TRUE Data and Information Protection

Published in July 2006
Article by Ifeanyi O. Asonye

INSIDE THIS ARTICLE:

Overview- Security Breaches

One by one, bit by bit, inch by inch patiently over the years, they learned the systems inside and out; then they went ahead to study people and business modus operandi. Suddenly, **in January 2005,** a new of wave data and information security breaches began to happen to individuals, various businesses, organizations, government and educational institutions. **The reports continued to roll in several times a month afterwards.**

A few years ago, not quite too long ago, the single biggest factor for **virus** and **malicious code** writers was just a case of **blatant ego.** Now, it's very obvious that **Cyber-vandals** graduated rapidly into highly sophisticated icons who are **trusted business people** and **professionals** and **they want to make serious cash**, and I mean **a lot of serious money.** **In some cases, they've used a most sophisticated software tool known as RootKits.**

The most embarrassing of the lot happened in the financial industry: ChoicePoint, CardSystems, Bank of America, Privacy Rights Clearinghouse, CitiFinancial, then Trans Union, Air Force and large retailers such as DSW Shoe Warehouse and B.J. Wholesale Club, **to mention only but a few.**

Update June 19, 2006- Data Breaches continue despite efforts and commitment to Information Security and Data Protection. **More than 90 of such incidents have been reported since January 2006, since the ChoicePoint incident, over 88 million personal information has been exposed.**

The media has been focused on the consumer's point of view and the very much less publicized are the true depth and breadth of **risks** and **costs** of **Financial Engineering**, Debit/ Credit Card, Personal and Business Account Fraud in the financial industry. The fact that many of the financial firms are insured by the FDIC, completely backed by the government, or both imply that the tax payers are fully responsible for the losses.

The Federal Trade Commission (FTC) estimates that about **10 million Americans** have their personal information pilfered and misused in one way or another every year, **costing consumers $5 billion**. **The cost to businesses is approximately $48+ billion annually.**

The sheer volume of data that's available when a computer system is compromised or through missing backup tapes makes it obvious why the problem is now being fought on all fronts. Costly but necessary and among the toughest sells for solution providers is Information Security, at least until their clients find out first hand on just how vulnerable that they are.

A few Cases in Point:

- In Feb. 15, 2005, ChoicePoint, Alpharetta, GA had bogus accounts established by **ID thieves, 145,000.**
- Feb. 25, 2005 Bank of America, Charlotte, NC, **lost backup tape 1,200,000.**
- In May 2005, credit card processor CardSystems (Atlanta, Ga.) revealed that a Cyber-criminal had harvested at least **200,000 card numbers** from the **40 million** **unencrypted transaction** records it had parked on an Internet-accessible system.

Click Here => **Chronology of Data Breaches Reported Since the ChoicePoint Incident**

Updated July 13, 2006 (Computerworld) -- William Sams, the CIO of Ohio University in Athens, Ohio, **has submitted his resignation**... 'The IT organization at Ohio University is **positioned for a major transition into a 21st century leadership position**," Sams was quoted as saying in the statement. "However, it has become clear to me that a new energy level and skill set is going to be required in order to allow our IT organization to realize its potential,' he added. The development should come as no surprise to anyone, given the scope of the breaches, said Pete Lindstrom, an analyst at Spire Security LLC in Malvern, Pa.

Some calamities have created an opportunity for savvy storage solution providers on most of the fronts. **Information Protection, Controls, Identity Systems of Systems Interoperability, Integration & Management, and 0s & 1s level Data Protection are now being required;** they must be implemented at all the different levels.

They will include **Access Control - Data**, **Audit Policies**, **File level** and **Storage System/ Sub-System Encryption**, **Authentication**, **Highly Secure Data Management Policy-Based Security** and **Strategies** using a *Consultative Digital Approach*, emerging *Project Management* and *Information Lifecycle Management methodologies*, integrating Data

Access Security at all levels of the **Application**, **Physical** and **Network stack**, and in creating secure **Disaster Recovery** and **Business Continuity Products** and Solutions.

Many fall into the trap of thinking that data protection simply means installing network firewalls and deploying effective antivirus software. While these basics are just a beginning, **in-depth data protection goes far beyond those essentials.** Said Beth Cohen, Thought Leader for Hot Technologies at The Advisory Council (TAC) in an article on Data Protection.

All of these, and all that will follow *must* be directly mapped and designed into the underlying System Architecture and Infrastructure**.** Everything including Reliability, Efficiency, Speed, and Redundancy are dependent on the System Architecture and Infrastructure**.** When it comes to information protection, would it matter the type of industry that you and your customers are in?

Going from the **Widgets to Data Bits** and **Bytes,** and **from the 0s** to the **1s Digits**, they are ultimately information and data which must be **protected**. The **data encryption products of your choice must be happy with your storage implementation and supported** by the entire **System Architecture** and **Infrastructure.** If they are a public company then, it must be **designed** to meet the **SOX (Sarbanes-Oxley**) Compliance requirements among others. 'The nature and placement of the storage system within the pipeline will affect operation and efficiency', *said Ifeanyi O. Asonye, after a recent study and consultative project for multiple, and multinational enterprise environments."*

Ifeanyi, explained further that the hierarchal structure of a Directory Service- 'Just like designing and building **a big house** or a **tall building**, the foundation and initial structure has to be carefully designed and built right the first time. It may be structured in so many **creative** ways'. This structure will hold all the 'wish lists' we have of a dream home, commercial, tall business or residential building or tower.

It has come to observation that when Windows 2000 with Active Directory arrived in 2000, most environments nonetheless implemented it same way as NT 4.0 Domains with Exchange Domain Sites and Directory Services. A few months, and a few years later, they executed something called 'dcpromo' to upgrade/ install the Active Directory only to find out that everything got broken in the process"**.**

During various board meetings in my role as a **member of Professional Advisory Committee** at the local community colleges, at that time in 2000-2001. I explained to the **board** and the **NT 4.0 Instructors** that the Active Directory was different from NT 4.0 Directory, and that **extensive retraining** is required to understand, teach and to coach on it. Only very few seemed to begin to understand that it was a real fact, not until the Directory Database in that production environment failed under an '**unsupported'** Forest/ Domain configurations and Design, Ifeanyi said.

Five years later, in the **Fourth Quarter of 2005**, for the first time, the revenues for Windows 2000/ 2003 based x86 topped spending for Unix systems, according to analyst firm IDC**.** Windows-based x86 Servers has shown continued growth, while the RISC and mainframe spaces showed decline. The **Features** and **Capabilities** of the Active Directory like the computer connectivity problems that it has solved enables a lot of things for has not been matched. The Active Directory technology built into it's Directory Services is something that IBM struggled with, and could not solve for more than 25 YEARS- It require a completely different mindset looking at it.

The Architecture of the Microsoft® Active Directory, and Identity Management and LifeCycle Servers, is like a Big Forest with many big trees, many branches and millions of leaves. Just like a Sea, and a very big Ocean, ….like planning a Big Town, whereby a Town Planner and what the Architect does to produce the Blueprints.

Over years, a building, a Town or an entire City, just like a Business Structure and a Business Model could be completely or partially Renovated, Restructured or Modified as needs Business and Designs change. That's what you get with the Active Directory, it's structured to connecting everything World-Wide!. The **directory** is extremely deep with **so much flexibility** that a solid understanding of the **business side** and the **directory** are **critical",** Ifeanyi pointed out.

From the overall Architectural, Infrastructural, and End-Users Applications perspective- Two environments are never exactly the same in so many ways. **A lot of the differences lie in the way things talk to each other.** The way things communicate include the **procedural** aspect of how things are done within the environment, **the policies** and controls that are in place, the **people that implement the systems**, who **work within the environment,** and to the access permissions on the business side, **from the way the Enterprise Organizational Structure is designed into Architecture, to the smaller applications such as Word, Outlook and to the Financial Databases.**

‘Extensive industry experiences, talents, knowledge and skills will count in getting the job done right with the right things. **Not the type as in playing with Microsoft Word, Excel or FrontPage.** We discussed how the different variations and combinations of Spyware, Malware, Worms and Trojan Horses happily and excitedly ‘climb’ over firewalls. This time, it is **not only j**ust about installing and implementing the **best firewall technologies**, the latest and the greatest **Anti-Spyware, Anti-Phishing** and **Anti-Malware Security Suites’**.

Ifeanyi, summarized that: ‘It's obvious that the right design structure is well-advised, than costly Hours, Days, Months and Years of **futile** Re-Engineering and Engineering Revisions. We must build and bring information and Data Protection, Business, Management, Technology, Engineering, Connectivity, Integration, Convergence, Unification and Merging all at once into the **System Architecture** and **Infrastructural Design,** from the ground up. **Not the other way’. Then you take the Microsoft® Active Directory into that Design the most widely used Directory acting as a building block for its Foundation.**

It's high time we considered a few other facts such as:

- **Current Online Data Mid-Sized firms: 5-10 Terabytes (TBs); Large Firms: Petabytes (PBs)**
- **Data Growth (at 50-70% per yr in Terabytes (TBs) and Petrabytes (PBs)**
- **Business Continuity and Redundancy (Costly to Implement)**
- **Disaster Recovery (Bedridden by Inefficient, outdated Technologies)**

Data Encryption Technologies (Several older PKI Technologies now have proven Flaws. At this moment, even if the size of the data is not **stupefying enough**, well there are **several complicated** and **stringent compliance requirements** and **tough new regulations like SOX, IPv6, HIPAA, CISSP, CISM, SB1386, FCAPS, GLBA, and FISMA.**

Microsoft® built tools for **data encryption** at the file system level using the New Technology File System (**NTFS**) they are now considered **crude, not quite sophisticated enough.** Microsoft® just came out with **BitLocker Drive Encryption; referred to as Secure Startup Full Volume Encryption.** One may be astounded to learn that 'underneath' the new Microsoft (newly acquired) Groove Networks Groove application, now known as **Office Groove**, is indeed a layer of a **new platform of Storage System that's superior to a file system**. It incorporates Advanced Security Mechanisms, **nice and fast search features** with seamless File and Folder Synchronization Capabilities through 'Firewalls' with Unique Storage Schemas that allows a wider variety of applications to be developed on top of it.

Microsoft has stepped up to the plate, and responded to its new and re-born **'Security Calling'** by solving key security problems that plagued businesses -**the security weaknesses of a USB drive** (Universal Serial Bus drive). **A USB drive basically will not carry security controls and permissions effectively**. A user can always pop a USB drive into a server or a desktop pc and copy data, bypassing your physical security, **or better still unplug and take home a USB storage solution on a server.**

With the new Longhorn Server (to be named Windows Server 200x upon release) and Vista, an administrator will be able to use the group policy to specify device IDs, a range of products or devices to be used and installed at the computer security level, but not others.

Scalable Storage with Security

A few years ago in the storage solutions area, technologies such as **Fiber Channel Storage-Area Networks (SANs)** with or without Clustering Technologies were very expensive and mainly available for Terabytes of Storage requirements.

Presently, we have robust alternatives such as the iSCSI SAN, NAS (network-attached storage) devices, and clustering technologies that are

Protecting The "Low-Level" Digital Zeros and Ones- The Ultimate Key to Complete Data and Information Protection

solid technologies to reckon with in the growing global storage market.

In a recent study and Consultative Active Directory, Exchange Design and Integration Project for various establishments; during an exhaustive Systems Analysis/ Briefings, we learned that some multi-billion dollar Global and Publicly Traded Companies use few 150 GB to 500 GB external USB drives that are plugged into the servers as a storage solution.

How many more of these kinds are out there? **Are there many more companies that are unknowingly putting themselves at risk for** costly litigation **and** public relations nightmares' **by not addressing these issues?**

The Limitations of the Tape Storage

Most environments and compliance regulations require maintaining **online data set**. On-line backup service has turned out to be a good news and bad news situation for the entire industry.

Making Data and Information active and available online is just one aspect of the challenge. High-level of security adds another level of complexity and difficulty. *In this type of scenario, for example, a publicly traded healthcare establishment will be faced with SOX, HIPAA, IRS and OSHA regulations.*

The limitations of tape backup system include, but not limited only to the **inconvenience** for quick recovery of individual files or groups of files, but also the complications associated with doing business globally.

Retrieving several **Terabytes** and **Petrabytes** of Data can easily **take many days. It is extremely important that mission-critical information** and **data is secure, highly available,** and **easily retrievable when a disaster strikes.**

Compliance Regulation relative to Specification

There is no doubt that 'compliance complications' can become overwhelming very quickly, all that you really need to do is: **'Throw enough Skills, Talents-STRENTHS and Resources at the Problem and a Rock-Solid Solution will be born'.**

In summary, we will consider the entire compliance and regulatory requirements for an environment with consideration to following factors:

- **Critical Information and Data Confidentiality,**
- **Security based- Physical Access**
- **Function-Based Information Access**
- **Group Membership Policies,**
- **ACL's (Access Control Lists)**
- **Application-Enforced Business Rules**
- **Data/ Information Encryption needs and Tradeoffs**

Bottom-line is that executing and managing large datasets, and meeting compliance and regulatory requirements begins by **creating clear, realistic** and **ACTIONABLE information management policies.**

Ultimate Business Information and Data Needs

Action, Executing through **Consultative Biz Approach (CBA)** and **Consultative Digital Approach (CDA)** step by step approach to Business Technology Solutions, **incorporating Ultimate Business Information and Data requirements**.

They are broken down into Four Unique Phases or Steps including:

- **Determining the Ultimate Business Dreams and Goals**
- **Specify Data Integrity and Value Requirements**
- **Determine High-Availability Requirements**
- **Determine Confidentiality Requirements**

Many technologies and encryption solutions that are available to Small, Mid-Sized and Enterprise Businesses, for example, **Data/ Pipeline Encryption, Server/ Host Based Encryption, and the Encryptions.** Our experiences, further studies, tests and research came out with impressive current and the **next generation** solutions with built-in encryption functionality at all levels.

What is the ultimate goal? What are we looking to accomplish?

...a World-Class secure **Business Information Access** and **Data Protection;** a **Highly Scalable Storage System** and **Sub-Systems,** *with* ***High-Availability***, ***Redundancy***, ***Instant Disaster Recovery*** and the ***Highest Level*** *of* ***Security***, appropriately **safeguarded,** and with **Accessible copies of the Information** and **Data in Multiple locations.**

Let's Connect! **Follow Us On Click Here =>:** **FaceBook** | **Twitter**