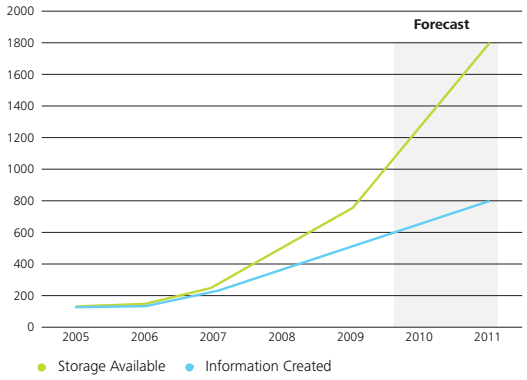
Protecting what matters

The world contains a vast amount of digital information which is diverse, complex and most importantly, continuing to grow at an exponential rate. Although this new information superhighway allows us to make gains in all sectors, it also creates a host of problems, not least of which is data protection.

According to market research company IDC, last year, despite the global recession, the Digital Universe set a record. It grew by 62% to nearly 800,000 petabytes[i].

This vast amount of data at our fingertips has made it possible for us to perform some of our greatest achievements including finding cure for diseases and exploring the boundaries of our universe to name a few. The constant correlation, integration and convergence of data continually represent opportunities to generate value and insight in the world of economics, science and society.

Global Information Created and Available Storage
Exabytyes

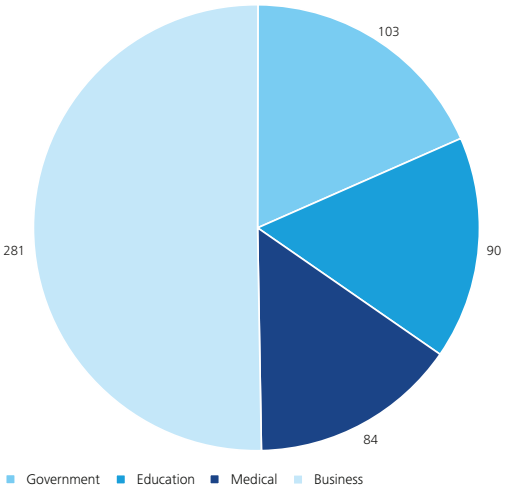


But all this data is also creating a host of new problems. Despite the abundance of devices and appliances to collect, store, use, and share all this information, current volumes of data already exceed the available storage space and organizations are having to strike a balancing act when it comes to ensuring data security.

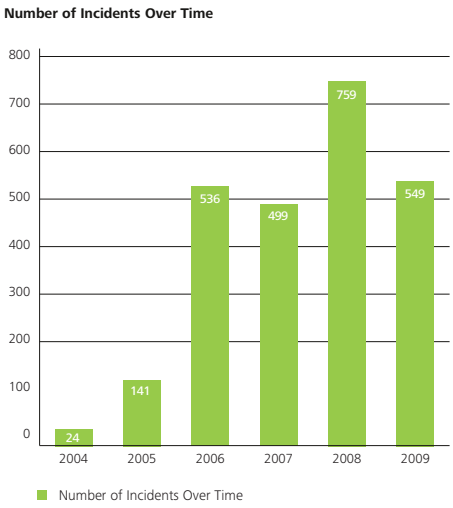
Sharing information is a strategic need for organizations seeking innovation and collaboration. At the same time, protecting one's organization's intellectual property is vital to its longevity.

According to the Open Security Foundation, 555 publicly reported data breaches involving personally identifying information in 2009 affected over 220,619,182 records[ii]. Although lower in terms of number of incidences from 2008, this number continues to represent an average increase year on year.

Incidents by Sector (549 Publicy Reported data breaches in 2009)



Economic and competitive pressures have changed the business landscape. Information must be used effectively and efficiently for an organization to be successful. Outsourcing, off-shoring, partnerships and mobile employees and customers have blurred organizational boundaries and complicated information management. Sharing information is a strategic need for organizations seeking innovation and collaboration. At the same time, protecting one's organization's intellectual property is vital to its longevity.



How to respond

A clear and well-defined approach supported by tools and experience, are the keys to success. Understanding the current operating environment, implementing the necessary controls and acquiring the right capabilities to protect a company's information assets are performed through a five-step process:

I. Know your data

Primary to protecting your information assets is to understand what information you have, where it is, its business value and who has access to it. It is also important to know how information flows in and out of your organization to your business partners, government agencies, employees, customers and ultimately, competitors. Many organizations are unaware of the information they possess and its critical importance to their ongoing business activities. As such, identifying sources and copies of information inside and outside of the organization's boundaries is critical. These sources can be structured or unstructured data in various forms, including endpoint devices, servers, archives, backups and prints.

Top management, business management, auditors, compliance officers and IT managers should work together to make sure data protection programs lead to cost-effective and well-controlled IT delivery.

Using business processes, software applications, customer segment information, auto-discovery tools, interviews and workshops, it is possible to obtain an inventory of the organization's information assets.

Data classification is the process of classifying information based on its operational value and regulatory value. This exercise can produce instant and powerful results that provide a demonstrable improvement in the way that client data is protected.

II. Know your data lifecycle

Once data is discovered it is important to understand its lifecycle from origination to processing, maintenance and disposal. Gaining a good understanding of the lifecycle of the data and its related controls at each stage clarifies many of the threats and vulnerabilities associated with its dissemination.

III. Know your channels

Data is seldom stagnant. It continuously flows throughout the organization and beyond. Identifying the channels used by the organization to collect, process and distribute information is a necessary step in understanding the threats, vulnerabilities and risks. The first three steps provide a clear understanding of the current state of data protection in the organization.

IV. Implement & monitor controls

Armed with knowledge of the existing vulnerabilities, threats and risks, it is time to implement the necessary controls. These controls fall into three main categories of preventive, detective and corrective controls that may protect:

- **Endpoints** such as desktops, laptops, mobile devices, software applications, fax machines, printers and other systems.
- **Channels** such as Internet, network, phone and e-mail.
- **Data lifecycle** such as creation/caption, organization, processing, storage and disposal.

Constant monitoring and measurement of controls is necessary for continuous improvement. As a result, an adaptive approach to evolve with the changing threats and risks is needed.

V. Acquire capabilities

To keep up with the shifting and evolving threats, it is necessary to acquire the requisite capabilities. These capabilities allow your information security to evolve with the challenges and prevent undesirable incidents proactively. The primary and requisite capabilities are:

- Information Governance
- Information Management
- Access & Identity Management
- Enterprise Application Security Management
- Communication & Messaging Security Management
- Risk Management
- Privacy Management
- Fraud Management
- Security Training & Awareness

In order to be most effective, any data protection program should be applied within the business context, focusing on where their use would provide the most benefit to the organization.

Top management, business management, auditors, compliance officers and IT managers should work together to make sure data protection programs lead to cost-effective and well-controlled IT delivery.

by **Fadi Mutlak**, senior manager, Enterprise Risk Services (ERS), Deloitte in the Middle East

Sources

(i) IDC White Paper sponsored by EMC, The Digital Universe: 2010 Update, May 2010
(ii) DatalossDB.org Data Loss Database, 2009 yearly report