RSA Conference 2013 Symantec Show Floor Survey
Key Findings

Key Findings

At the RSA Conference 2013, Symantec conducted a data access and mobility survey of 275 attendees. These were professionals who are involved in the planning, management, oversight or implementation of information security in their organizations. The survey reveals that the increased use of mobile devices is making the insider threat more relevant than ever before. Key findings are outlined below:

IT sees the benefits of mobility outweigh the risks. Companies making the move to mobility are seeing increased productivity and other benefits. When asked to compare the benefits and risks of mobility, 48% of IT respondents say that mobility benefits are more than the risks and challenges, while just 25% say the benefits are less.

- Top three motivators for move to mobility
  - Business drivers (63%)
  - User demand (59%)
  - Financial savings (49%)
- Top risks for employee owned devices
  - Data leakage, i.e., data taken out of company by employees via mobile (79%)
  - Theft or accidental loss of valuable or sensitive information (77%)
  - Preventing unauthorized network or applications access from mobile (76%)
  - Malware infection that spreads to internal computing devices (73%)
  - Lost or stolen devices (70%)
  - Compliance violations leading to fines or sanctions (65%)

IT is very aware of the insider threat. Although 76% of businesses saw cyberattacks in the past year, the increased use of mobile devices highlights the need to protect against possible insider threats. IT has a high awareness of employees transferring work documents outside the business:

- 62% of employees say they believe it is okay to transfer work to personal devices or Internet file-sharing services.*
- 63% of IT respondents agree that employees think it is okay to transfer work to personal devices or Internet file-sharing services.

IT and employees are at odds over consequences for violating policy. There is a disconnect when it comes to the consequences of taking sensitive information against policy. IT believes they enforce policies more often than employees perceive policies are enforced. Either way, IT trusts that employees are cautious in their use of data.

Confidence in a connected world. Symantec™

RSA Conference 2013 Symantec Show Floor Survey
Key Findings

Key Findings continued

- 47% of employees say their organization takes action when employees remove sensitive information that is against policy.*
- 74% of IT respondents say their organization takes action when employees remove sensitive information that is against policy.
- 60% of IT respondents say that most employees in their organization are cautious in the use and handling of sensitive or confidential information.
- 43% of employees say they are cautious in their use and handling of sensitive or confidential information.*

IT doesn't have a clear grasp on employee attitudes that justify taking corporate data. Responses of employees and IT differ when asked why employees think it is acceptable to move work documents to personal devices and cloud services:

Reason	Employee Responses*	IT Responses
Sharing the business information does not negatively impact or harm the company	53%	22%
Company policy is not strictly enforced	51%	33%
Business information is generally available and not secured	44%	17%
Employee who shares this information does not receive any economic gain	38%	19%
Business information was authored or co-authored by the employee	30%	28%
Computer or device retaining the information is secure	30%	24%

*What's Yours Is Mine: How Employees are Putting Your Intellectual Property at Risk, Symantec in partnership with the Ponemon Institute, February 2013

Confidence in a connected world. Symantec™

RSA Conference 2013 Symantec Show Floor Survey
Key Findings

Recommendations

The survey results illustrate how inudstry trends such as mobility and insider threats are motivating businesses to focus more on security. The following guidelines can help organizations reduce risks:

- **Being cautious about mobility is okay; being resistant is not. Start embracing it.** Organizations should take a proactive approach and carefully plan an effective mobile implementation strategy.
- **Understand that all data is not equal.** For organizations looking for a safe route across the minefield that is the future of IT, understanding data, its importance and risks is a good place to start.
- **Implement policies restricting how employees can access and share sensitive data.** Developing and maintaining simple policies can be a powerful step to safeguarding corporate data. Make sure employees are aware that policy violations will be enforced and that theft of company information will have negative consequences to them and their future employer.
- **Educate employees.** Organizations need to let their employees know that taking confidential information is wrong. IP theft awareness should be integral to security awareness training. By maintaining oversight, you can ensure employees know how and when to use mobile devices and cloud services efficiently and securely.
- **Implement monitoring technology.** Support education and policy initiatives by using monitoring technology to gain insight into what IP is leaving your organization and how to prevent it from escaping your network. Deploy data loss prevention software to automatically notify managers and employees in real time when sensitive information is inappropriately sent, copied or otherwise inappropriately exposed. This helps increase security awareness and deters theft.

Confidence in a connected world. Symantec™