A Practical Discussion on How to Prepare For, and Hopefully Avoid, a Catastrophic Data Breach

2015 Corporate Counsel Institute

April 29, 2015

Lucie F. Huger
Patrick J. Cotter
Mary Ann Wymore

“Information is the New Oil!”

- Companies are collecting and storing mass amounts of data on a regular basis.
- This data may include information about employees, customers, intellectual property/trade secrets and business operations.
- This data has value to the companies producing/collecting it, to their competitors and to unknown third parties.

Everywhere

- **With the popularity of social media; conducting business on personal devices; and outsourcing certain business functions to third parties, data breaches are becoming more prevalent.**

Possible Outcomes Affecting Business Operations Resulting From A Breach

- Loss of customers
- Damage to business reputation
- Compliance obligations
- Government investigations (federal and state)
- Civil litigation

Common Causes of Data Breaches

- Negligence
- Malicious or criminal attacks (hacking or theft of electronic devices)
- Corporate espionage/malfeasance

Which Data Breaches are being Litigated?

- Probability of a lawsuit is positively correlated with the number of records lost.
- Probability of a lawsuit is positively correlated with the presence of actual harm (financial loss, emotional distress) and negatively correlated with credit monitoring being offered.
- Lawsuits are more likely to occur from breaches caused by improper disclosure of information, as opposed to a computer hack, for example.
- Probability of a lawsuit is positively correlated with the compromise of personal information requiring a heightened level of protection by individuals affected.

Romanosky, S., Hoffman, D., Acquisti, A. (2013). Empirical Analysis of Data Breach Litigation. iConference 2013 Proceedings

Proactive Approach to Avoid a Catastrophic Data Breach

1. Know Your Data

Map the Data:

- What information is stored;
- Who has access to it;
- Is it essential to business operations; and
- Do you have data retention policies?

2. Know the Law

Determine whether particular regulations/requirements/statutes apply to your operations:

- HIPAA: applies to "protected health information" used/accessed/disclosed by "Covered Entities;" "Business Associates;" "Subcontractors" and is enforced by the OCR.
- GLBA: applies to "financial institutions" and is enforced by the FTC.
- PCI: a set of requirements developed by major card brands to ensure that all companies that process, store or transmit credit card information maintain a secure environment.
- Particular state data security statutes. (47 states, in all)
- If international operations, it will be necessary to determine whether there are foreign compliance obligations.

3. Have Your Policies In Place

Review data security/privacy policies:

- Are they in written form;
- Regularly updated;
- Are they tailored to the organization (texting, social media, BYOD, cloud storage, use of external storage devices); and
- Are employees provided with education about the policies?

4. Do You Have a Privacy Statement?

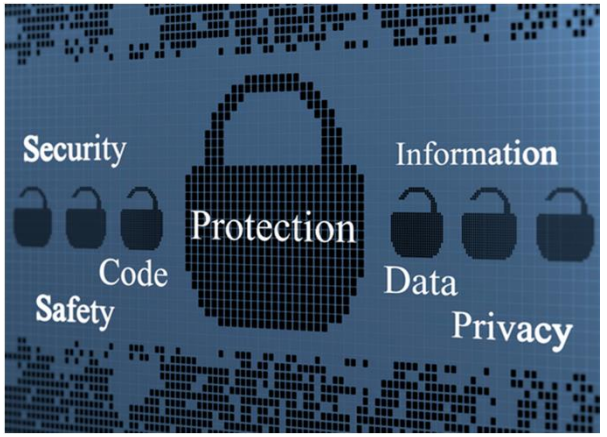
Review privacy statements

- Are they up to date;
- Do they reflect current practice; and
- Does your web presence reflect reality?

5. IT Assistance

Engage IT firms to assist with computer security protection:

- Is encryption possible;
- Is antivirus software adequate;
- Are firewalls adequate;
- Is software up to date;
- Is multifactor authentication used; and
- Are security assessments appropriate?



6. Insurance

Review policies of insurance for cyber liability coverage.

7. Third Party Agreements

Draft agreements with third parties who may have access to data, to ensure proper protections.

8. Have a Plan and Hope to Never Use It

Develop incident response plans.

GREENSFELDER
ATTORNEYS AT LAW

Are you in need of a data risk review?

Lucie F. Huger
314/345-4725
E-mail: lfh@greensfelder.com

GREENSFELDER
ATTORNEYS AT LAW