DATA LOSS: A Pivotal IT Security Risk

Sending an email to the wrong recipient, or attaching the wrong file, are common mistakes that we all have done at some point. For organizations, the prevalence of email for mass communication, combined with high-speed computing and data networks, Web 2.0 applications and mobile computing have made the risk of data loss considerably high in modern-day business environments.

Some numbers on data loss

- 20% Of outbound e-mail that contains content which poses a legal, financial or regulatory risk.
- $7.2M Average cost of a data breach in 2011.
- 650% Estimated enterprise data growth in the next five years.
- 77% of organizations have experienced data loss in the last year, with the majority of data loss incidents based on unintentional errors.

Top three sources of data loss across organizations and enterprises

1. USBs and laptops
2. Corporate email
3. Public webmail

Biggest IT Security Challenges

- Managing the complexity of security (51%)
- Enforcing security policies (35%)
- Preventing data breaches from outside attackers (29%)
- Preventing data theft by employees or other insiders (23%)

Best practices to prevent a breach:

1. Understand the organization’s data security needs
   - Have a clear view and record of the types of sensitive data that exist within the organization, as well as which types of data are subject to government or industry – related compliance standards.

2. Classify sensitive data
   - Begin by creating a list of sensitive data types in the organization and designating the level of sensitivity.

3. Align security policies with business needs
   - An organization’s security strategy should protect the company’s information assets, without inhibiting the end user. Start by defining company policies in simple business terms that are aligned with individual employee, group or organization’s business needs.

4. Secure data throughout its lifecycle
   - Businesses should consider implementing data security solutions that secure their sensitive data in multiple forms – correlating users, data types and processes – and protect it throughout its lifecycle: data-at-rest, data-in-motion, and data-in-use.

5. Eliminate the compliance burden
   - Evaluate government and industry-driven compliance mandates and how they impact an organization’s security and business flow.

6. Emphasize user awareness and engagement
   - Involve the user in the security decision process. Technology can help educate users about corporate policies and empower them to remediate security incidents in real-time.

Data Loss Prevention is like a neighborhood watch program — you need to be able to rely on your employees to become the first line of defense. People, along with good security policy and enforcement, can ensure that security is practical, smarter and more effective.