

The Cost of InSecurity

Learning About How to Avert Data Breaches and Lower Costs

Healthcare organizations, banks, colleges and businesses face the constant risk of unauthorized or accidental release of sensitive data and personal consumer information. The recent security breaches disclosed by retailing giant TJ Maxx, Ohio University, monster.com, and the Veteran's Administration demonstrate the severity of the issue.

There are many ways organizations expose themselves to data breaches including employee mistakes and theft, customers, as well as contractors and suppliers with whom the organizations shares data and systems. Web applications and File Transfer Protocol (ftp) represent growing risks. In order to facilitate real time information and improve customer service, many organizations have recently turned to web applications and ftp between business entities so information is shared more readily.

The cost associated with data breaches can be enormous and infinite. Research firms Gartner and Ponemon Institute estimate costs ranging from \$150 - \$197 per record inclusive of incident response, PR and lost business. Not to mention the distraction required while senior management tends to unexpected spending allocations, media inquiries and regulatory action. Expect media and customers to react differently to unexpected disclosures. A University that recently experienced Internet disruption noted only 1 in 5 media reports accurately described the incident.

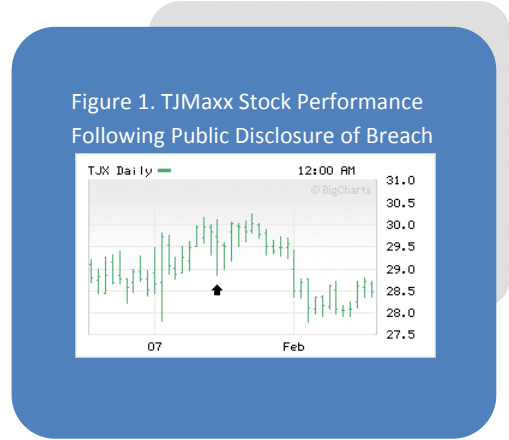
A data breach can have severe repercussions including reputational costs to organization and brand. Following any breach, an organization can lose market capitalization and shareholder value calling into question senior management's ability to

lead the organization. For example, in the 60 days following TJX's January 2007 announcement, TJX stock lost \$3 per share which resulted in \$1.4 billion drop in market value. This happened while consumer confidence was already dipping making a bad situation even more lasting. Research firm Gartner estimates 60% of those consumers affected by a breach will not repeat business with the afflicting organization. For example, if TJX's 44.7 million affected card holders spent an average of \$100 per month and 60% choose not to repeat business that would represent approximately \$2.6 Billion in lost sales in one month. Customers

"Organizations must understand their overall risk," according to Allen Scalise, industry executive, President, Great Lakes Networks LLC. "They need to have visibility into each data vector and a risk assigned to each to determine the probability of a real breach."

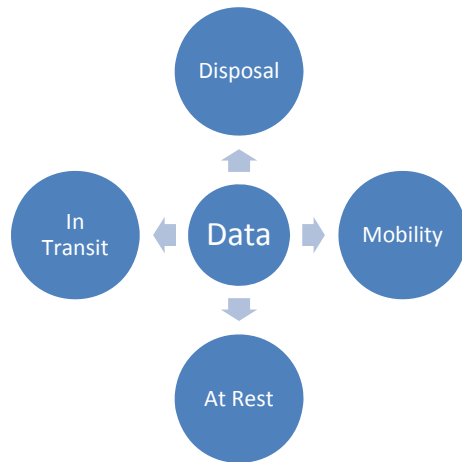


may also have negative perceptions and questions about an organization after a disclosed breach. Ohio University suffered five breaches including student and alumni donor personal information, patient records, employee personal information and technology transfer center research largely supported by grant monies. If alumni and government officials begin to question and hesitate to provide future monies, this type of post event loss perpetuates for years causing more financial burdens. Veterans will consider alternatives before signing up for more services such as VA offered insurance programs. The result is lower recurring revenue streams for the Veteran’s Administration.



Consider the short term costs. At Ohio University, emergency funds were needed for incident response and PR costs. The University spent millions of dollars in the first 90 days, practically wiping out the entire capital budget for the fiscal year. As a result the University likely had to resort to unexpected short term borrowing from key lenders at higher rates costing the University even more. Undoubtedly, this unexpected demand will cause lenders to scrutinize future lending and credit terms.

Figure 2. Examine Data Vectors and Assess Risk



Notifying customers whose information has been disclosed has a significant cost. For Ohio University, the “800” number and call center costs were estimated to be over \$1 million dollars. Rush orders for printing were costly and first class postage expensive. Hiring consultants on short term notice and writing a plan for remediation and corrective

action has significant cost. As part of your PR campaign your organization may want to enlist the help of credit watch services. Be prepared to pay for it. Credit monitoring services are estimated to be \$6-8 per record per year if not more.

If your organization faces regulatory compliance such as HIPAA, GLBA, CIPA, state notification laws or industry standards such as PCI, law enforcement, compliance representatives and regulatory agencies will become involved. If your organization faces regulatory compliance and state disclosure laws, you can expect a great deal of scrutiny from regulators lasting months. Class action lawsuits are inevitable and costly potentially extending several years in some cases. Given TJX had woefully neglected its security measures, the FTC imposed settlement required outside consultants audit the retailer for the

next several years. Fines, settlements and orders may be imposed with on-going costs involved to manage, implement, measure and report regularly. Expect greater scrutiny in the future from internal audits and external examinations or when applying for public monies.

The total monetary cost of a data breach could easily climb into the millions. For example, Ohio University spent an estimated \$4 million in technology upgrades and \$4 million in incident response costs on a \$200 million annual budget, a 4% cost when measured against total annual revenue. Even soft costs such as damage to reputation can have short term and long term effects. Expect a decline in customer business, class action law suits, regulatory action and fines and more. TJX's estimated bill is expected to surpass \$1 billion over a five year period including costs of compliance with the FTC Settlement, new security technology upgrades for 2,500 stores, plus contractor and consultant fees. If the perpetrators are to be caught, expect additional costs for criminal trial and renewed media coverage.

Today's organization must take a holistic view of the ramifications of a serious data breach. This approach must include awareness training for employees, policy enforcement and compliance measurement, self audits, outside validation, and a watchful eye on data movement in your ecosystem. The bottom line is a holistic view will yield risk posture and the ability to weigh in early on corrective measure and budgetary priorities in line with the business objectives and goals.

"Organizations must understand their overall risk," according to Allen Scalise, industry executive, President, Great Lakes Networks LLC. "They need to have visibility into each data vector and a risk assigned to each to determine the probability of a real breach occurring. The data on each vector and asset should be rated and a dollar amount attached including potential loss in the event of a breach."

Taking a holistic view also means organizations must be part of the overall risk management strategy and include all key stakeholders from customer service to senior management. This would allow you to assess operation, reputation, and business cost.

In order to obtain visibility into data vectors you may secure outside assistance, trusted partners, to help regularly protect against data theft, augment risk mitigation efforts, audit business partners, train employees and work with senior management on priorities. The objective should be to achieve a holistic approach to protect the organization and its customers to perpetuate the business.

Great Lakes Networks LLC – You and Your Data Can Rest Easy™

- SECURITY
 - Awareness Training
 - Data Loss Prevention
 - Visibility and Risk Assessment
- PROFESSIONAL SERVICES
 - Technology Integration Solutions
 - 7x24 Managed Support

August 2008

www.greatlakesnetworks.com

(877)800-2310

