White and Williams LLP

Creating a Culture of Cybersecurity in the Workplace

By: Jay Shapiro
Cyber Law and Data Protection Alert
10.9.15

A workplace that protects its cybersecurity can minimize opportunities for breaches and other situations where liability may arise. Although the technical requirements of creating a secure cyber network fall on experts in computer and Internet security, there are important legal considerations.

Two priorities are developing a culture of a cyber secure workplace and identifying the parameters of the workplace.

Establishing the Cyber Secure culture

Employees need guidance about cybersecurity. Best practices for businesses include setting forth their cybersecurity policies in clear directives that are effectively published to employees. Certainly, when a business has policies that meet these standards it has enhanced legal ability to enforce these rules. Clear policies put employees on notice about conduct that puts a corporation's data and systems at risk.

There are a number of critical elements that go into establishing these policies, but it is beyond dispute that a one-size-fits-all policy is far less helpful than a policy that is designed specifically for the particular business.

The nature of the business and how it operates both provide valuable perspective and, in many instances, demonstrate a need for consistency with applicable laws and regulations. For example, if the business is involved in healthcare matters then HIPAA (Health Insurance Portability and Accountability Act) regulations must be adhered to, as well as other laws that relate to the security of electronically protected health information.

Similarly, businesses in the financial services industry are pressured by federal and state regulators to secure their information, even that which is shared with legal counsel.

Define the "workplace"

An essential element to cybersecurity is to assess how "workplace" is defined by a business. If employees use mobile devices and laptop computers regularly, then the policy should address security relating to those devices. Employees who use home offices and their own computers must be advised of the implications of those practices. A data breach has no less legal significance if it occurs on an employee's own device.

Finally, a policy is only as good as the implementation. Just as a door lock is ineffective when it is not used, a cybersecurity policy has little impact when it is not enforced. It is not unusual for an employee to assert that the failure of a business to enforce a cybersecurity policy results in a ruling that the policy is inapplicable. This argument is often made in the context of email privacy claims.

Keep in mind that effective enforcement can minimize the opportunities for data breaches or intrusions, significant sources of legal liability.

For additional information on how you can establish and implement a cybersecurity policy, contact Jay Shapiro (shapiroj@whiteandwilliams.com | 212.714.3063) or another member of the Cyber Law and Data Protection Group.