As the nearly daily headlines reporting on data breaches make clear, the question is not if your company will suffer a cyberattack, but when. Indeed, unauthorized network intrusions are on the rise and continue to cost companies of all shapes and sizes millions of dollars every year. According to just one study, the estimated cost for data breaches incurred by companies will rise to a staggering $2.1 trillion globally by 2019. Today’s cyber threats are multifaceted. They include the digital theft of confidential business information and proprietary technology. That is your company’s digital crown jewels. The risks also include loss of customer, employee, or patient data, ransomware and cyber extortion, destruction of information and systems, and cyber-enabled financial crimes such as business email compromise.

The legal risks stemming from cyberattacks also arise from a number of different directions. Following a cyberattack, companies will inevitably face private lawsuits from different constituencies such as customers whose information has been compromised, business partners, shareholders, as well as government or regulatory enforcement actions from a variety of agencies, including the FTC, the SEC, HHS if patient data is involved, financial regulators, and State Attorney Generals, to name just a few.

It is critical then for corporate executives and general counsel to take the steps necessary to reduce both the likelihood of cyberattacks and minimize the legal, regulatory, and business impacts following a breach. Those steps include the following. First, senior management and the board must be engaged in key cybersecurity matters. Board meeting agenda should include time to review and discuss cybersecurity issues and resource allocation. It is also important to assure there is direct reporting to C-suite executives on key cybersecurity risks, preferably independent of the IT Director. Second, a company should implement an information security policy which sets forth rules and guidelines to ensure the security of the information stored digitally at any point in your network. And then regularly provide employee training on the information security policy to ensure that it is understood and followed.

Third, it is critical to develop an incident response plan that guides your company’s response to cyberattacks and data breaches. The incident response plan should be tailored to your company and your industry, and it should identify the key members of your incident response team including the IT division, key business segments, the general counsel’s office, the HR division, and outside counsel. Since it is virtually impossible to prevent a cyberattack, it is crucial to put in place and regularly test the incident response plan in order to reduce all of these risks that are associated with cyberattacks and data breaches.

[End of Audio]