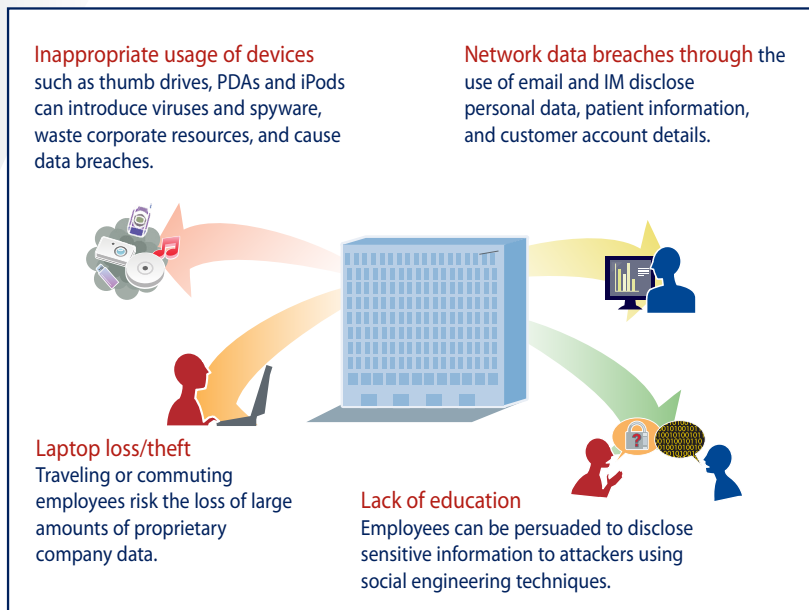


## ASSESSING DATA RISKS

Achieving data lifecycle security requires a complete understanding of data-in-motion, data-at-rest and data-in-use.

Employees and other trusted entities store sensitive information not only on corporate servers and file shares, but on laptops, thumb drives, external hard drives, and smartphones. They transmit sensitive data via corporate email, webmail, social networking applications, instant messaging, and more.



Knowing where your data is stored, how it's transmitted, and what your trusted insiders are doing is the first step towards data lifecycle security.

**\$6.75 Million**  
*Average cost of a data breach<sup>1</sup>*

**222 Million**  
*Number of records exposed in 2009<sup>2</sup>*

**87%**  
*Number of attacks considered avoidable through simple controls<sup>3</sup>*

**498**  
*Number of reported data breaches in 2009<sup>2</sup>*

**1**  
*Number of data breaches that can ruin your company's reputation*

<sup>1</sup>Ponemon Institute's "Fifth Annual U.S. Cost Of A Data Breach Study," 2009

<sup>2</sup>ITRC Breach Report 2009

<sup>3</sup>2009 Verizon Business Data Breach Report



## DATA RISK ASSESSMENT

infoLock Technologies' comprehensive Data Risk Assessment identifies real-world risks to your business data. Our service includes:

- **EXTRACTION POINT ANALYSIS**  
careful assessments of data, network, and endpoint-level activity through network monitoring strategies and automated tools
- **DATA MAPPING**  
analysis of data-at-rest and data-in-motion. Where does data reside (servers, laptops, removable storage devices, etc) and is it secure?
- **ACCESS CONTROL REVIEW**  
who can access data, and do they require this access to perform their job function?
- **DATA LEAKAGE**  
is sensitive data leaving the organization unencrypted?
- **IT POLICY REVIEW**  
assessment of existing policies and employee awareness of these policies, and the need for updates based on current regulatory mandates
- **HUMAN RESOURCES POLICY REVIEW**  
examine and improve policies to help identify, monitor, and potentially remove problematic insiders
- **PERSONNEL INTERVIEWS**  
understand the security posture from the perspective of front line managers and staff
- **SOCIAL ENGINEERING/ PENETRATION TESTING**  
assess the efficacy of existing security awareness training and identify

## CREATING THE SOLUTION

The Data Risk Assessment concludes with a comprehensive report detailing the results, and an executive level presentation to discuss appropriate remediation strategies. Whether this strategy requires security awareness training, infrastructure reconfiguration, or third party solutions, you can take comfort in knowing that you have made the right choice to improve your security posture, and you will achieve your expected Return on Security Investment.



infoLock  
TECHNOLOGIES