CORPORATE COMPLIANCE INSIGHTS
THE PREMIER GLOBAL NEWS SOURCE FOR COMPLIANCE, ETHICS, AUDIT & RISK

July 11, 2019

5 Ways to Bolster Cyber Safety and Minimize Risk

By Robert J. Munnelly, Jr.

Decades of experience in the age of broadband and security breaches has taught us important lessons about the steps companies should take to protect themselves, employees and customers from cybersecurity threats. Every company should make an effort to adopt specific action items so as to maximize opportunities for long-term cyber safety in this increasingly interconnected world.

Following are five actions companies must take to prepare.

1. Respect and Plan for Cybersecurity Threats

Cyber thieves can target any person or business, and all companies should undertake planning to address potential threats. Security breaches have harmed companies of all sizes and in all industry segments. Companies should not wait to experience a threat before commencing planning and implementation efforts: A breach, ransomware demand, wire transfer redirected to an offshore account, company sale terms negotiated downward because buyer due diligence uncovered a breach history or lack of reasonable security protection can all be avoided with appropriate planning and coordination.

2. A Written Information Security Plan (WISP) is Essential

A WISP that reflects a company-specific, risk-based assessment of legally protected data and associated risks of loss is critical for good cyber health, even where not required by applicable state laws (such as in Massachusetts or Rhode Island) or federal laws (such as for HIPAA/HITECH health information or Gramm-Leach-Bliley financial information). At a minimum, the WISP should address:

- the scope of the plan (both geographic and included or excluded affiliates);
- persons responsible for implementing and updating WISP provisions;
- user passwords and access controls;
- threat protection and intrusion protection software and hardware;
- encryption of laptops holding sensitive data, data traveling over broadband and, increasingly, data at rest in the company network;
- physical security (such as front door security and locked doors and cabinets);
- periodic security and penetration testing;
- contractual protections applicable to vendors holding company protected data;
- annual employee security training;
- a mandatory post-breach review process; and
- an annual WISP update process.

If you have a WISP that does not address all of these elements, take steps to upgrade it.

3. Implement Additional Data-Related Plans and Policies

The WISP should not be your company's only data-related policy. Other important policies include:

Incident Response Plan (IRP) – Having a written plan for responding to breaches enables decisive action and can minimize potential breach-related costs and business harms. Sound IRPs include internal company response team members (including WISP responsible persons, a member of top management, in-house legal, IT and HR executives), external team members (including breach legal counsel, outside public relations, computer forensics and insurance brokers), key breach response action items (documenting breach discovery and timing, isolating infected equipment, retaining forensics professionals, using counsel to interview persons involved in breach issues, communicating to employees about the importance of avoiding unfounded speculation as to breach causes, identifying data-related insurance policies and sending policy notices and meeting state/federal breach notice requirements); and, for larger companies, war-gaming breach scenarios.

Emergency Response/Data Recovery Plan – Companies should plan for responding to data loss or unavailability due to fires or natural disasters, serious breaches or computer ransomware attacks and ensure that network recovery occurs as quickly as practicable. Companies should also have off-site data backup arrangements sized to the extent and importance of its data needs in order to minimize outage-based business losses.

Website Terms of Use/Privacy Policies – Companies need terms of use (also referred to as terms and conditions) that expressly identify and proscribe avenues for website misuse and disclaim possible grounds for company liability from users. Terms of use are typically developed with or linked to privacy policies that disclose what the company is doing with all forms of user data received by the website. These policies have gained increasing importance in light of the new European General Data Protection Regulation (GDPR) – largely echoed in California rules that will take effect next year – that data holders must obtain express informed consent for all of the company's present and future uses of customer/user data, as careful disclosures coupled with "I consent" boxes are likely needed to evidence GDPR compliance.

Other Data-Related Policies – Businesses must also develop a variety of other data policies required by other applicable laws or rules, such as HIPAA/HITECH business associate agreements, GDPR-required standard contract clauses codifying minimum required data safeguards, mobile "app" terms and conditions and the like.

4. Data-Intensive Companies Should Consider Cyber Insurance

Companies with retail business lines or significant potential data loss exposure should investigate cyber-specific insurance policies in addition to other insurance. Companies should carefully investigate coverages that are suitable to the business – including whether the policy covers only the company's own costs or whether it protects against claims brought by affected consumers and other parties – and the nature of costs covered (e.g., breach-related forensics, legal fees, mailing, call center and fees for breach notices and credit freeze offerings to consumers).

5. Plan for Annual Data Security Reviews and Improvements

As cyber threats have rapidly expanded and evolved, your company's WISP, data policies, employee training practices, threat protection hardware and software and insurance should evolve and change as well. Annual reviews of WISPs and related policies, as well as regular investments in security audits, penetration tests or both can identify critical holes to be addressed. In particular, security audits typically provide prioritized recommendations for immediate, medium-term and long-term action items than can help guide company budgets.

Cyber threats are one of the many realities of doing business today. Knowing the risks and putting plans in place will help companies avoid these cyberattacks or, in the unfortunate event of a breach, will prepare you to respond properly and minimize the damage to your customers, employees and business.

Robert J. Munnelly, Jr. practices in the regulatory area at Davis Malm. His data security and information privacy practice focuses on advising and working with companies to develop written plans, improve security-related policies, support compliance training and respond to potential security breaches. He also has extensive experience with legal and regulatory issues faced by energy, cable television and telecommunications companies in New England and nationally.

DAVIS MALM ATTORNEYS