements are needed. Based on this analysis, DbProtect provides tools and detailed **remediation** instructions to eliminate database vulnerabilities. Finally, DbProtect **enforces** database security processes by monitoring and responding to deviations from authorized behavior.

### DbProtect Precision Database Activity Monitoring

DbProtect helps organizations to understand their database ecosystem, focus on suspicious and unauthorized database activity and streamline their database security operations. This unique approach is **Precision Monitoring**.



## DbProtect™

### DBPROTECT FOR ENTERPRISES

DbProtect is a centrally managed enterprise solution for comprehensive database security, risk and compliance. Based upon proven technology, the DbProtect platform integrates database asset management, policy management, vulnerability management, rights management, configuration and patch management, Database Activity Monitoring with Active Response, and analytics and reporting for a complete enterprise solution. DbProtect enables organizations with complex, heterogeneous environments to optimize database security, manage risk, and bolster regulatory compliance.

## AppDetectivePro™

### APPDETECTIVEPRO FOR AUDITORS AND IT ADVISORS

A network-based, discovery and vulnerability assessment scanner, AppDetectivePro discovers database applications within your infrastructure, assesses their security strength, and identifies user access. Backed by a proven security methodology and extensive knowledge of application-level vulnerabilities, AppDetectivePro locates, examines, reports, and fixes security holes and misconfigurations as well as identify user rights and privilege levels.

## ABOUT APPLICATION SECURITY, INC. (APPSECINC)

AppSecInc is a pioneer and leading provider of database security and compliance solutions for the enterprise. By providing strategic and scalable software-only solutions – AppDetectivePro for auditors and IT advisors, and DbProtect for the enterprise – AppSecInc supports the database lifecycle for some of the most complex and demanding environments in the world across more than 1,300 active commercial and government customers.

Leveraging the world's most comprehensive database security knowledgebase from the company's renowned team of threat researchers, TeamSHATTER, AppSecInc products help customers achieve unprecedented levels of data security while reducing overall risk and helping to ensure continuous regulatory and industry compliance.

For more information, please visit: [www.appsecinc.com](http://www.appsecinc.com) | [www.teamshatter.com](http://www.teamshatter.com)

For a free database vulnerability assessment visit: [www.appsecinc.com/downloads/appdetectivepro](http://www.appsecinc.com/downloads/appdetectivepro)

Follow us on Twitter: [www.twitter.com/appsecinc](http://www.twitter.com/appsecinc) | [www.twitter.com/teamshatter](http://www.twitter.com/teamshatter)

**APPLICATION  
SECURITY, INC.®**

[www.appsecinc.com](http://www.appsecinc.com)