Digital Risk:
A BOARD RESPONSIBILITY

Australia's way of life is now integrally linked with the Internet. The Internet provides a global means of communication and interaction that underpins much of our lives – for government, business and individuals. But while the Internet offers a huge range of opportunities, it also brings risks associated with a criminal and malicious activity that seeks to exploit those who use it. In particular, the activities and transactions conducted by business online require diligence to ensure that Australians maximize the opportunities offered by the digital economy (Cyber Crime & Security Survey Report 2012 CERT Australia, Mark Dreyfus)

Digital transformation is the process of integrating digital technology / online business models. into all aspects of business, requiring fundamental changes in technology, culture, operations, and value delivery. According to Forrester research, Such a strategy focuses on:

- Deliver easy, effective and emotional customer experiences. Creating more personalized and engaging experiences for customers
- Focus operations on things customers value. Improved processes for suppliers and customers
- Build platforms and partnerships to accelerate and scale.
- Innovate at the intersection of experiences and operations. Development of new revenue streams

As a result of increased reliance on the internet for enabling digital transformation, businesses also face digital risk. Digital risk can impact the financial sustainability, reputation, customers, shareholders, data, and intellectual property of a business. In broad terms, digital risk management compliments digital transformation by identifying and mitigating digital risk and minimize chances of the risk occurring.

This article describes the following type of emergent digital risks that are becoming mainstream and demand are overall fiduciary response from boards.

1. Cyber risks
2. Reputation risks
3. Fraud risks/cybercrime
4. Regulatory risk
5. Intellectual property risk

Cyber risks

Cyber risk is risk associated business continuity risk when its systems and infrastructure are rendered unoperational due to cyber hacking events. Cyber risk has emerged has a direct result of businesses reliance on technology for their operations. Cyber risk is associated with financial loss, loss of customers or damage to an organization's reputation.

CISCO Systems estimated that 10 billion devices were connected to the internet in 2013, and predicted that this number would rise to 50 billion by 2020.

Activities that can materialize to cyber risks include:

- Malicious security breach
- Social engineering/ Ransomware attacks
- Internet of Things vulnerability
- Third party vendor vulnerabilities
- Supply chain system integration vulnerability
- Lack of security management strategy
- Bring Your Own Device (BYOD) at the workplace
- Human error by employees
- Logging into insecure WiFi using company devices
- Unsecure data storage and theft

Reputational risk

According to the Reputation Institute, a "reputation" is the emotional connection stakeholders have with a company. Adverse reputational situations can be customer related issues, technology or moral, social or ecological issues resulting in loss of revenue.

Poor publicity and negative perceptions usually follow spurred on by ever-active social media and other forms of instant communication made possible by digital advances. Due to the internet harmful information can spread in an instant. Unfortunately, a loss of customers and fall in share price often leads to financial loss for the business.

New information shared by the Australian Millennial Research Report 2019 has uncovered 10% of Millennials said they would change their bank because of the Royal Commission. (The Australian Millennial Research Report 2019). Most millennials are also high users of social media and communicate and share decisions with peers through digital social platforms.

Fraud

In the recent past, cyber crime has emerged as the greatest threat to businesses resulting from digital transformation. Cyber crime costs the economy more than $445 billion every year. In early 2018, one think tank estimated that cybercrime costs the global economy the equivalent of 0.8 percent of GDP. The financial sector in pursuing digital strategy may be particularly vulnerable as the sector transacts most money. The sector is also debating with issue of ownership of fraud liability related to handing of third party monies in order to come to an agreement on ownership of liability.

Cyber criminals are continuously devising new method forcing business managers to react. Fraud awareness and education is now an integral part of digital risk management strategy.

The many causes of cyber crime include:

- Online payment methods/false bank accounts/ intercepting payments/self authorisation
- Online scams/Charity fraud/Dating scams/ Lottery scams
- Hacking /Data Theft/Email hacking
- Identity Theft/Credit Card/Medical
- Social Engineering /Trickery/Impersonation– Financial Fraud
- Phishing /Denial of Service/Malware– Financial Extortion

Regulatory Risk

Regulatory risk in a business is the potential for losses occur when laws and regulations in business are changed. Regulatory risk may lead to Directors and Officers holding the liability for the risk.

In wake of Privacy laws in Australia, Consumers now expect that their most personal information will be handled sensitively and carefully; and significant consumer backlash awaits companies that fail to meet these expectations.

Maximum penalties for serious or repeated interferences with privacy would be increased, from $2.1 million to the greater of:

- $10 million; or
- Three times the value of any benefit that was gained by the company through misusing the personal information; or
- 10 per cent of a company's annual domestic turnover.

Businesses can be liable for misleading and deceptive conduct via social media publications, including (depending on the circumstances) for statements not made directly by the company or for failure to remove abhorrent violent material from a platform.

Mandatory regulatory requirement to notify individual customers of a privacy breach has increased expenses for all business for legal, postage and advertising expenses

Intellectual property risk

Businesses with intellectual properties are prone to digital risks as ideas, brandings, confidential information, trade secrets are potentially accessible to anyone due to the internet. Similarly intellectual property may be stored and shared digitally with supply chain partners such as subcontractors, investors, employees, and business associates. Examples of direct intellectual property threats come from Copyright pirates, Brand impersonators, Patent floaters, Business secret thieves.

The risk involved with storing and sharing such information with the third party is termed as intellectual property risk, it opens the company to potential infringement and loss of intellectual property.

Conclusion

Digital transformation opens great opportunities for any business. It is the digital risk that businesses shall need to contend with through an overall fiduciary strategy as it challenging the measures in place for maintaining trust of customers and stakeholders.

It is important that companies build their risk management strategies transparently and with clarity, ensure information governance in collection, storage, use and archiving of data and define ownership of risk and liability in the supply chain

About the author

Meena Wahi is a company director, business strategist and thought leader with extensive experience in providing business solutions to organisations and government departments. Through identification and management of growth opportunities, process improvements, and business and operational risk management, Meena is able to resolve complex organisational issues ultimately leading to business growth. Meena provides business and operational advice on cyber, fraud, data, intellectual property, and reputational risk management.
She has founded 2 successful two startups, advised numerous government departments and collaborated closely with senior executives, directors and CEOs.

Contact Meen via https://www.linkedin.com/in/meenawahi/ and meena@dataprivacyinsurance.com.au