Praxonomy Blog
EMPOWERING BOARDS

Secure the Organisation by Securing the Boardroom

Written by Carissa Duenas on March 26, 2019

With the prevalence of online threats and attacks on corporate entities of all kinds and sizes, cybersecurity is an area that cannot be simply relegated to the I.T. departments of organisations to handle.

Securing the corporation is an essential component of sound business strategy that is developed, refined, and shaped by C-suite leaders and Boards of Directors. Security is not solely an information technology concern, it is a risk management issue for the organisation.

Put in this context, these questions arise:

- What does this mean for the Board?
- What are some of the responsibilities of the Board to ensure the security of the corporation?
- How does securing board-related activities impact the overall security of the organisation?
- How might board portals help?

SECURING THE ORGANISATION

Legal Obligation To Exercise Fiduciary Duty of Care

All members of the Board are bound by a legal obligation to act in good faith for the business. The fiduciary duty of care requires that Directors exercise competence, diligence, and prudence when supporting – or furthering – the organisation's objectives. The Board is also expected to make well-informed decisions that serve the collective benefit of the corporation and its shareholders.

This fiduciary duty of care applies to cyber-risk strategy and oversight as well.

Individual directors are increasingly being held accountable for cybersecurity incidents. For instance, the Yahoo! and Equifax data breaches led to a number of class-action lawsuits that sought to impose direct liability on directors for, among others, a breach of duty of care specific to the board's oversight on data security.

Directors, therefore, cannot afford to overlook the issue of cybersecurity. To do so would not only subject the organisation to vulnerabilities, but they also expose themselves to legal liabilities for their failure to fulfil their duties as Board members.

Comply With Security Regulations

The Board needs to ensure that it complies with data protection and privacy regulations set by various regulatory bodies so as to prevent the organisation from suffering hefty financial fines that can severely impact the bottom-line.

To cite an example: in May 2018, the European Union's General Data Protection Regulation (GDPR) took effect. The GDPR is the most important change in data privacy and regulation for business entities that conduct business in the EU. Organisations can be fined up to 4% of annual global turnover for breaching GDPR or €20 Million (whichever amount is higher).

The Board needs to stay on top of shifting and evolving security regulations and laws – as a matter of compliance and good governance.

Minimise Potential Impact on Tangible and Intangible Assets

For some Boards, securing the organisation has yet to be deemed as a critical area of concern. But when security doesn't rank high in the order of priorities as other components of strategy (i.e. financial,

operational, compliance, etc.), the entire organisation can be compromised. Tangible and intangible assets of the corporation can be severely impacted by security lapses and lead to the erosion of shareholder value. This should be a concern for every Board.

Assets At Risk

A.) FINANCES

Security breaches can be so significant as to change the narrative of a company's performance and valuation. When FedEx was subjected to a cyber-attack in 2017, it cost the company USD $400 million – impacting its 2018 fiscal forecast by more than USD $1.00 per share from what was initially predicted prior to the attack. The financial setbacks were also reflected in a decline in operating income and margin in the first half of the succeeding fiscal year, largely due to the costs of the incident (i.e. recovery and remediation) along with lower volume business.

B.) REPUTATION

The potential loss of customer and stakeholder trust may be difficult to regain after a data breach. Customer acquisition costs might jump significantly, and retaining existing customers may turn out to be a challenge since faith and goodwill in the company have diminished. While that has a direct impact on the business, the indirect consequences are worth noting as well – such as the inability to attract investors, acquire top-notch talent, and work with qualified partners.

C.) INTELLECTUAL PROPERTY AND COMPETITIVE ADVANTAGE

An attack on Forrester Research allowed hackers to acquire research content that was available only to its paying customers. Although the hack was contained, it highlights the fact that cybersecurity incidents are not confined to the disruption of production systems.

In other cases, losing proprietary information and intellectual property can have a crippling effect on an organisation's competitive advantage especially if trade secrets are compromised and subsequently divulged, shared, or applied.

SECURING THE BOARDROOM

It's important to consider that Board members can create cybersecurity risks for the organisation. Therefore, security systems and protocols should be applied at this level. Directors have access to – and share amongst themselves – highly-sensitive, valuable, and strategic information. It would be no surprise if Board members are prime targets for cybercriminals.

Let's take a look at how securing board-related activities impacts the overall security of corporations.

Adoption of Secure Communication Practices Minimises Direct and Indirect Losses

The use of personal emails or paper-based methods of communication continue to be prevalent in the dissemination of board-related information. This is problematic because personal email accounts can be easily compromised and binders or folders can be lost. Lost board data makes the organisation vulnerable to various exploits and lead to direct and indirect losses as discussed above.

How Board Portals Help

Board portals help mitigate the security risk around the physical loss of documents, hacking, phishing, and other targeted attacks that seek to obtain and make use of sensitive organisational board information. Premium board portals invest in security technology and adhere to rigorous global quality standards precisely because they have identified what's at stake for the business.

For organisations that are keen on adopting a cultural mindset that factors in security, the use of a board portal assures stakeholders of the business that the Board functions and operates in such a manner that is aligned with the organisation's overall appetite for risk management.

Here are some of the features or properties that secure board portals have and how they help protect the organisation:

A.) SECURE-BY-DESIGN

Security cannot be an afterthought in the development of applications, especially board portals. The most secure of board portals integrate security measures, protocols, and considerations throughout the development process – making board-related information less susceptible to data breaches and cyber-attacks.

B.) DATA ENCRYPTION

File and data encryption ensures that board information remains private and secure even if it lands in the wrong hands. Secure board portals have robust encryption frameworks to preserve the integrity and confidentiality of data. Files are protected by access controls and users' unique decryption keys.

C.) CUSTOM-PERMISSION SETTINGS

The most secure board portals are able to apply custom-permission settings for its users. This means that Directors are granted appropriate rights to view, edit, or delete documents and/or files. Board information can also be disseminated only to specific individuals (or groups) depending on their roles, the situation, and existing board structure.

For example, if a Director belongs to the Audit Committee, he or she can access all audit-related material but may not be able to access the data assigned to members of the Compensation Committee (unless, of course, they were given specific rights or permissions). Custom-permission settings affords Directors the flexibility to control security on a granular level.

D.) IN-APP MAIL / MESSAGING FUNCTIONALITY

E-mail is not a closed-loop system. Emails can be easily sent to unintended recipients. One of the highlights of premium board portals is their in-app mail / messaging functionality – which can substitute for email communications between members. It does away with the multitude of risks associated with emailing and "closes the loop" because messaging is confined to members of the board portal, e.g. Directors and/or portal administrators.

E.) ISO 27001 CERTIFIED

A cloud board portal provider that is ISO 27001 certified meets the global security standard for managing the security of the information it holds – including data assets entrusted to the organisation, i.e. board-related information. Boards who utilise board portals that are ISO 27001 certified can rest assured that they are partnering with a provider who has the infrastructure, systems, and policies to ensure the security of their data.

As a final note, the organisation's commitment to security begins at the top. For the business to instil in its workforce the value and importance of securing the organisation as part of its core corporate strategy, leaders must set the tone for it. Boards have an obligation to cybersecurity and this ought to begin in the boardroom. Securing board-related information not only exhibits a proactive stance towards cybersecurity issues, but it is also reflective of a thoughtful, prudent approach to effective risk management – which, ultimately, is a step in the direction of good governance.

ABOUT THE AUTHOR

Carissa Duenas is a marketing consultant and content contributor for Praxonomy. She began her management consulting career at Accenture and has since worked in a consultant capacity for leading organisations in the technology sector and communications space. She is a contributor to The Globe and Mail, Canada's leading national daily.