Who's Been Futzing With My Data?

Pervasive Delivers Data Security for Business-Critical Applications

175 Pleasant Street Arlington, MA 02476 617-747-4045 www.baroudi.com

"The Internet opened up opportunities for digital criminals."

Overview and Summary

The explosion of computer usage that came with the PC spread computer skills far and wide. The Internet connected a vast web of machines, opening up an array of opportunities for businesses, including, unfortunately, opportunities for digital vandals and digital criminals both within and outside the corporation. In this paper we examine the whole field of Data Security, touching on Network Security at some points, but not considering it in any depth. We then review Pervasive Software's recent data security release in the light of our findings. Our conclusions are as follows:

- The business risks of data destruction, data corruption and digital crime are escalating rapidly, while the value to the business of data itself is also increasing at a similar rate. The need for comprehensive data security is thus greater now than it ever has been – and it is growing.

- An avalanche of legislation has been enacted across the world which virtually mandates the implementation of data security for most organizations. The upshot is that **not** implementing data security may soon be too big a business risk to contemplate, for fear of legal consequences.

- In the early years of computing a necessary compromise led to the current reality that no natural audit trail exists for monitoring changes to data. For this reason, even widely used database products do not offer comprehensive data security.

- Pervasive Software is not alone amongst database vendors in providing data security features, but is currently the only vendor that provides a comprehensive range of such capabilities within a purpose designed interface. In this, it can currently count itself as the database market leader.

- Pervasive has released a new version of its product set, which deals with all the issues of data security from the data management perspective. Most notably it provides the missing piece – the audit trail.

- We have reviewed the capabilities that Pervasive now offers, and conclude that Pervasive covers all aspects of data security including: disaster recovery, access control, auditing of data changes, auditing of data access, alerting, securing of data on disk and the securing of data in transmission.

- These capabilities are equally applicable to all uses of the Pervasive.SQL database, and are provided with the typical economy and ease-of-use that is the hallmark of Pervasive's software products.

The Data Security Landscape

In the early days of computing, computer power was expensive, storage was expensive – indeed everything was expensive. Because of this, only *absolutely* necessary data was stored on computer. This was an unavoidable compromise and it has had long term consequences.

Strange as it may seem, updating and deleting data is not a good idea. Instead, we should add new values when data changes and simply flag records as deleted *without* wiping them out. When data is updated the previous value it had is destroyed. When an item is deleted, it is destroyed completely. With it goes the audit trail, and incidentally, useful information. Yet we have been doing this for decades, and we still do it, even though we now have huge amounts of storage space available. We got into the habit. Almost all the development software tools in the world assume that deleting and updating data is an acceptable practice, and so our applications continue to do this.

The consequence is that applications have no natural audit trail for data. Thus, it is possible in many situations for data to be changed and for no record of the change to exist. This is good news for someone who wants to perpetrate a computer fraud. It is good news for hackers. It is good news for anyone who wants to damage, steal or falsify computer data.

"Strange as it may seem, updating and deleting data is not a good idea."

Gathering Clouds

This situation might have persisted much longer had it not been for the Internet. By combining many of the world's computers in a single network, the Internet exposed a whole raft of weaknesses in computer security, which in turn put a great deal of data at risk. And, of course, there were many violations of data – the destruction of data by vandals, electronic fraud, data theft and identity theft among them.

The capability of the Internet also shone a light on the problem of data privacy. Privacy legislation has been on the statute books in many parts of Europe since the early 1980s. And it has since been strengthened as concerns about data security and privacy have grown.

The U.S. has moved along a different path, not introducing general data privacy legislation, but gradually introducing a whole series of laws which are now beginning to amount to the same thing. It is easy to see why this happened if you look at digital crime statistics.

The table below shows the Computer Emergency Response Team (CERT) statistics of the number of incidents reported to it in recent years (visit www.cert.org for more detailed information):

Year	1998	1999	2000	2001	2002
Incidents	3,734	9,859	21,756	52,658	82,094

"The number of incidents is roughly doubling each year."

The number of incidents is roughly doubling each year. These figures only record incidents reported to CERT, which specializes in providing security assistance. Other statistics give a broader picture. For example, according to a 2002 FBI study, ***Computer Crime and Security Survey***, 85 percent of survey respondents detected security breaches in 2001 with two thirds of them claiming that they lost money as a consequence. In other words, the level of digital crime is extremely high – so high that companies who have not been affected should probably attribute it to luck.

"The Comdisco study estimated that only 18 percent of companies have disaster recovery capability.

"A high proportion of security problems come from within the organization."

Data Disasters

The sad events of September 11th 2001 drew a good deal of attention to disaster recovery, concentrating the minds of IT professionals and business people on what is possible in this world. In fact, many of the businesses in and around the Twin Towers were in the financial sector and had implemented some form of disaster recovery, so the data damage was not as great as might have been expected. Indeed the major victims of data loss and consequent business destruction in that event were staff agencies, travel agencies and other less computerized businesses.

While impressive, such major disasters are not the real IT concern. According to a 1997 Vulnerability Index Study from Comdisco Inc. (Rosemont, Ill) only about 5 percent of catastrophic data loss has natural or otherwise unavoidable causes, while 68 percent is caused by human error and technology failure, and 2 percent is intentional, such as computer viruses. The Comdisco study also estimated that only 18 percent of companies have disaster recovery capability.

Another sobering statistic (from University of Texas Center for Research on Information Systems) is that of the companies that lose data in a disaster, *50 percent never reopen and 90 percent go out of business within 2 years of the event.* The conclusion is obvious. For many businesses, data is a major asset and its loss is likely to be catastrophic.

Frauds Through The Database

The current epidemic of security breaches has been brought about by a combination of factors, including the ever-declining cost of technology, the widespread knowledge of how to use it and the global computer-to-computer connectivity that the Internet delivers.

Nevertheless, a high proportion of security problems come from within the organization. A recent survey, the CSI/FBI ***Computer Crime and Security Survey*** for 2003, indicated that 45 percent of the companies surveyed had detected unauthorized access by insiders. A UK government survey, ***Information Security Breaches Survey 2002*** carried out by PricewaterhouseCoopers, produced similar results. It found that in small companies in the UK, 32 percent of the worst incidents were caused by insiders, while in large companies the figure climbed to 48 percent.

The CSI/FBI survey found that the greatest financial loss was due to the theft of proprietary information, with losses due to fraud being the third-highest source.

The threat comes both from without and within. There many are examples of digital criminals that made the news. Vladimir Levin, a graduate of St. Petersburg Tekhnologichesky University, managed to defraud Citibank's computers of $10 million, by stealing customer codes and passwords and then using them to wire transfer money out of the bank to a variety of accounts he controlled.

Another example in 1999 involved the attempted ransoming of data. A hacker who went by the alias of Maxim, and who the FBI believes operated from Eastern Europe, stole details of 300,000 or so credit cards from the CD Universe store. When the store refused to pay him $100,000 to destroy the information, he posted the data on a Web site, titled The Maxus Credit Card Pipeline. While the site was operational, visitors could snatch credit card numbers with the associated name and address of the holder.

Threats also come from within. An example is provided by the case of Stephen Carey, a 28-year-old computer engineer from Eastbourne, Sussex in the UK. He was hired by sheet metalwork firm RP Duct Work in April 2002 to do maintenance and upgrades on the company's database. However, he botched the job and RP Duct Work refused to pay for the work.

Carey had left a back door into the company's network which he could access from home. In revenge for his firing, he deleted a database full of designs, causing damage estimated at $75,000.
It is a fact that insiders (contractors or staff) are usually better placed than outsiders to cause damage or perpetrate fraud.

There are many other examples – some of them extremely simple – mostly involving companies that prefer not to be named. A well-placed member of staff may simply change a shipment's delivery address then change it back to the original details once goods are dispatched. A common fraud by dishonest staff in the area of procurement is to set up a fake company from which to procure goods and have genuine supplies "pass through" that company, adding a margin en route. We heard of one case where a company discovered that it had less staff than the payroll showed when it sent each employee a bottle of champagne to celebrate good quarterly results. The HR department had not deleted staff from the payroll when they moved on to other jobs, they just altered the details of the account to which the paychecks went.

All of the above examples involve staff using business applications to defraud the company they work for. The people involved didn't need to subvert the software or the data, they just fraudulently abused the computer capabilities they normally used.

"It is a fact that insiders …are usually better placed than outsiders to cause damage or perpetrate fraud."

Human and Technology Errors

Data destruction and data corruption often occur inadvertently, rather than as a result of malicious intent. There are examples of data being destroyed by disk failure or by errors in software or simply by operational staff making mistakes. Usually such errors are discovered quickly and, if effective back-up and disaster recovery procedures are in place, the situation can be rectified quickly. Here's one example: A recruitment company that had a disk failure discovered too late that it had lost one of its back-up tapes. Several days work had to be re-entered, and of course, the time lost in the aftermath meant lost revenue.

"Data destruction and data corruption often occur inadvertently rather than as a result of malicious intent."

Data corruption is more pernicious because it can persist for a while before it is noticed, and hence recovering from it can be difficult. An example: An insurance company had a software error that was corrupting some of the data on the database. The error put its systems out of action for several days, and it took weeks for it to get them functioning properly again.

User error can also be a source of problems. Users sometimes do not understand the possible impact of their actions. There have been several cases of incorrect prices being put up on Web sites and causing an avalanche of orders. A Hitachi monitor was offered on the Buy.com site in 1999 for $164.50, instead of $588, for a period of 4 days, due to human error. Approximately 7,000 customers brought a lawsuit against Buy.com, which eventually agreed to pay $575,000 in compensation. Similar brand-damaging errors have been made by Amazon, Kodak, Argos and others, and they still occur. Price data is extremely sensitive data and is usually subject to extensive checking procedures. But users still make errors and if there is no audit trail of data, the errors may never be discovered or prevented from happening.

There is also the fact that software can cause data errors. A common one is where a monetary amount grows too large for the data item that holds it and gets truncated, giving it an incorrect value. Such errors can lead to disputes between ISVs and their customers over the source of a specific data error – especially if the ISV cannot find the cause in the affected software. Where there is an audit trail, the cause of error will be immediately clear.

The Universe of Data Security

Having examined data security from both the legislative and the business perspective, we are now in a position to set out a complete picture of data security requirements. In total there are 8 aspects to data security:

1. Security Against the Destruction of Data. This requires disaster recovery capability plus comprehensive back-up and recovery capabilities. The danger here is that data will be irretrievably destroyed or corrupted.

2. Control of Access to Data. This means implementing effective user access controls and permissions, so it is possible to know who is carrying out any activity within the database. Where such controls are absent, identifying who did what is not possible.

3. Audit Trail of Who Changed Data When and How. This requires the database to keep a record of all transactions, with before and after information, and link this to the identity of whoever made any given change. This ensures that there is a full record of all transactions, including any that might be fraudulent.

4. Audit Trail of Who Accessed Data When and How. Similar to the above item, except that it records who accessed data and may therefore have copied it or passed it on.

5. Alerting Systems. This is the ability to detect anomalous circumstances from audit records of changes to data which might indicate fraudulent behavior or severe user errors. Data security is enhanced by catching fraudulent events and severe user errors as they happen, and alerting IT or security staff at once.

"Data security is enhanced by catching fraudulent events and severe user errors as they happen and alerting IT or security staff at once."

6. Security of Data on Disk. Aside from theft of data via access through applications, data can also be stolen directly from where it is stored on disk or tape. The usual defense against this is to encrypt data when writing it to disk.

7. Security of Data in Transmission. Data can also be stolen as it is transmitted between computers, by software that monitors network traffic. Hackers are known to have such software tools. The best defense against this is to encrypt data when passing it between computers.

8. Perimeter Security. Finally, even if data is protected in all the above ways, there is still the possibility of it being corrupted or deleted by an act of vandalism from an intruder on the network, or by a virus. Recovery will be possible if back-up and disaster recovery are in place, but there will still be business interruption. Preventing this involves deploying firewalls, virus detection, intrusion detection systems and other such technology.

If we address all of these eight points thoroughly then we can claim to have secure data. If additionally we also have documented procedures of how the company will respond to any circumstances that threaten the data, then the IT operation will likely satisfy any formal data protection and security compliance procedures.

An Avalanche of Legislation

The perilous state of IT security has not gone unnoticed by legislators across the world. In fact there has recently been an avalanche of legislation that affects IT security across the world, prompted both by increasingly serious IT security breaches and genuine concerns about an individual's data rights. So most organizations, large or small, are now exposed to legal risks if their IT security is inadequate.

Data security legislation has evolved differently in the U.S. than in Europe. U.S. legislation evolved from the ground up, in response to events, whereas in Europe legislation derives from the OECD data protection principles that were published in 1980.

"Most organizations, large or small, are now exposed to legal risks if their IT security is inadequate."

The Strands of U.S. Legislation

Prior to 1999, the only data privacy legislation on the statute books in the U.S. was specific to information held by the cable industry and to educational records. However, since then there has been a slew of legislation, most of which has just come into force or will soon come into force:

Gramm-Leach-Bliley

The Gramm-Leach-Bliley Act (GLBA) of 1999 targets the financial sector, protecting personal financial information collected by banks, insurance companies, brokerages and other financial institutions. There are associated compliance procedures, for which the compliance deadline was July 2002, but quite a few institutions covered by GLBA are not yet fully compliant. After all, compliance takes time and costs money.

Sarbanes-Oxley

The Sarbanes-Oxley Act (SOA) was rapidly introduced into law in July 2002, following the rash of corporate scandals that began with the collapse of Enron. The legislation aims to restore investor confidence, primarily by having the CEO and CFO of publicly held companies personally certify the company's financial reports. Under SOA, any financial misrepresentation is punishable by fines, imprisonment or both, regardless of intent. Therefore, SOA has its greatest impact on the data security of financial applications.

As a consequence of SOA, accountancy best practices now demand the assessing and monitoring of data security, integrity and availability. It is quite likely that these best practices will ultimately be applied to all companies rather than just publicly held companies – as a common standard. The kicker here is that compliance with SOA ultimately requires an ability to audit changes to data.

"The kicker here is that compliance with SOA ultimately requires an ability to audit changes to data."

California Senate Bill 1386

In 2002, the State of California's Stephen P. Teale Data Center was hacked. The Data Center runs the payroll for the State of California. So for a considerable length of time the successful hacker had access to confidential information about 265,000 employees of the state: names, addresses, bank account details, etc. The Data Center did not notify anyone about the security breach for many weeks, leaving state employees – including of course, State Senators – ignorant and open to identity theft attacks.

"With HIPAA, it is necessary to keep track of who accessed information when, where and how."

The consequence of this was California Senate Bill 1386 (CA SB 1386), which came into law at the beginning of July 2003.
The bill demands that all organizations provide Californians with immediate notification when confidential information about them has been compromised due to a breach of security on any computer system that stores their personal data. This law is intended specifically to deal with identity theft, which is said to be the fastest growing crime in the U.S. (Estimates suggest that as many as 7 million U.S. citizens have experienced it in some way.)

As far as the bill is concerned, confidential information means social security number, driver's license information, credit card information and the like. However, the law does not just apply to California: it applies worldwide to any company holding information on Californian residents. It is foreseeable that other state legislatures will imitate California, exacerbating the issue further for companies storing such information.

HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 is aimed at protecting a patient's personally identifiable health information. HIPAA's privacy compliance deadlines took effect in April 2003, but healthcare organizations in the U.S. have until 2005 to implement related security changes.

HIPAA applies to all medical providers who collect protected health information, and carries financial and criminal penalties for any violation, deliberate or otherwise. With HIPAA, it is necessary to provide protected data access, data recovery plans and keep track of who accessed information when, where and how.

The European Picture

European data protection law derives from a 1980 paper produced by the Organisation for Economic Co-operation and Development (OECD); **Guidelines on the Protection of Privacy and Transborder Flows of Personal Data**. Various E.U. countries enacted laws, based on these guidelines, culminating in 1998 with a general E.U. law. The guidelines deal with many issues about how personal data is obtained, how it is used, and individual's rights to change it if it is incorrect. However, the guidelines also demand that:

Personal data must be protected by reasonable security safeguards against loss, unauthorized access, destruction, use, modification or disclosure.

As a whole the OECD principles and legislation deriving from them have become a model for legislation in many parts of the world, including other non-E.U. countries in Europe. Most European countries, from Albania to the Ukraine, had put local legislation in place by 2002.

Most of this E.U.-derived legislation requires that transfers of personal data from E.U. countries take place only to non-E.U. countries that provide an "adequate" level of privacy protection. Naturally this has had an impact on U.S. companies that trade internationally.

As a consequence, the U.S. Department of Commerce issued a document entitled **Safe Harbor Privacy Principles** in July 2000**.** In it, the Department of Commerce advises on what "adequate" means for U.S. companies holding personal data on E.U. citizens. As you might expect, the advice given is to abide by the data privacy principles enshrined in E.U. law.

Pulling It All Together

There has been an escalation in the various business risks associated with IT security and data security that comes from multiple sources:

- The external threat to data from digital vandals and thieves has grown dramatically with the escalation in IT security breaches.
- The threat from within the organization has been growing and involves not just vulnerability to computer savvy employees becoming hackers, but also employees using legitimate application capabilities to perpetrate fraud or destroy data in some misguided "act of revenge."
- To these we can add the continuing threats to data due to error, whether human error, software error or simply hardware failure.
- These threats have escalated the overall possibility of critical data being destroyed or corrupted and thus increased the need for comprehensive disaster recovery as well as more robust data security in all areas.
- On top of this we have recently witnessed the enacting of laws in most of the advanced economies of the world that expose a company to legal risks in the event of any critical data being stolen or destroyed.
- Some of these laws mandate that a company keep an audit trail of access and changes to critical data.

So, in addition to the direct business threats, data security legislation across the world is tightening up to the point where ***not*** implementing data security will soon be too big a business risk to contemplate. Implementing data security to address the threats and satisfy prevailing legislation is not a simple task. It involves keeping a proper audit trail of changes to data and also an audit trail of all access to data. And this brings us back to where we started in this paper.

Because of the way that computing evolved, there is no inherent audit trail for data. The consequence is that new capabilities need to be added to existing database technology if the security risks are to be addressed.

*"Data security legislation across the world is clearly tightening up to the point where **not** implementing data security will soon be too big a business risk to contemplate."*

And Moving On…

Having reviewed the whole subject of data security, we can now take a little time to examine the capabilities offered by Pervasive to address the problem. In doing so we will first provide a brief introduction to the Pervasive.SQL database and its components and then review its security offerings in the light of the eight data security criteria that we defined on page 6.

"The consequence is that new capabilities need to be added to existing database technology if the security risks are to be addressed."

"From Pervasive's view, data security encompasses three distinct dimensions; availability, accountability and integrity."

Pervasive Data Security

Pervasive is an established database company that provides a comprehensive data management solution for application developers focused on small to mid-sized businesses. Its relational database, Pervasive.SQL, is applicable to transaction processing, query applications and mixed workloads.

The product has established a reputation for high performance and scalability combined with ease-of-use. Pervasive claims, with external validation, that it offers the lowest cost of ownership of competitive commercial database products. Pervasive.SQL is also an embeddable database that can be used transparently in distributed applications. The latest release of the product has been enhanced to improve its data security capabilities. In this release:

- it offers replication capabilities via Pervasive DataExchange, which can be used to set up disaster recovery configurations. It can also be used in other processing scenarios, such synchronizing multiple databases or relaying data to query servers.
- it has newly released a further complementary product, Pervasive AuditMaster. This is integrated to work with Pervasive.SQL, and delivers transaction intelligence and proactive monitoring capabilities.

Together, with Pervasive.SQL, which has also had security features added in this release, these components are targeted at providing comprehensive data security.

Pervasive's View of Security

From Pervasive's view, data security encompasses three distinct dimensions; availability, accountability and integrity. The diagram below illustrates how these dimensions are tied together.

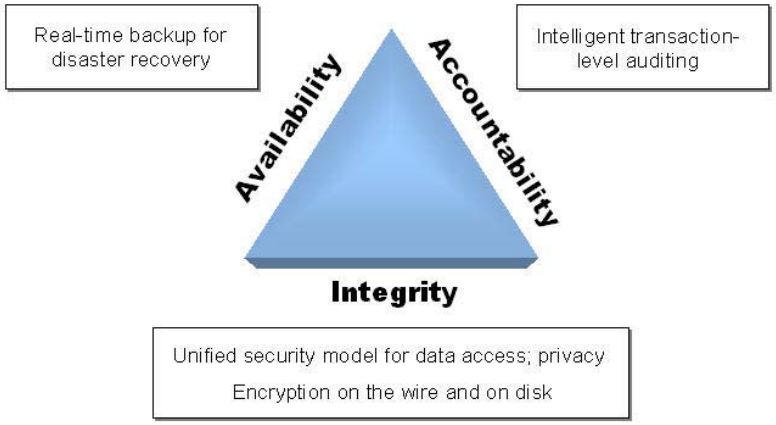

Fig 1 The Pervasive Security Triangle

From Pervasive's perspective, availability is about ensuring the availability of data, which means providing real-time back-up of data to enable the swift recovery of applications if they fail and, in extremis, disaster recovery. Accountability is about knowing who did what to data, when and how, or who accessed what data, when and how. Integrity is about ensuring that data cannot be read or corrupted while in transmission or while stored on disk or other media.

How Pervasive Data Security Stacks Up

In the previous section of the report, we described eight aspects of data security that constitute the full picture:

- Security Against the Destruction of Data
- Control of Access to Data
- Audit Trail of Who Changed Data, When and How
- Audit Trail of Who Accessed Data, When and How
- Alerting Systems
- Security of Data on Disk
- Security of Data in Transmission
- Perimeter Security.

We can now examine the capabilities of the Pervasive product set to see how well it aligns with these criteria.

"With Pervasive.SQL it is possible to ensure that all access to data in the database only happens through the database."

Security Against the Destruction of Data

Pervasive DataExchange provides a full replication capability that can be used within a disaster recovery configuration, with server hardware residing on a back-up site. DataExchange can also be used to synchronize multiple databases (in whole or in part) and this capability could also be used as part of a disaster recovery arrangement. The interval between data being written to disk and replicated can be scheduled according to need, and can, if desired, be set as low as one minute.

Pervasive.SQL also provides the usual comprehensive back-up and recovery database capabilities to deal with situations where machines or software fail. It is comparable to other industrial-strength databases in its capability to manage back-up and to enable swift recovery following any failure.

Control of Access to Data

The majority of industrial-strength databases provide a means of linking users to data as it is written away to the database, granting or denying permissions to access and change data, and recording who did what. Pervasive.SQL is no exception.

Capturing this information is necessary if an audit trail of data is going to be kept. As with other databases, this capability can be used or not used, and if it is going to be used then data access policy per user or user role needs to be determined and implemented. Note also that applications which use the database must provide identity information to the database.

With Pervasive.SQL it is possible to ensure that all access to data in the database only happens through the database. All programmatic or user interfaces to the database pass through the same control procedures, which cannot be circumvented.

"It records who did what to which data, where, when and how."

Audit Trail of Who Changed Data When and How

This is where Pervasive AuditMaster comes into its own. It resides in the kernel of the Pervasive.SQL database taking a before and after image of each database record as it is written. It records who did what to which data, where, when and how – capturing the user ID, network station ID, date and time, application, database table and operation type, along with the application data. It records all database events rather than those for a specific application, recording the important contextual data that most databases do not record, including non-DML events such as error messages.

"AuditMaster keeps an audit trail of itself, storing queries and their results, metadata changes and all alert triggers."

Rather than simply being written away to a log file, the before and after images are held in a database table, so that they can be analyzed if desired, using AuditMaster's querying capability – which is structured so users can make query requests on the basis of who, what, where, when and how. It is also possible to access this data using any common database reporting product.

There is a small performance overhead for using AuditMaster, which averages out at about 3 percent of normal database operation. Such an overhead is inevitable in any product implementing this kind of capability, and is, in any event, very low.

Because it is integrated into the kernel of the database there is no possibility of users or programmers interfering with its operation. Furthermore, AuditMaster keeps an audit trail of itself, storing queries and their results, metadata changes and all alert triggers.

Audit Trail of Who Accessed Data When and How

Aside from recording all changes to data, Pervasive AuditMaster can also record all accesses to data, so it is possible to determine who had access to any specific item of data in case of a breach of confidentiality. As when dealing with changes to data, AuditMaster also records much more data than the database access information.

Access details are stored in the same database table that stores update information, and the same simple "who, what, where, when and how" query capability is available to query such data.

Alerting Systems

Pervasive AuditMaster does not just gather information for analysis, it also provides the ability to define alerts that are triggered by specific conditions, such as, say, a change to an invoice amount. Once an alert is set, AuditMaster will carry out an associated alerting action if the condition that is being tested for is found.

The default action is to send an email to a designated email address, but greater sophistication can be programmed in if desired. The alternative is to invoke a user-written routine, which might, for example, send out an SMS message to a mobile phone. If desired, each condition can invoke a different action – although in practice the user will probably want to classify alert conditions and responses into a small number of groups.

"It requires no programming, it is simply a matter of specifying data security rules, or possibly error conditions, using a simple interface."

Alerts can be defined on individual values or on ranges, so checks can be placed on individuals or groups of users, specific application transactions, specific remote PCs, specific times of day or night, specific data items that might be subject to fraudulent change and so on. Again it is a matter of who, what, where, when and how. Happily, it requires no programming; it is simply a matter of specifying data security rules, or possibly error conditions, using a simple interface.

AuditMaster alerts may appear similar in some ways to database triggers, but there are distinct differences. They provide access to security data that other database products do not make available. They are not intended for, or designed for, adding application logic or any of the data dependency logic for which triggers are often used. One might legitimately use this mechanism to test for large (and hence probably erroneous) value changes in critical data fields such as prices, as in the Buy.com example. Such errors might be due to software error, human error or deliberate malevolence.

In any event, alerts are confined to and designed for data security, and they can be implemented by staff that do not have programming experience. If implemented intelligently, they can make a powerful contribution to data security.

Security of Data on Disk

Data can be stolen by simply copying or even stealing the disk(s) on which it resides. The best defense against this is to encrypt the data as it is written to disk, using an encryption scheme that is very difficult to break. All encryption schemes can be broken by brute force if enough computer power is applied directly. So the best that can be done is to make the process very difficult. To this end, Pervasive.SQL provides 128-bit data encryption to disk as an option.

Security of Data in Transmission

Pervasive DataExchange has the option to encrypt data while in transmission, using a 128-bit key, so that information cannot be stolen "off the wire." As Pervasive.SQL is frequently used in a distributed environment, where a good deal of data passes between multiple databases, encryption is a particularly important security feature for the product. This encryption capability ensures that data is encrypted when replication is used to send data between databases or to back-up databases.

Perimeter Security

Although necessary, perimeter security is not a matter for the database and hence cannot be addressed from there. However, this should not deflect those who are considering implementing comprehensive data security from also considering whether the perimeter security of the network is adequate. If it is not, then the possibility of data being corrupted or deleted by an act of vandalism increases. However, if all of the data security points discussed above have been addressed, the data will still be safe.

In Summary

The combination of Pervasive.SQL, Pervasive DataExchange and Pervasive AuditMaster provides a comprehensive data security capability that manages the whole gamut of data security issues. In this paper we have looked at the data security issue from both the legislative and pragmatic views, to provide as complete a picture as possible of current data security requirements.

Baroudi Bloor's conclusion is that Pervasive provides all the features that are needed for secure data management and delivers them with its customary, easy-to-use and well designed interface. At the moment, it can claim to lead the market.

"Pervasive provides all the features that are needed for secure data management and delivers them with its customary ease-of-use…At the moment it can claim to lead the market."

This paper was created for Pervasive Software by Robin Bloor and edited by Carol Baroudi of Baroudi Bloor, a research, analysis and strategic advisory company serving the IT industry.

Robin Bloor is Research Director of Baroudi Bloor and President of Bloor Research, one of the world's leading IT analyst and consultancy organizations, distributing research and analysis to IT user and vendor organizations throughout the world. Contact him at ***robin@baroudi.com****.*

Carol Baroudi is CEO and founder of Baroudi Bloor. Her more than 20 years IT industry experience include: her role as VP, Emerging Technologies, at Hurwitz Group; her co-authorship of the best-selling Internet book of all time – The Internet For Dummies; information architecture; management consulting; and software development. Contact her at ***carol@baroudi.com****.*

BAROUDI BLOOR

175 Pleasant Street ◢ Arlington, MA 02476 ◢ 617-747-4045 ◢ www.baroudi.com