

The True Cost Of A Data Breach

By Barry Kouns
Vice President of Information Risk Assessment



Companies reporting a data breach estimate the average cost per compromised record to be \$197, an increase of 8 percent over 2006. Data breaches involving third-party organizations such as outsourcers, contractors, consultants and business partners rose by more than 11 percent and cost the organization \$231 per record.

Let's take a moment to consider how the obvious, and not so obvious costs of a data breach could impact your credit union.

Remediation Costs - the direct costs to replace lost or stolen devices and the necessary investment in strengthening the existing logical and physical security controls.

Legal Fees - aside from attorney fees and actual monetary damages, lawsuits can obligate a credit union to conduct additional training, system upgrades and provide credit monitoring.

Notification Costs - the cost of materials, printing expenses and postage; plus the cost to draft, review and approve the letter and physically complete the mailing; often multiple communication channels are required such as email, personalized letter and phone calls.

Support Costs - the cost of establishing a mechanism for answering questions from affected members; plus any necessary modifications to the credit union's website.

Credit Checks/Monitoring - the cost of providing affected individuals with credit checks or credit-monitoring services, which could be credit union, initiated or court mandated.

Reduced Funds or Member Erosion - the cost to the credit union from withdrawals and reduced deposits as member confidence and trust is rebuilt; plus the cost of recruiting and training caused by employee attrition if the data breach involved employee data.

Marketing \$\$ to Repair Image - loss of previous marketing investment; plus the additional costs of increased future marketing expenses to regain market position and rebuild the credit union's reputation.

As you can see, clearly the costs associated with a data breach are not insignificant. Information security is a business critical function and could be a matter of survival for credit unions.

It's all about trust

The days of limited data access and simple Information Technology (IT) security controls are long gone. Today, the need to make data available from virtually everywhere needs to be balanced with security controls to protect its confidentiality and integrity. Regulations and legislation make protecting non-public personal information imperative. When it comes to information security, members expect and demand that we acknowledge the value of their personal information and apply safeguards to assure its protection from unauthorized access and misuse. The question is, how do we convince, first ourselves and then our members, that we have in fact properly valued our information assets and implemented the appropriate information security best practices? The following 10 best practices can help you form the basis of your information security program:

1) Like most everything else, management must set the tone for information security through thought, word and deed. Information security is a business issue and not an additional duty for the IT department.

2) Management's expectations about information security should be clearly stated in policies that are well communicated, formally issued and

acknowledged by all stakeholders, not just employees.

3) Define classification guidelines to distinguish an information asset in terms of its value, legal requirements, sensitivity and criticality to your credit union in order to assure it is suitability protected.

4) Understand that protecting your credit union's information is best accomplished through people, process and technology. Training and awareness needs to be an on-going process and not just an annual event before the examiners arrive.

5) Establish formal procedures to ensure a quick, effective and orderly response to an information security event or data breach.

6) Establish an information security risk assessment methodology that can be used to identify appropriate security controls and ensure that risk assessments produce comparable and reproducible results.

7) Consider information security a continuous improvement process. Look for ways to improve performance or to avoid issues by being proactive, rather than reactive.

8) Make the appropriate investment. Often investments in additional resources, training and education and/or outside services are just as effective as investments in technology.

9) Instead of implementing ad hoc approaches to securing your information, investigate and implement the appropriate best practices. Chances are there is a proven best practice to address the risk you face.

10) When in doubt, seek objective advice from an experienced third party subject matter expert.

*Remember, Think Security – Act Smart.
Good luck.*

