Data Protection and Privacy
A Business Perspective

Managing and controlling data has become more difficult. Your business relationships have probably grown also. So have the associated risks. Between outsourcing and offshoring, supply chains, alliances and partnerships, the very definition of the enterprise has changed. You may outsource your payroll, human resources, warehousing, manufacturing, or order fulfillment. Doing so exposes critical personally identifiable information (PII) data and your intellectual property secrets. You also share data with your customers. The new reality is there is no separation between business partners, customers, competitors and you.

It's no wonder that data privacy issues and actual breaches continue to grow. Information moves freely between business partners and gets replicated, combined, and modified along the way. Data is transferred from corporate servers to laptops, USB drives, and smart phones. Information is copied into spreadsheets, databases and emails. It gets transmitted and stored both properly and improperly. This data carries a significant price tag for collection, storage, and maintenance. It also carries a significant potential dollar and reputation cost if it is misused or lost. The end question becomes, do you have any idea where your data is?

The answer too often is no. The importance of data to effective decision making continues to grow as organizations spend increasing amounts on business intelligence and analytics. However the quality and integrity of the data is often compromised. Many organizations don't tag, identify, catalogue, or classify their data. They fail to handle it properly in terms of storage, management, retention, retrieval, or destruction. They really don't know if they are retaining the right data, good data or the wrong data. While a critical data inventory is required, too often organizations perceive a low cost benefit and choose inaction.

Since many organizations lack control of their data they often don't know when or how they suffered a data breach. The consequences can be enormous. Data breaches can often go undetected. The resulting fire drill to mitigate gaps and enhance security may be the least of your worries. Potential revenue and reputational lost is the real risk. It can take months to recover.

The costs to you can include:

- Damage to public trust and branding
- Loss of business and reduction in revenue
- Damage to relationships with customers, employees, and business partners
- Cost of litigation and regulatory fines
- Cost of compliance with intrusive enforcement requirements
- Cost of remediation efforts and postponement of other investment priorities

What's your biggest Security Risk

Where does your biggest security risk lie? Is it hackers, terrorists or natural disasters? Or is it the people and entities you interface with daily? It's actually your employees, customers and business partners. While fraud is always a problem the bigger issue is that humans are susceptible to error, carelessness, fatigue, and distraction. They are also vulnerable to phishing and other social engineering attacks. Breaches are as much a result of careless behavior as they are of malicious intent.

- Individuals often pass information to others in the organization who do not have the same permission or access rights creating data leakage
- Routine personnel activities like promotion can often create situations where individuals gain new access rights without ever relinquishing their old permissions
- Individuals often leave machines unattended while they perform other activities or responsibilities
- Business partners do not maintain strong segregation of duties controls and separation of customer data

When a major security or privacy breach occurs, CEOs, CFOs, and CIOs suddenly get motivated. They ask are we protected? Our systems are secure, right? This can't happen to us? Unfortunately, the answer too often is yes it can.

Data breaches have become all too common. In recent security surveys almost 50% of respondents reported five or more breaches per year. And the costs can quickly add up. A simple malicious insider attack can take on average 14 days to remediate at a cost of $18,000 per day.

Consider the major data loss recently suffered by a large financial company. To deal with the event, they sent postal notifications to several million customers whose PII data had been compromised and purchased several months of credit report monitoring for each affected consumer.

So why do so many organizations wait for a crisis to affect a competitor or a new compliance regulation to act ? They often don't see the tie between strong security governance and customer retention , revenue enhancement and overall organization stability until a problem occurs. Also, the ROI for security and data protection expenditures from improved decision making with better data, less data breaches, and better industry and customer relationships is not well understood.

Developing a Data Protection and Privacy Plan

So what needs to occur? Organizations should:

- Develop effective and efficient risk management approaches
- Complete and maintain an accurate inventory and valuation of information assets
- Make a sufficient investment in information security and privacy
- Utilize proven solutions that enable the safe delivery of information
- Perform proactive mitigation of threats that are increasingly targeted and sophisticated

To be truly effective, security and privacy should transcend policy-making and become everyone's issue. Threats and opportunities must be broadly understood; priorities and shared responsibilities communicated; and the message transmitted to stakeholders up and down the organization. Data security and privacy is more than just an IT problem. However, most organizations place responsibility for data protection and privacy with the information technology group.

Security and privacy has grown substantially more complex in recent years, necessitating a multidisciplinary approach. The CIO and IT can take a leadership role, but legal, compliance, HR, and other business units should be involved. At its core, security and privacy is a business issue, not a technology issue.

So how do you complete a data inventory project on your own terms before a breach or crisis occurs. You should:

- Develop a full understanding of your data assets
- Consider regulatory requirements
- Determine their true risk and net value
- Strengthen protections or loosen restrictions as needed

The team will examine data structures and management practices, catalogue existing information, assess and assign risk and value. It will determine how you handle your own data, along with that of your customers and vendors. It will examine your data gathering and retention practices. Other questions answered should include:

- Why are we collecting this data?
- What are we doing with it?
- What is the value of the data?
- Are we gathering superfluous or unnecessary information?
- What risks are we mitigating or creating?

Remember once you have a better understanding of what data you have and its value, secure it. Conduct security and data protection awareness training. Most employees are honest and loyal. You can maximize these attributes by providing training around security and privacy. Raise awareness in areas such as data security and dealing with suspicious activities. Lastly, involve employees in refining processes and plugging security gaps.

Some final thoughts

Data has real value to your organization. Don't become another data breach statistic. Be proactive. Know the what, where, why of your data. Keep in mind:

- It's hard to restrict access to something if it's not controlled
- The cost of prevention is less than the cost of remediation
- Data protection and privacy is a business not just an IT concern
- Adherence to policies, procedures, and regular monitoring is key
- Be flexible. Yesterday's threats will not necessarily be tomorrow's
- Data is an asset and it's value and risks should be known
- Only accept third party data that you really need
- Security and privacy is not a project with an endpoint. It is a continuing journey.
- Strong stakeholder and management buy-in is critical