


- 
- 10 things your company can do to increase your security right now!

Comprehensive suite of security & privacy solutions with the specific service offerings:

- Security & Privacy Assessments
- Security & Privacy Planning
- Security & Privacy Design & Implementation
- Cyber Security Institute
- Ongoing Security and Privacy Services



Security and Privacy

10 things EDS will do to ensure your Corporation's Security

- 1 Review your company's **business continuity plan** for adequacy and currency. Pay special attention to new IT systems and processes that might not have been included in the original plan. Consider testing all or part of the plan if this hasn't been done recently. Ask your critical vendors about their abilities to help in a crisis.
- 2 Check the procedures for making and storing **backups of critical data**, including personal computers. Backups should be taken frequently and stored outside the facility. Consider making several sets of backups and distributing them among several off-site locations. Make sure that the backups are useable by randomly choosing one or more sets and restoring the data. In too many instances, data thought to be safely backed up can't be accessed when needed
- 3 Make sure your **facility physical security** plans are up to date, including instructions for contacting local fire, police, and rescue authorities. Does your security force have a written procedures manual and follow it? Have they been tested recently? Do they know when to call in local authorities and who has the authority to decide to do so? How (and how well) do you control visitors and vendors in your facilities?
- 4 Review your **IT security policies and procedures** for completeness and currency. Do your security procedures reflect what you really expect your employees to do? Are they up-to-date regarding your IT environment? Pay special attention to intrusion detection systems (IDS), passwords, anti-virus and incident response procedures, and network monitoring for early indications of issues
- 5 Review your **human resources procedures** for potential weaknesses. Consider the adequacy of your background checking processes for new hires, vendors, etc. Do you have an adequate way to communicate with your employees in an emergency? Are your employees "security aware"? If trouble looms, consider distributing key workforce, vendors, facilities, and processes as much as possible. Insure that a failure or crisis in one location is contained to that location if possible, and has minimal impact on the business as a whole. This will help avoid the "domino effect" where a crisis in one location quickly spreads to engulf an entire company.
- 6 Ask your **critical vendors** about their plans and capabilities to deal with emergencies. If you rely on one or more critical vendors to keep your business going, a crisis that effects them could spill over to you if they are unable to provide you service.
- 7 Do you have **executive protection plans** in place for key executives? Are all members of your key staff aware of how and when this plan will be put into effect?
- 8 Review your **insurance coverage**, including property and casualty, "key man" insurance, cyber risk insurance.
- 9 Look for **all types of threats** to your business, your employees, or your market. Recent events have made us think of terrorism as a major threat, but don't forget other diverse threats, such as: employee or non-employee workplace violence, labor actions or disputes, public occurrences (like a meeting where violent protests are likely), cyber threats (including computer viruses and denial of service attacks), hoaxes, and industrial espionage
- 10 Revisit **budgets** for Business Continuity Planning and IT Security to insure their adequacy. Often security budgets are among the first casualties in a budget crunch. As we have seen in the past two weeks, this is often a "penny-wise and pound foolish" approach. Proper planning for IT disasters can repay it's cost many times over when the crisis actually hits. Poor or nonexistent planning can ultimately cost much more in lost business, destroyed or damaged information or physical resources, and personnel disruption.