

Research Concepts Survey: IT Departments and Data Breach Prevention

Revealing current attitudes, data protection strategies and their effectiveness



A new survey of 185 IT professionals indicates that while data breach prevention is a top priority, current data protection strategies are consistently undermined by employees.

Table of Contents

- Executive Summary..... 2
- Data Breach Legislation 3
- Major Findings
 - Data Breach Prevention is a Top Priority 4
 - Data Breach is Both Common and Costly 5
 - Prevention Measures Are Consistently Undermined by Employees 6
- Recommendations: Take a Multilayered Approach to Data Security..... 7
- Endpoint Security from Absolute Software 8
- More Information..... 9

Survey Respondents

Survey respondents were primarily in IT management or executive leadership positions at organizations with an average of 5,806 employees. More than 80% of respondents were in a position to determine technology solutions purchased and 35% were responsible for their organization's overall security budget. All respondents were recruited from Network World's Technology Opinion Panel via an email invitation. For more information on Research Concepts Market Research, please visit: www.research-concepts.com.

As the amount of information stored digitally on company servers, stationary computers and mobile devices such as laptops continues to escalate, protecting that information from public data breach is becoming a priority for IT and compliance departments.

In September 2007, market research firm Research Concepts surveyed 185 IT professionals from Network World Magazine's Technology Opinion Panel about the state of computer and data security in their organizations. The survey probed attitudes toward the prevention of data breach, current prevention measures employed by IT departments and the perceived effectiveness of those methods.

Regulatory Compliance

State-level data breach notification legislation has fueled a shift in the way organizations view the security of sensitive information such as customer social security numbers, electronically protected health data, and other personally identifying information. No corporate department is more closely tied to the protection of this data than IT. For example, the theft of laptop computers managed by IT is responsible for nearly 50% of all data breaches.*

Major Findings:

- **Data breach prevention is a top priority:** More than 80% of those surveyed rated protecting corporate data as an important initiative. By comparison, only 38% of those surveyed ranked complying with governmental regulations as very important.
- **Data breach is common and costly:** Fully 25% of those surveyed indicated that their organization had experienced a data breach in the past and more than 60% of IT managers felt that a data breach would cost their organization in excess of \$10,000. Nearly 65% were very concerned that a data breach would result in public embarrassment and media scrutiny for their organization.
- **Preventative measures are consistently undermined by employees:** According to IT professionals surveyed, less than one in 100 employees consistently follow company data and computer security policy. More worrying is the fact that 72% of respondents felt that employees were responsible for the majority of data breaches.

Survey respondents reported the use of a wide-array of data protection strategies and technologies that are highly-dependent on diligent employee action to remain effective. Only endpoint security – the ability to force devices carrying sensitive data to secure themselves – provides data breach protection that does not rely on employees for effectiveness.

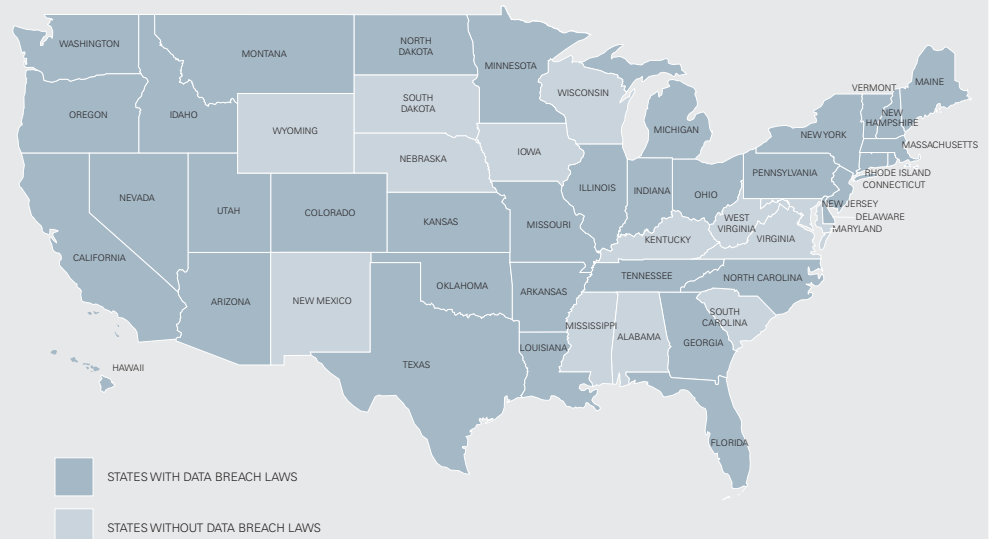
In the four years since California Senate Bill 1386 became the first state-level legislation to specifically require data breach notification, 36 additional states have followed California's lead and enacted similar legislation. While state data breach laws vary in terms of fines and notification requirements, the average cost of managing a data breach has risen in recent years and is now estimated at US\$197 per breached record. Typical costs include credit protection for those affected, increased marketing costs resulting from attempts to recover lost customers and the legal and public relations costs of managing the breach itself.

$$\# \text{ of records} \times \$197 = \text{Cost of Breach}$$

Calculating the costs of data breach:

A recent Ponemon Institute report estimates that a breach costs a company \$197 per missing record.* In many breach situations, the number of records affected is in the hundreds of thousands, with the most extreme case involving 27 million current and former U.S. military personnel. In such cases, the cost to manage the breach can reach into the tens of millions – providing strong motivation for organizations to protect their data and themselves.

37 US states have data breach legislation



81% of IT professionals surveyed said that protecting corporate data from breach was their top security concern.

Laptop theft linked to data breaches

Survey respondents also appear to see a direct correlation between laptop theft and the possibility of data breach. In the event of a laptop theft, more than 75% of respondents said they were very concerned about the possibility that confidential information would be exposed and potentially misused. A further 60% were very concerned that the theft of a laptop computer would result in identity theft and nearly 25% said they would be willing to pay between \$10,000 and \$50,000 to have a stolen executive's laptop returned to their organization.

Despite the widely-acknowledged link between laptop theft and nearly 50% of data breaches, survey respondents reported that a surprising number of mobile computers continue to go missing. Nearly one quarter of those surveyed reported that between 3% and 10% of their entire laptop population was lost or stolen each year. Incredibly, 60% of survey respondents said that they were unable to recover a single stolen computer – meaning those computers remained in the hands of thieves.

Thieves with keys: employees steal laptops

The fact that the majority of lost or stolen laptop computers are never recovered is made more concerning by the likelihood that thieves have the necessary passwords and encryption keys to access confidential information. Nearly 40% of IT professionals surveyed believe that their own employees – those with intimate access to login credentials and other passwords – are responsible for most cases of computer theft. So, while 94% of survey respondents password-protect company computers and more than 50% protect sensitive information with encryption technology, confidential information can still be accessed in an alarming number of laptop theft cases.

One quarter of organizations surveyed have experienced a data breach

Survey respondents indicated that data breaches are astonishingly common. A full one quarter of IT professionals surveyed said that their organization had experienced a data breach in the past. Perhaps more concerning is the fact that more than 30% of respondents felt that data breaches have occurred yet their organization is unaware of them.

What information is breached?

Survey respondents reported a wide-variety of information involved in data breaches. Data breached included social security numbers (16%), credit card numbers (4%), intellectual property (18%), customer information (20%) and employee information (20%).

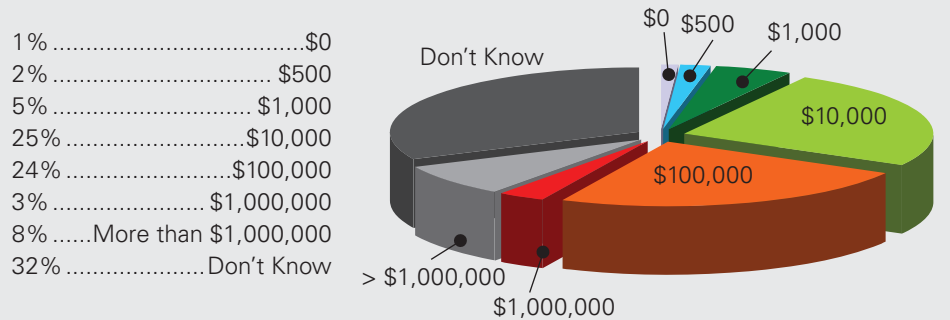
The increasing incidence of computer theft could be contributing to this sentiment. More than 30% of respondents believed that computers had been stolen from their organization without the company’s knowledge – pointing to the difficulty organizations have accurately inventorying their computers.

IT professionals believe data breaches are costly

When asked what impact a significant data breach would have on their organization, IT professionals surveyed were most concerned with their organization’s public reputation and potential loss of credibility. More than 80% of respondents felt that a data breach would have a negative impact on their company’s reputation. Respondents also expected an impact on the bottom line, with 41% expecting a loss of customers and 51% indicating that they would expect to lose revenues in the event of a breach. A further 48% anticipated fines or monetary penalties in the event of a breach.

Figure 1.1 The Hard Costs of Data Breach

35% of IT professionals surveyed believe a data breach will cost their organization over \$100,000. 11% believe it would cost \$1 million or more.



One in 100 employees consistently follows corporate policy

Perhaps the most startling revelation is that IT professionals believe only one in 100 employees consistently follow corporate policies regarding data and computer security. More than 55% of these IT professionals reported reliance on corporate policies for the use of mobile computers and accessing sensitive files. Unwillingness to consistently follow corporate policy has far-reaching implications for all data breach prevention measures that rely on the diligence of employees for effectiveness. Encryption software, for example, has long been thought of as the most effective means of safeguarding sensitive information. However, encryption technology is highly-dependent on end users to provide effective protection.

Employees and contractors responsible for most incidents of data breach

More than 40% of IT professionals surveyed said that they currently have computer asset tracking and theft recovery software installed on their computers and 31% of those surveyed plan to provide this protection for additional computers in their population in the next 12 months.

IT professionals surveyed were equally grim when asked who they believe commits the most incidents of data breaches within their organizations. More than 70% reported that their own employees – those responsible for correctly encrypting data, safely locking laptop computers and regularly changing authentication passwords on their computers – were responsible for most incidents. Nearly 20% indicated that they felt non-employees with access to sensitive information committed the most incidents of data breach in their organization. Non-employees such as temporary contractors pose a significant challenge for IT managers, because they often are not required to comply with company policy and they often are authorized to access and digitally store sensitive information. Contractors are also much more likely to work on third-party computers – that are not protected by corporate data security solutions like encryption software.

It is no surprise then, that IT professionals are seeking endpoint security solutions that provide protection for sensitive information regardless of employee action. More than 40% of IT professionals surveyed said that they currently have computer asset tracking and theft recovery software installed on their computers and 31% of those surveyed plan to provide this protection for additional computers in their population in the next 12 months. The majority of those surveyed also indicated that they would be interested in an endpoint security solution that would help recover their PDA or Smartphone in the event that it was lost or stolen.

Clearly, insiders such as employees and contractors with access to confidential information, the necessary passwords and encryption keys represent a glaring hole in security policies that rely heavily on encryption alone.

Single-point security solutions cannot adequately protect organizations from all points of possible data breach. Instead, a multifaceted or layered approach to computer security and data protection is required, comprised of “CPR”: Compliance, Protection and Recovery:

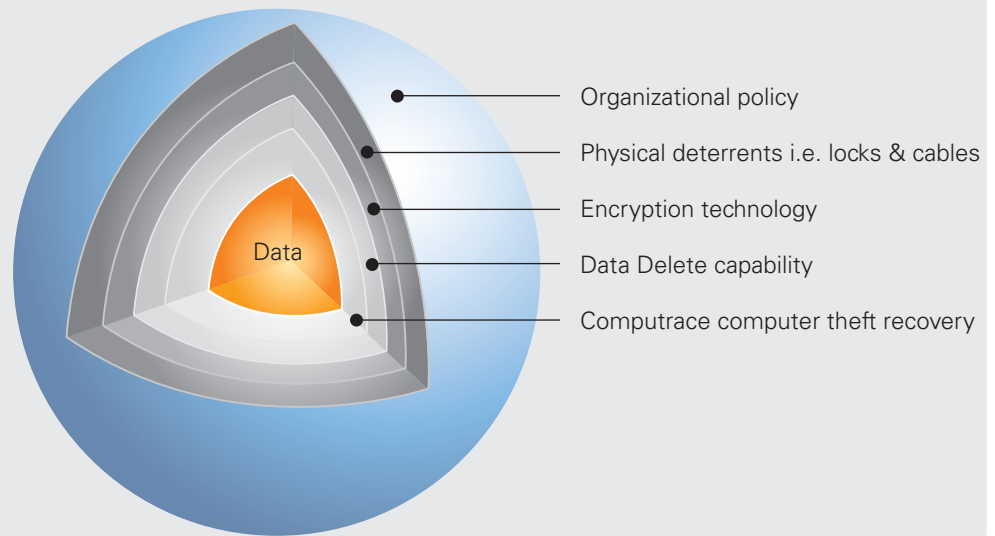
Compliance – Complying with all applicable mobile data protection regulations, with an easily accessible audit trail.

Protection – Protecting data on mobile computers includes encryption, strong authentication and the ability to remotely delete sensitive data on stolen devices.

Recovery – Recovering lost or stolen devices returns them to the control of the organization and facilitates prosecution.

By adopting the multilayered approach to computer security, organizations can minimize the risks to confidential information resulting from lost or missing computers. Together, documented security policies, physical theft prevention, accurate IT asset tracking, encryption, remote data delete and theft recovery capabilities provide the highest level of protection available to organizations concerned about data security.

A Layered Approach to Computer Security



Computrace endpoint security from Absolute Software forms an ideal platform for supporting a multilayered approach to protecting mobile computers and the sensitive information they contain. Pre-embedded in the BIOS¹ of computers from the world's leading computer manufacturers during the manufacturing process, Computrace is centrally managed by IT and requires no end user action to be effective.

Accurately Inventorying Computers – By logging into the Online Monitoring Center, IT personnel can create near real time reports on the computers in their inventory, their configuration, current user and location – whether they are connected to the local area network or in the field

Recovery – Using Computrace, the Absolute Theft Recovery Team can track missing computers and work with local law enforcement to recover the computer backed by a \$1,000 recovery guarantee.²

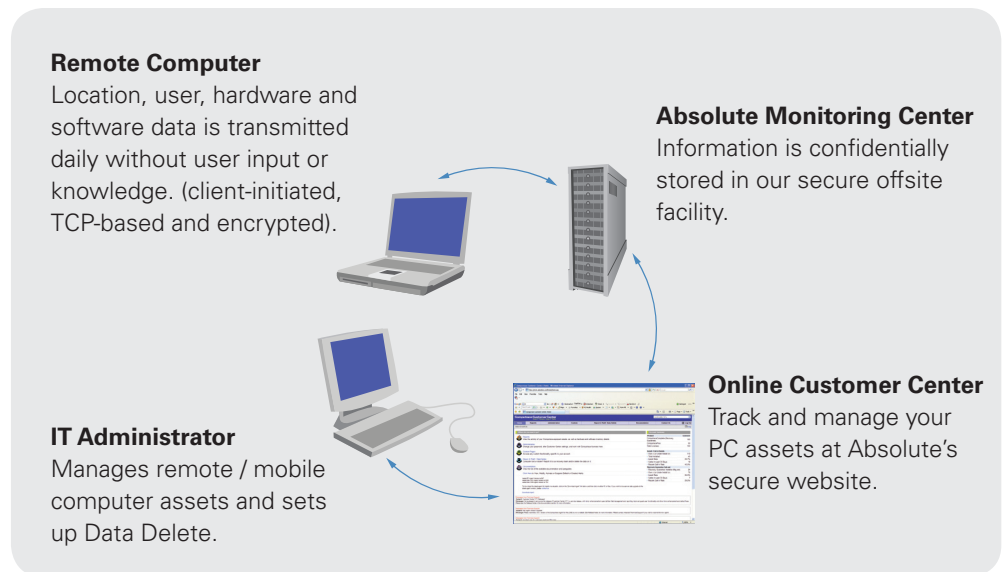
Emergency Data Delete – Computrace allows IT professionals to remotely delete sensitive data from missing laptops. Organizations can then assess whether they are required to publicly announce a data breach.³

Policy Enforcement – Computrace can detect unauthorized software installations, missing hardware and can report on software installed – allowing IT departments to ensure that key programs, such as antivirus, are current.

Lifecycle Management – In addition to remotely deleting health information in emergency situations, Computrace can be set to automatically delete data from computers at lease end or at a pre-determined retirement date.

How Computrace Works

When a computer protected by Computrace is reported stolen, the embedded Computrace agent sends a silent signal to Absolute's Monitoring Center providing critical location information. Absolute then works with local law enforcement to recover the computer backed by a \$1,000 recovery guarantee. The stealthy Computrace software agent can survive accidental or deliberate attempts at removal or disablement. With embedded support in the BIOS of a computer, the Computrace agent is capable of surviving operating system re-installations, as well as hard-drive reformat, replacements and re-imaging.



For more information on Compliance, Protection and Recovery, and the software tools used in a layered approach to computer security, contact Absolute Software today.

Absolute Software
Suite 1600, Four Bentall Centre
Vancouver, BC, Canada
V7X 1K8

Tel: 604 730 9851
Toll-free: 1 800 220 0733 (US & Canada)
Fax: 604 730 2621

About Absolute Software

Absolute Software Corporation (TSX: ABT) is the leader in Computer Theft Recovery, Data Protection and Secure Asset Tracking™ solutions. Absolute Software provides organizations and consumers with solutions in the areas of regulatory compliance, data protection and theft recovery. The Company's Computrace® software is embedded in the BIOS of computers by global leaders, including Dell, Fujitsu, Gateway, HP, Lenovo, Motion, Panasonic and Toshiba, and the Company has reselling partnerships with these OEMs and others, including Apple. For more information about Absolute Software and Computrace, visit www.absolute.com or <http://blog.absolute.com>.

Appendix A - Additional Resources

Complete survey results available at: www.absolute.com/img/NWW-survey.ppt

* "2007 Annual Study: US Average Cost of a Data Breach," November, 2007, Ponemon Institute, LLC

- ¹ For a complete list of BIOS-supported computers visit www.absolute.com/BIOS
- ² Recovery Guarantee - certain conditions apply. For full details visit: www.absolute.com/pdf/eula.pdf
- ³ Remote Data Delete - certain conditions apply. For full details visit: www.absolute.com/pdf/eula.pdf