



Basic Data Protection Strategies:

Top 5 Strategies to Protect Your Data – And Your Business

We lock our businesses, our homes and our cars to restrict wrongful entry and burglary. We invest heavily in security systems to deter and prevent loss. But how can we similarly protect intellectual property?

A recent *Trends in Proprietary Information Loss*, Survey Report sponsored by Pricewaterhouse Coopers, revealed that the U.S. Chamber of Commerce and the ASIS Foundation found that both Fortune 1,000 and small to mid-sized businesses were likely to experienced proprietary information and intellectual property losses ranging from \$53 and \$59 billion. These losses involved:

- R&D (49%)
- Customer lists and related data (36%)
- Financial data (27%)

How would your organization react, and what would it lose, given this type of exposure?

No company is 100 percent safe, whether storing information electronically or in paper file cabinets.

Data loss occurs every day through various channels including current and former employees, competitors and on-site contractors. But just as devastating, if not worse, are the uncontrollable effects of civil unrest and natural disaster like earthquake, flood and fire. While there's no way to stop the sharing of information in business, just as it's not feasible or realistic to lock physical doors and windows of your business establishment 24/7, there are measures you can take to minimize your risk.

Here are 5 ways to protect your data:

1. Assess Your Inventory and Risk

Conduct a comprehensive inventory of your business information. Catalog electronic data and identify type and purpose. Once cataloged, rate the risk of each based on its importance to the organization's ongoing operations.

For example:

- Is the information essential to mission-critical business functions (such as payroll, banking or legal documentation),
- Is the information required for business continuity but not detrimental should systems falter for a brief period of time (such as email), or deferrable should systems falter for an extended period of time (such as past employee or past customer archives)?
- Is the data sensitive or unrestricted?

Once a comprehensive inventory is in place along with risk-ratings for each category, management can quickly record and assess risk at file creation.

2. Implement New Policies

Implement new policies defining procedures for security breach, system failure or threat. This should include remediation and reporting strategies. All businesses should also have a confidentiality policy signed by all employees. This policy should outline employee responsibility, information use and disclosure practices.

3. Access Controls and Authorization

When dealing with sensitive information, have processes in place restricting physical and/or electronic access. This might include keyed or coded entry for paper or password restriction for electronic files or folders, firewalls and program encryption. Organizations should also require employees to use shredders when destroying confidential documents.

4. Ongoing Communication

Sharing information is a natural instinct among social groups and communities. This means, you should continually communicate with your employees, sub-contractors and consultants. You want to ensure all parties understand what information is confidential and what their responsibilities are in safeguarding its integrity.

5. Maintain a Clear Accountability Trail

With employees aware of their responsibilities, businesses should hold them accountable for confidentiality leaks and breaches caused by their actions. This means consistent disciplinary action for all individuals violating company policy.

Just as physical security is critical to protecting assets and inventory, businesses must make information security a high priority. Information security should include inventory, valuation, access controls, consistent communication and clear accountability trails. When organizations implement a comprehensive program using each of these five strategies, they're well on their way toward maximum data protection.

Using these basic strategies, you can protect your company and your data.

For further information go to www.tritoncomputercorp.com