Data Security Team

BERNSTEIN SHUR
COUNSELORS AT LAW

What Keeps You Awake At Night?

Bernstein Shur Can Help Before & After a Breach

Before the Attack

1. Meet without charge for an initial discussion of the risks, regulatory and legal requirements, and appropriate preventative action plans.
2. Assess your internal procedures and compare to best practices for protection. Perform security audits as narrowly or as broadly as needed.
3. Identify reasonable foreseeable internal and external risks to the security of any electronic, paper or other records containing personal information.
4. Review, edit and negotiate third-party contracts with vendors to assure maximum protections for systems and data.
5. Review insurance policies to assess adequacy of coverage and coordinate with brokers to ensure appropriate coverage.
6. Coordinate with experts to evaluate the adequacy of the technical protections within your and your service providers' computer systems.

After the Attack

1. Coordinate with technical experts to assess the cause and scope of the breach. Determine necessary mitigation steps.
2. If a breach has occurred, conduct a prompt assessment of legal consequences.
3. Determine responsibility for giving notices to people whose information has been compromised and to any credit bureaus and governmental agencies with regulatory authority. This is an essential and very complicated task with potential for severe penalties if not handled properly.
4. Draft all notices required.
5. Prepare information for your employees including instructions regarding which company representatives are authorized to field calls related to the breach.
6. Prepare scripts/information sheets for your representatives authorized to take calls. If warranted, one of our attorneys will participate in each call.
7. Assure that prompt notices are given to appropriate insurers and advocate for coverage on your behalf.
8. Assist in the resolution of adverse civil claims - without litigation when possible.
9. Assist in enforcing indemnity and other contractual rights against service providers that may be at fault in the breach.

Security Breaches Are Extremely Costly To Your Reputation & Bottom Line

You need experienced advisors to navigate technical, legal and insurance issues.

The impact of data security breaches can be devastating to businesses. In 2011, it cost corporations an average of $417,748 and 18 business days to "clean up" after a breach.[1] Despite enormous and increasing resources devoted to combating it, the incidence of data breaches and other cybercrimes continues to grow.

Bernstein Shur's data security team works with you both before and after cyber-attacks to prevent and mitigate losses. We work closely with a network of experienced advisors to address the technical, legal and insurance issues involved.

[1] Second Annual Cost of Cybercrime Study, Sponsored by ArcSight, an HP Company, conducted by Ponemon Institute LLC, August 2011, at 2, available for download at www.arcsight.com.

Team Members

Mike Bosse
mbosse@bernsteinshur.com | 207 228-7276

Dan Mitchell
dmitchell@bernsteinshur.com | 207 228-7202

Jack Montgomery
jmontgomery@bernsteinshur.com | 207 228-7249

Tony Perkins
tperkins@bernsteinshur.com | 207 228-7222

Josh Silver
jsilver@bernsteinshur.com | 207 228-7263

Asha Echeverria
aecheverria@bernsteinshur.com | 207 228-7279

Eben Albert
ealbert@bernsteinshur.com | 207 228-7364