The Human Factor in Data Protection

Executive Summary

Sponsored by Trend Micro

Independently conducted by Ponemon Institute LLC

Publication Date: January 2012
The Human Factor in Data Protection
Executive Summary
Ponemon Institute, January 2012

Ponemon Institute is pleased to present the results of The Human Factor in Data Protection: Executive Summary. Sponsored by Trend Micro, this research focuses on how employees and other insiders can put sensitive and confidential information at risk and what organizations are doing to reduce this risk. We believe the threats posed by insiders are becoming more prevalent because of the mobility of the workforce, proliferation of mobile data-bearing devices, consumerization of IT and use of social media in the workplace.

The study surveyed 709 IT and IT security practitioners (hereafter referred to as IT practitioners) in the United States. On average, respondents have more than 10 years of relevant experience. Only IT practitioners who have some level of responsibility for data protection in the organization participated in this study. Forty-five percent of respondents are at the manager level or higher in the organization. Seventy-eight percent are in organizations with a headcount between 100 and 5,000.

According to 78 percent of respondents, their organizations have experienced a data breach as a result of negligent or malicious employees or other insiders. Employees losing laptops or other mobile devices, mishandling of data at rest and in motion and malicious employees or other insiders are the root causes of many of these data breaches in organizations. To manage the human factor risk, organizations are turning to such enabling technologies as access governance, endpoint security management, SIEM and security intelligence among others.

Unfortunately, it seems that even when employees make unintentional mistakes most of these breaches are only discovered accidentally. Rarely do employees self-report the incident. While technologies are important in data protection, so is it critical for organizations to reduce the risk of employee negligence or maliciousness through policies, training, monitoring and enforcement.

The following are 10 risky practices employees routinely engage in, according to the findings of the study:

1. Connecting computers to the Internet through an insecure wireless network.
2. Not deleting information on their computer when no longer necessary.
3. Sharing passwords with others.
4. Reusing the same password and username on different websites.
5. Using generic USB drives not encrypted or safeguarded by other means.
6. Leaving computers unattended when outside the workplace.
7. Losing a USB drive possibly containing confidential data and not immediately notifying their organization.
8. Working on a laptop when traveling and not using a privacy screen.
9. Carrying unnecessary sensitive information on a laptop when traveling.
10. Using personally owned mobile devices that connect to their organization’s network.

The next section reports the key findings of our independently conducted survey research. The results provide guidance on how organizations can best address the human factor in data protection and reduce the likelihood of a data breach.
Key findings

**Employee negligence or maliciousness is the root cause of many data breaches.** Over 78 percent of respondents say negligent or malicious employees or other insiders have been responsible for at least one data breach within their organizations over the past two years. Most respondents say their organization’s sensitive or confidential business information is protected fully (24 percent) or partially (43 percent) by data protection technologies such as encryption and data loss prevention (DLP).

The top three root causes of these breaches are employees’ loss of a laptop or other mobile data-bearing devices, third party mishaps or flubs and system glitches. Despite growing concerns about cyber crime, only 8 percent report an external attack as the primary root cause of a data breach experienced by their organizations.

**Detection of data breaches is often accidental.** If employees are reluctant to self-report a data breach, organizations need better technologies to know when a breach has occurred so that an incident response plan can be quickly put in motion. Detection or discovery of these data breaches is most often accidental, according to 56 percent of respondents. Unfortunately, only 19 percent of respondents say that employees self-reported the data breach making it difficult to promptly resolve the breach. Thirty-seven percent say that an audit or assessment revealed the incident and 36 percent say that data protection technologies revealed the breach.

**Certain data security technologies and governance practices are considered very important in preventing a data breach.** Access governance, endpoint security management, security intelligence, encryption of data at rest and data loss prevention are the top security technologies considered most important in reducing data loss or theft.

The governance practices that are most important are: establishing a data protection team, obtaining sufficient resources for implementing data protection activities and appointing a leader in-charge of data protection across the entire organization.

**To address the human factor in data protection, specific security and governance procedures are preferred.** The most important security measure is to manage and monitor end-user privileges and entitlements followed by criminal background checks before granting privileged access and the consistent application of security governance practices.

**IT practitioners’ perceptions about security activities, infrastructure, priorities and strategies provide insight into the vulnerabilities organizations must address.** The majority of respondents (67 percent) believe that their organizations’ security activities are not enough to stop a targeted attack (or Advanced Persistent Threat) or a hacker. Sixty percent of respondents do not agree that their organizations’ data security activities thoroughly protect information assets from negligent or malicious insiders.

With respect to the security infrastructure, 64 percent of respondents agree that their organization needs to re-architect their security infrastructure because someone (hacker or malicious insider) is trying to steal data and 62 percent say the infrastructure needs to focus on data-centric (inside-out) security with sensitive or confidential data being the main element.

A high data protection priority in organizations is data intelligence that identifies the “who, what, when and how” data is accessed. Another priority is not to trust anyone internally and definitely not anyone externally. Further, security strategies cannot be viewed as a hindrance to business operations and practices, according to 81 percent of respondents. Strategies also need to focus on consumerization of IT and insecure mobile devices accessing corporate applications and data assets.
Employees’ lack of attention to data protection combined with an increase in sensitive data on mobile devices is putting sensitive and confidential information at risk. Employees very frequently (19 percent) or frequently (37 percent) store sensitive data on their laptops, smartphones, tablets and other mobile devices.

Employees are often in non-compliance with organizations’ data protection policies. While respondents cite the majority of employees do not turn off or disengage security settings and understand and proactively comply with their organization’s data protection policy, other risky behaviors are proving to be barriers to safeguarding data in the workplace. As mentioned in the introduction, there are risky behaviors that can lead to the loss or theft of sensitive and confidential information. Specifically, it is rare for employees to notify their organization after losing a USB drive containing data. It is also rare for employees to shred paper documents containing confidential or sensitive information.

Conclusion

Based on the findings, it is recommended that organizations take the following steps:

- Create awareness among employees and other insiders about the need to spend more time and effort on data protection activities.
- Ensure data protection policies address areas where an organization is most vulnerable to a data breach.
- Investigate governance and technology solutions that are both efficient and cost effective.
- Make sure those who are given privileged user status are knowledgeable about the risks.
- Require immediate notification if a mobile device containing sensitive and confidential information is lost or stolen.
- Create policies for the use of social media in the workplace.

The human factor risk, from both internal and external sources, poses a very real threat to an organization’s sensitive and confidential information. The risk of data breach, as shown in this study, is especially great due to employees’ loss of a laptop or other mobile data-bearing devices. Given the potential for a costly data breach and loss of reputation due to the exposure of confidential information, we believe it is critical for companies to expand the focus of their data security initiatives to ensuring employees and other insiders understand the importance of data protection.

Ponemon Institute

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

As a member of the Council of American Survey Research Organizations (CASRO), we uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.