Top Business Reasons Why You Need to Encrypt Your Data

Alliance Storage Technologies, Inc.

Confident Data Archiving Strategies

7

Lost or Stolen Devices

There are a lot of ways these devices can disappear: accidental loss, malicious employees, lack of tracking, etc. According to hhs.gov, since September 2009, there have been 646 breaches impacting 500 or more individuals. More than half of the incidents involved lost or stolen unencrypted devices.

The headlines are out there:

- Four McLean Hospital backup data tapes go missing, thousands affected - four unencrypted backup data tapes went missing.
- UK Insurer (Royal Sun Alliance) loses portable storage device from data center with sensitive customer data.
- Employee with California bank puts customer loan data at risk - An employee handled mortgage loan files stored on a removable disk drive in a manner contrary to the bank’s policies and instructions
- California dentist announces theft of server containing patient information – (office burglary)
- Data at risk following burglary at Liberty Tax Service office in California - Computer towers containing the personal information were stolen during a burglary
- Advocate Medical Breach - four unencrypted computers stolen during an office burglary

6 You may incur many additional expenses including the cost of reissuing cards to customers

If the breach involves credit card information, the cost of reissuing cards can likely fall to you. According to a Bank Technology News article, the cost of creating and mailing a new debit card for a small community bank under $1B in assets is around $11. Larger banks have economy of scale on their side, which brings the cost down to $2.70. Reissuing credit cards ranges from $12.75 to $2.99 for the larger banks.

- **On top of the $25M AT &T settlement, the company was ordered to:**
  - Develop and implement a comprehensive compliance plan
  - Conduct a privacy risk assessment
  - Implement an information security program
  - Prepare a compliance manual
  - Provide employees with regular training on privacy law and the company's privacy policies
  - Appoint a senior compliance manager who is privacy certified
  - Notify all affected customers and provide them with free credit monitoring services

- **Target Corp. agreed to reimburse thousands of financial institutions as much as $67 million for costs incurred from a massive 2013 data breach**

5 You could face potential lawsuits by individual customers in the event of a breach

A breach of personal information can be very damaging to customers. Suits can range from large class action to individual breach victims. Plaintiffs can seek damages for damage to credit, costs of credit and/or identity theft monitoring, costs of card replacement, risk of future harm, emotional distress, fraudulent purchases, and more. Example:

- A law firm has initiated a class action lawsuit against Home Depot for the exposure of 56 Million debit and credit card numbers. According to a New York Times interview with former security employees of the company, Home Depot security allegedly relied on outdated software to secure its systems.

4 You may incur the costs of a forensic investigation conducted by an independent agency

Determining how the breach occurred, who was responsible, and what technology, electronic systems, and processes were involved will require analysis. Depending upon your industry, or simply for the reassurance of your customers, you may be required to secure these services from independent agencies. Most regulatory bodies will require a full justification of how the breach occurred and what actions were taken to remedy the situation. This can be quite costly, particularly to a small business. Example:

- Homebridge retained a data forensics and cyber security firm to assist in investigating the incident after valuable human resource records were accessed and used to file fraudulent tax returns.
- HITRUST, a data security organization, paid for an independent security assessment program for associates of five insurance plans and pharmacy chains after their systems were hacked expositing 111 health records.

3 Small businesses are potential targets

Small business typically do not have the resources of large companies or dedicated professionals to handle network issues and subsequently fall prey to hackers, cyber attacks and other data breaches.

- Business News Daily reports " that small businesses fall into hackers' cyber security 'sweet spot'. They have more digital assets to target than an individual consumer has, but less security than a larger enterprise."
- Symantec's Internet Security Threat Report 2013 reports that In 2012, 50 percent of all targeted attacks were aimed at businesses with fewer than 2,500 employees.
- The National Small Business Association Technology Report indicates that in 2013, 44% of small businesses reported having been attacked with an average cost of $8,700.

2 You can experience damage to your business reputation

A breach does not just damage large businesses with known brands. Small firms, doctor and dental offices, and corner markets equally can experience reputation and brand damage due to data loss or breach.

The Ponemon Institute conducted a survey of nearly 850 executives, found that the average time it takes to restore an organization's reputation is one year. Do you have a year to devote to recovering from damage to your reputation? Wouldn't it be much easier just to encrypt your data?

A research study commissioned by Semafone® indicates that the majority of people surveyed would not do business with a company that had failed to protect its customers' credit card data. 86.55% of 2,000 respondents stated that they were "not at all likely" or "not very likely" to do business with an organization that had suffered a data breach involving credit or debit card details.

1

AND THE #1 REASON…

Fines and Penalties – Need we say more?

Pay now or pay later. Encryption is far less expensive than a data breach. The list of businesses and organizations that have had to pay fines and penalties due to a data breach is becoming endless and the fines are staggering.

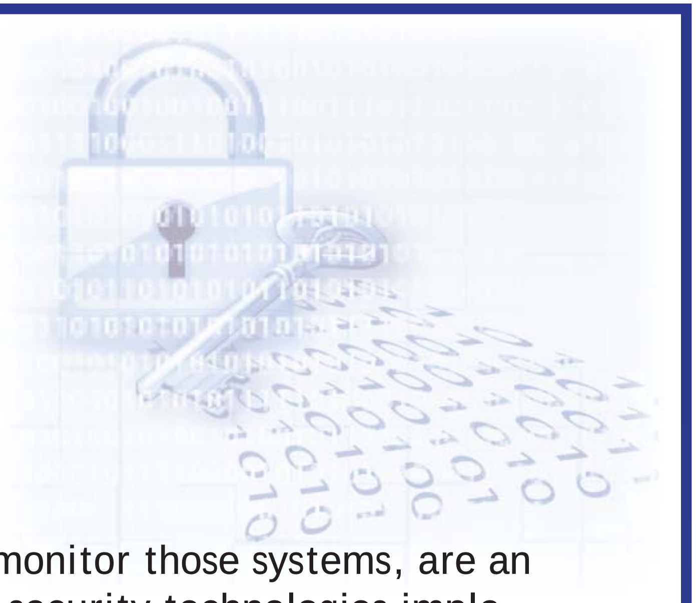
Here are just a few:

- Target: the firm's latest earnings report indicates that the net expense of the breach stands at $162 million. The actual total has now reached a gross expense of $191 million.
- AT & T: $25 Million
- Anthem: $1.7 Million

Healthcare faces the greatest penalties here are some from the hhs.gov website:

- Parkview Health System, Inc. (Parkview) will pay $800,000 and adopt a corrective action plan to correct deficiencies in its HIPAA compliance program.
- New York and Presbyterian Hospital (NYP) has agreed to pay OCR $3.3Mil to settle potential HIPAA violations
- Idaho State University (ISU) has agreed to pay $400,000 to the U.S. Department of Health Human Services (HHS) for violations
- Phoenix Cardiac Surgery, P.C., of Phoenix and Prescott, AZ, has agreed to pay the U.S. Department of Health and Human Services a $100,000 settlement

Conclusion



The majority of breaches are preventable through implementation of data encryption. All data is subject to a breach and consequently, should be encrypted according to the device on which it is to be stored, transferred, transported, or archived.

Data security is multifaceted. Implementing operational policies and procedures, training for employees, and safeguards to monitor those systems, are an extremely important part of the security equation. Additionally, security technologies implemented must protect data and secure all known and unknown points of access from unauthorized intrusion.

Why leave mission critical data vulnerable to attack or theft?

ASTI systems cannot prevent hacking, cyber leaks, malware or malicious insider attacks, but what we can do is secure your archived data using a multi-layered approach to data security. ASTI's NAS solutions offer standard security protections:

- Support for multiple industry-standard authentication services: Windows Active Directory, Local User Level Security, or LDAP which prevent unauthorized access to data
- Unquestioned record authenticity with true Write-Once-Read-Many (WORM) optical media with >50 year life expectancy
- Encrypted data transmission to offsite replicated systems

Add the Data Encryption Feature

On top of an already secure system, you can add the insurance of ASTI's optional Encryption feature and completely lock down your data. FIPS 140-2 compliant, AES 256-bit encryption offers the highest degree of data protection and secures:

- All removable media
  - Online / Nearline
  - Offline (whether local or offsite)
- Disaster recovery copies
  - In transit
  - Local or Offsite
- Data stored on the Cloud
  - During transmission
  - At rest

Benefits Far Outweigh the Costs

The cost of ASTI encryption is measured in pennies per record versus thousands to millions for a breach. As an example a breach of a single stolen device with 50,000 customer records, could cost anywhere from $125,000 to $4.4 Million to remedy, not counting fines. The cost to encrypt those same records might range from $.03 to $.10 (depending upon record/file size) or $1,500 to $5,000.

Would you rather pay now or pay later?

Protect yourself, your investment and your business - let ASTI help. As the professional data archiving leader with decades of experience and knowledge, we have the expertise to help you define and implement an archiving solution specific to your environment with designed-in encryption. Find out now how you can prevent this from happening to you… *Contact ASTI Technical Sales now!*

About
Alliance Storage Technologies, Inc.

Alliance Storage Technologies, Inc. (ASTI) develops and manufactures products and solutions specifically designed for professional data archiving. Innovative solutions incorporate best practice strategies and feature modular, flexible architecture and are adaptable to any business or industry. Seamlessly integrated with leading content and storage management software platforms, and directly accessible as network attached storage solutions, ASTI's archive solutions are trusted worldwide for the protection of archive data.

Archiving products and can be configured for each customer's specific environment and are suitable for businesses of any size from small organizations to the largest enterprise or government. ASTI partner affiliations include world class value added resellers, distributors, and integration partners.

Best-in-class Service Direct support programs are designed to meet the demanding needs of global 24x7 operations.

Contact ASTI
Technical Sales
Today to learn more:
(719) 593-7900

Alliance
Storage Technologies Inc.

Alliance Storage Technologies, Inc.
10045 Federal Drive - Colorado Springs, CO 80908
www.alliancestoragetechnologies.com Telephone: 719-593-7900 Fax: 719-593-4164