Cybersecurity: What Does it Mean to Be Completely Prepared?

By: Jonathan D. Klein, Esq.

So often articles related to cybersecurity focus solely on assessment and preparedness against external forces (*e.g.*, cyber-criminals, hackers, ransomware, etc.), yet do not convey the full array of protections necessary to ensure complete cyber-preparedness for a business. By contrast, this article explores the less talked about, but equally important, intersection between cybersecurity and employment law to demonstrate why businesses must also be protected from internal forces. Only by realizing the importance and necessity of maintaining, reviewing, and constantly updating policies, procedures, protocols, and training will a business be able to face any cyber-related issue without delay and/or major institutional damage.

In a time when there is rarely a day that goes by when the subject of cybersecurity is not at the forefront of news stories, it is commonplace to hear horror stories of businesses where a disgruntled executive departs and exposes his or her former company to privacy attacks or the innocent actions of an employee, *i.e.*, opening a suspicious email, compromises key proprietary data. In addition to the standard protections from external forces, to ensure continued success and safety, businesses must – without delay – learn how and why to assess their current cyber-preparedness, particularly against careless use of electronic mail, Internet usage, electronic data and equipment, and rogue employees.

Whether you are a practitioner with clients who should be thinking more globally about cybersecurity or you happen to be in the legal field within a business reading this article, the time is now to start the conversation about the following evaluative questions. Sitting around hoping that your client or your business will not be affected by a cybersecurity issue is a dangerous stance and will invariably lead to a dire situation from which the client or business may not ever recover. Of course, this article alone is not going to be sufficient to fully prepare your client or business to be fully cyber-prepared, but it is certainly a good starting point to realize what must be done to ensure proper protections are in place.

Does the business have the right policies?

As noted, cyber-preparedness does not just mean simply having a cybersecurity incident response plan, although that is naturally a critical component that every business should have (it's just not the focus of this article). From an employment law perspective, internal cyber-preparedness means ensuring that a business has appropriate policies in place to protect the most sensitive information of that business. For example, a business should consider immediately reviewing and updating, *inter alia*, workplace equipment policies, workplace privacy policies, social media policies, Internet-access policies, usage policies, and employee exit protocols to address current data security and privacy protection issues/regulations.

These are just a handful of the policies, procedures, and protocols a business should consider implementing, reviewing, and updating to ensure sufficient protection from internal forces as well as external forces. Without these critical policies, procedures, and protocols, a business could easily fall victim to a cyber-attack. Such internal policies, procedures, and protocols, however, are not only important from a cybersecurity standpoint, but also to ensure that employees understand business expectations and potential discipline for their actions. The limits of these policies, procedures, and protocols may vary greatly by business and industry, but they should, at a minimum, establish rules of behavior necessary to guarantee that all employees (regardless of level, title, and seniority) are aware of appropriate boundaries.

Has the business properly trained its employees?

In addition to creating, implementing, and updating policies, procedures, and protocols, much of cyber-preparedness also involves appropriate training to ensure that employees are not exposing a business to a data security risk while also understanding how to comply. Training can take a variety of forms, but must – as a matter of best practice – be on-going in order for employees to appreciate the severity of the topics discussed and any new developments. Some topics to consider training employees on include, but are not limited to: effective password management, what to do if a device is stolen (including reporting and discipline depending on the situation), the importance of maximum privacy settings, identifying and flagging potentially harmful spam and malware electronic mail, what is expected upon being asked to leave or voluntarily leaving the business.

One of the hardest aspects of training employees (at any level) is making the entire process easy to understand while at the same time not too painful. In this regard, the key to effective training is to engage employees on security awareness in a way that educates but does not lecture – a bored employee is not going to listen, but zone out instead, undoing the entire point of such training in the first place and once again exposing the business to the risk of a cyber-related incident. With a staggering percentage of recent cyber-attacks on businesses being the result of improper, but avoidable, employee action, this training must make a lasting impact. Teaching employees the risks involved will better prevent organizational losses.

Cyber-preparedness means having strong protection against both internal and external threats and cannot be achieved without a comprehensive cyber security governance framework customized to the risks and threats facing a business. Every business must commit to the on-going process of assessing its weaknesses, develop individualized policies, procedures, and protocols, and maintaining appropriate security measures. Any lawyer reading this who thinks that these issues can be generally addressed through generic policies, procedures, and protocols is gravely mistaken. Only by taking these steps, tailored to a business, will that business and its employees make good decisions to stay ahead of the curve and enjoy continued success.

Jonathan D. Klein is a Senior Attorney at Clark Hill PLC in Philadelphia, Pennsylvania. He has extensive experience representing clients on a wide range of complex commercial litigation and on issues related to cybersecurity and data privacy. Jonathan's diverse practice includes, but is not limited to, financial services litigation, appellate work, and drafting cybersecurity incident response plans, counseling companies if/when a breach occurs, and developing/drafting valid and enforceable internal cybersecurity-related policies, privacy policies, and terms of use. Jonathan also frequently speaks and writes on cybersecurity and data privacy matters for legal and professional groups. Jonathan welcomes opinions about this article and can be contacted at jklein@clarkhill.com or 215.640.8535. Stephanie K. Rawitt, a Member at Clark Hill PLC also in Philadelphia, Pennsylvania, contributed to some of the employment law aspects of this article.