When company leaders hear the words ‘cybersecurity incident’, their natural inclination is to associate it with the information technology (IT) functions of the company. However, cybersecurity incidents are often the primary force driving cybersecurity events. When a company has such an incident, it impacts not only the technical operations but also the business operations and public relations. According to the Association of Corporate Counsel’s recent survey of legal officers worldwide, 85% of respondents believe that cybersecurity incidents are a significant threat to their companies.

The trend for companies to associate cybersecurity incidents with the information technology (IT) functions is understandable. However, legal officers worldwide have noted that cybersecurity incidents are often the primary force driving cybersecurity events. When a company has such an incident, it impacts not only the technical operations but also the business operations and public relations. According to the Association of Corporate Counsel’s recent survey of legal officers worldwide, 85% of respondents believe that cybersecurity incidents are a significant threat to their companies.

The trend for companies to associate cybersecurity incidents with the information technology (IT) functions is understandable. However, legal officers worldwide have noted that cybersecurity incidents are often the primary force driving cybersecurity events. When a company has such an incident, it impacts not only the technical operations but also the business operations and public relations. According to the Association of Corporate Counsel’s recent survey of legal officers worldwide, 85% of respondents believe that cybersecurity incidents are a significant threat to their companies.

The trend for companies to associate cybersecurity incidents with the information technology (IT) functions is understandable. However, legal officers worldwide have noted that cybersecurity incidents are often the primary force driving cybersecurity events. When a company has such an incident, it impacts not only the technical operations but also the business operations and public relations. According to the Association of Corporate Counsel’s recent survey of legal officers worldwide, 85% of respondents believe that cybersecurity incidents are a significant threat to their companies.

The trend for companies to associate cybersecurity incidents with the information technology (IT) functions is understandable. However, legal officers worldwide have noted that cybersecurity incidents are often the primary force driving cybersecurity events. When a company has such an incident, it impacts not only the technical operations but also the business operations and public relations. According to the Association of Corporate Counsel’s recent survey of legal officers worldwide, 85% of respondents believe that cybersecurity incidents are a significant threat to their companies.

The trend for companies to associate cybersecurity incidents with the information technology (IT) functions is understandable. However, legal officers worldwide have noted that cybersecurity incidents are often the primary force driving cybersecurity events. When a company has such an incident, it impacts not only the technical operations but also the business operations and public relations. According to the Association of Corporate Counsel’s recent survey of legal officers worldwide, 85% of respondents believe that cybersecurity incidents are a significant threat to their companies.

The trend for companies to associate cybersecurity incidents with the information technology (IT) functions is understandable. However, legal officers worldwide have noted that cybersecurity incidents are often the primary force driving cybersecurity events. When a company has such an incident, it impacts not only the technical operations but also the business operations and public relations. According to the Association of Corporate Counsel’s recent survey of legal officers worldwide, 85% of respondents believe that cybersecurity incidents are a significant threat to their companies.

The trend for companies to associate cybersecurity incidents with the information technology (IT) functions is understandable. However, legal officers worldwide have noted that cybersecurity incidents are often the primary force driving cybersecurity events. When a company has such an incident, it impacts not only the technical operations but also the business operations and public relations. According to the Association of Corporate Counsel’s recent survey of legal officers worldwide, 85% of respondents believe that cybersecurity incidents are a significant threat to their companies.

The trend for companies to associate cybersecurity incidents with the information technology (IT) functions is understandable. However, legal officers worldwide have noted that cybersecurity incidents are often the primary force driving cybersecurity events. When a company has such an incident, it impacts not only the technical operations but also the business operations and public relations. According to the Association of Corporate Counsel’s recent survey of legal officers worldwide, 85% of respondents believe that cybersecurity incidents are a significant threat to their companies.

The trend for companies to associate cybersecurity incidents with the information technology (IT) functions is understandable. However, legal officers worldwide have noted that cybersecurity incidents are often the primary force driving cybersecurity events. When a company has such an incident, it impacts not only the technical operations but also the business operations and public relations. According to the Association of Corporate Counsel’s recent survey of legal officers worldwide, 85% of respondents believe that cybersecurity incidents are a significant threat to their companies.
The enforcement actions in Wyndham, R.T. Jones, and LabMD related to the companies’ policies and procedures. An employee using an unauthorised computer program brought down LabMD, emphasising the need for appropriate policies, procedures and training.

What can a board do? It should ensure the company has an adequate cybersecurity risk management programme. Such a programme requires team effort from within and outside of the company and should consist of several phases.

The programme should begin with an initial risk assessment to identify each company’s unique risks to determine its baseline security posture. It should be tailored to the company’s business and examine how much and what type of data the company transmits or stores, the various ways that are available to access the company’s network and how those entry and exit points are protected. It should examine who has access to what data and what internal safeguards are in place to protect it. It should examine what IT assets and security assets are in place, how they function and how often they are tested and upgraded. It should assess the company’s internal and external policies and procedures as well as the existing, and existing training of the workforce. It should also examine the company’s contracts and business relationships to see how data is handled and what obligations are in place. By looking at this, as well as other data, the assessment should determine the overall risk exposure of the company by measuring the magnitude of risks it faces multiplied by the likelihood of those risks.

Thinking strategically
The next step is to develop a strategic plan for improvement. Using the risk assessment and looking at the needs and security requirements of the company’s industry, the strategic plan should focus on improving the company’s security posture by creating specific action items that are prioritised, based on the severity of risk to the company.

Either next or, if circumstances warrant it, simultaneous with developing the strategic plan, deploy necessary IT and security assets that are the first line of defence against attacks on the company network. The timing for this step will depend on what is learned during the risk assessment, especially in situations where penetration testing is performed as part of the risk assessment and reveals substantial weaknesses in network defenses.

Implementation of the action items developed in the strategic plan is the next step. A critical component is to prepare and adopt appropriate internal policies and procedures. Once adopted, they should provide the structure to use when training the company’s workforce (and management) on how to protect the company’s data.

Training is critical for several reasons: first, it’s an opportunity to reinforce a culture of security within the company; second, it helps members of the workforce understand the policies and procedures; third, and perhaps most importantly, training should incorporate case studies to demonstrate key principles and help teach the trainees how to think about variations on the examples given as rarely are any two real-world situations identical.

One of the key policies that should be prepared is a cybersecurity incident response plan that will be the company’s playbook should it experience a cybersecurity incident. This response plan should be given to appropriate personnel within the company and they should tabletop test the plan.

Next – and at regular intervals, as determined by the unique needs of the company – its cybersecurity posture should be reassessed and refined using the same process, from the beginning.

Finally, each of these steps should be well-documented so that if a cybersecurity incident ever occurs the company has documented evidence to show that it recognised the cybersecurity risks it faced and took reasonable steps to protect against the risks and respond, should they occur.