

We've all read the stories and seen the headlines about security breaches such as: Cyber attacks on Estonia's government—claims Estonia makes were launched by Russia or Russian sources—almost shut down the government.

- **Monster.com** breach, where 1.3 million job seekers' personal information was stolen.
- The international cyber crime landscape is rapidly evolving and the United States is the number one target. According to the most recent Symantec Internet Security Threat Report, the United States experienced 30% of all malicious cyber activity in the first half of 2007, more than any other country.

What are the potential costs to business worldwide and to the United States?

- The World Economic Forum estimates a 10-20% probability of a breakdown of the critical infrastructure in the next 10 years. Additionally, it estimates the global economic cost of approximately \$150 billion.
- Research conducted for the Business Roundtable by Keybridge Associates suggests that the economic costs to the United States for a month-long Internet disruption would be more than \$200 billion.

What must business and government consider if the Internet is disrupted?

- When the Internet is unreliable for an extended period, companies are likely to turn to conventional methods of communication and processing such as mail delivery, telecommunications, office supply and shipping, which puts an enormous amount of stress on these industries.
- Success in mitigating the economic impact of a disruption will largely depend on the management of the surge in demand and industries sufficiently scaling up operations using spare capacity, temporary labor, etc.
- Early warning by government of a major threat or growing attack against the Internet might help minimize the damage to company IT systems and to business operations dependent on the Internet.
- The U.S. Computer Emergency Readiness Team (US-CERT) portal can be a good source of information when a cyber attack has regional or national impact.

Where can technology be helpful, and how does EDS address these problems? In a recent speech at SMU EDS CEO Ron Rittenmeyer said:

- Some organizations use security audits and invest in security training in effective password policies and advanced systems architecture.
- Practicing good physical security, such as locking doors... locking up laptops, and CDs is also included, as 70% of data breaches according to the Ponemon Institute result from the loss of off-network equipment such as a laptop.
- Encryption...remote data wiping...and new "data leakage" technologies must be used to augment and support good security policies.
- Advanced content scanning and analysis of a company's outgoing data can help detect the leakage of sensitive or classified information.
- Older tools that EDS has used for years—such as anti-virus and firewall technologies—are "table stakes" for security.
- The use of systematic and routine software updates and patches can pay huge dividends in preventing security incidents.
- Using "zero touch" technology that EDS jointly developed with Microsoft, allows EDS to deploy system upgrades to secure an enterprise up to five times faster—and with less risk.
- EDS supports developing national standards around data security and the legislation introduced by Rep. Tom Davis (R-Va) and Senator Norm Coleman (R-Mn) on government data security breaches.