InsideCounsel

Technology: We have met the enemy, and he is us

The cause of lost data is usually internal

BY JOHN COWLING, DANIEL NELSON
October 12, 2012 • Reprints

In a prior column, we discussed the inevitability of technology-related accidents occurring at virtually every company. One particularly common mishap is the loss of customer, client or employee data. These data breaches may present a substantial problem for organizations, as the number of discrete records lost often runs into the hundreds, thousands or millions. Even if there is no evidence of actual misuse of the lost data, the costs to provide legally required notice, together with the potential cost of mitigation efforts such as providing credit monitoring, quickly mount. If the breach is sufficiently serious to interest regulators such as the Federal Trade Commission or a state's attorney general, then costs associated with investigation, defense and, potentially, future mandatory compliance and fines further add to the data loss burden.

Many people think of data loss as the work of hackers, offshore data thieves and other external threats. But, as Pogo once said, "We have met the enemy, and he is us." The vast majority of data loss events are an inadvertent, or sometimes intentional, "inside job." If your organization experiences data loss, it will most likely be an employee, not an external actor, who caused the loss.

In a recent Forrester Research survey, respondents cited external attacks as the causal event in only 25 percent of data loss cases. Other causes, such as employee loss of data, employee misuse of data or malicious insider activity combined to pose a far greater threat to organizations' information assets. We recently provided counsel with respect to data losses arising from a laptop stolen from an employee's car, and a professional data thief who moved from company to company as a human resources employee, stealing employee personal information at each stop. Regulatory authorities pursue

enforcement actions arising from, for example, data losses arising out of the theft of an employee's briefcase, and employees ignoring company disposal rules for sensitive data.

Focusing on several key elements of a company's data flow and storage can mitigate this internal threat. Start by asking questions regarding employee access, transmission and storage/disposal of company-held data.

Key access questions include:

- In what ways can employees access data?
- What security measures are in place to guarantee only authorized access?
- Is access allowed to persons beyond those who reasonably need it?
- What measures are in place to log employee access?
- Is access limited to on-site means, or can employees remotely access data?
- What gateways to sensitive data are available via smartphone or other mobile device?

Key transmission questions include:

- What data is validly being carried outside the organization's "four walls"?
- What methods to carry or transmit data are available to employees (including USB access, third-party email accounts and data stored locally on laptops)?
- Is unencrypted data being transmitted?
- What vendors receive company data, and how is the data transmitted to those vendors?
- What systems and procedures are in place, if any, to log data being moved?

Finally, storage/disposal questions include:

- Where is company data stored? Does the company control these storage assets, or does it rely on third parties?
- Is internally stored sensitive data encrypted?
- Is sensitive data being held for period longer than necessary?
- What policies and procedures are in place to ensure secure disposal of data? Is there any audit or follow-up to ensure adherence?

A sound data security strategy must account for the threat of internally generated data loss events. Key components of the strategy should include appropriate policies, training, appropriate technology and auditing. An organization's policies should include ones on allowable access to sensitive data, allowable transmission of data, and appropriate retention and disposal of data. Hiring policies should include provisions, perhaps as simple as required reference checks, for employees whose jobs allows for access to sensitive information. Employee training should cover the company's data security and retention/disposal policies, as well as information to emphasize the potentially disastrous consequences of inappropriate data practices. The company's information technology team should engage in questions of internal data security. Finally, companies should implement procedures to chronicle access and transmission of data, and routinely check for data-policy compliance.

About the Author

John Cowling

John F. Cowling *is an attorney in the St. Louis, Missouri office of Armstrong Teasdale. He practices primarily in the areas of commercial litigation, environmental litigation and information technology law. He has employed computers and litigation technology in his practice for many years. Additionally, he is the President of Lawgical Choice, an Armstrong Teasdale subsidiary, that provides legal technology services to law firms and legal departments.*

About the Author

Daniel Nelson

Daniel C. Nelson *is a partner in the St. Louis Missouri office of Armstrong Teasdale. He works primarily in the area of commercial litigation, with a particular emphasis on contract, real estate, sale of goods, securities and internal governance issues. He is the leader of the firm's Real Estate Litigation and Electronic Discovery practices.*