2000 – 2021 21 Years 2000 – 2021

GOVERNANCE

May 2021 Issue 321

The crisis in governance

‘Nevertheless, toothless enforcement against the company directors responsible for scandals and bother still looks likely to remain the order of the day and plague the future nearly as much as it does the present.’

Gerry Brown

Overseeing cyber risk at board level

‘Measuring what matters is key. Directors should ask management about the metrics used to identify and manage risk. By measuring the right things, and having adequate governance attention, corporations can better manage their risk environment.’

Roberta Sydney

Content

News

International

Global News

Features

Feature

Overseeing cyber risk at the board level

Roberta Sydney provides key questions for boards to consider as they oversee cyber risk and prepare to recover from incidents.

Attack targets for cyber hacking are numerous and growing with the ubiquity of the Internet of Things (IoT) and Artificial Intelligence (AI) along with the number of connected devices in our offices and homes. Further, remote work, a growing global trend pre-Covid, will likely be a permanent fixture – further broadening the attack surfaces for bad actors. Amidst this backdrop, cyber attacks are up 6,000% worldwide since the pandemic began, adding to the challenges that boards and management are handling. According to Dell/EMC, in 2019, cyber attacks on businesses cost approximately $600bn annually worldwide.

> ‘A company should not build a $2,500,000 fence to protect a $10 bill.’

Which data to protect?

A company should not build a $2,500,000 fence to protect a $10 bill. Creating and maintaining a cyber programme costs money – and boards should oversee how management spends that budget to protect mission-critical assets and systems. In a mobile technology world, it is impossible to protect everything. Therefore, prioritisation is a must. Boards should ask management to identify essential data and designate business-critical systems and to reassess that list as the business grows and evolves.

Resources like the US National Institute of Standards and Technology (NIST) Cybersecurity Framework can help identify the weakest links: (1) identify key assets, (2) protect against intrusion, (3) develop a way to detect when things go awry, and (4) create a recovery and business continuity plan.

How bad can it get and how long does it take to detect a breach?

It is not a question of whether there will be a breach, sadly, but when and how significant it will be. The recent NotPetya attack on a global retailer cost $15m daily in revenue and it took the company almost five days to recover. Further, NotPetya spread in seconds after the initial infection. Hundreds of servers, desktops, and phones for this highly connected business were rendered useless, impacting 10,000+ employees. The malware exploited operating system vulnerabilities and burrowed into third party software via a software patch. While good detection and prevention strategies were in place, they did not prevent the event. Therefore, boards need to ask management about their recovery strategy as a key component in business continuity management.

One fact that might scare boards and management is how long it takes to detect a breach. FireEye reports that the ’median well-time’, which is the amount of time an attack goes undetected, is lengthy and differs widely between regions. They reported that the mean well-time for 2018 in the Americas was 71 days, EMEA was 177 days and APAC was 204 days.

A board needs to ask management about breach detection measures, attempted cyber attacks and engage immediately when a significant breach occurs.

Is overseeing cyber risk also a ‘people’ issue?

Some think that cyber is just a technology issue. However, people are a critical element in an effective cyber risk management programme. *Security Magazine* reports that insider attacks – caused by human error or malicious attacks – are among the most difficult to prevent and detect. Boards should ask management for reporting on periodic penetration testing – also known as red-teaming – to determine if additional training is required. Often, these tests reveal that sophisticated phishing emails fool employees and board members who inadvertently click on links.

Since breaches can cause great losses to an organisation, its revenue stream, its stock price, as well as its reputation, a board should ask regularly about the human side of the cyber programme.

Who owns cyber risk management at the board level?

Cyber is part of risk management as with other marketplace risks that corporations face. Boards should understand the risks, and then manage or mitigate them. Often, cyber risk is relegated to the Chief Technology Officer or Chief Information Security Officer (CISO), and the topic is placed under the purview of the already stretched audit committee. Setting up a board risk committee that incorporates cyber into its enterprise risk assessment framework and having the full board engage in regular conversations about the full suite of risk management and business continuity planning activities is a preferred approach.

Measuring what matters is key. Directors should ask management about the metrics used to identify and manage risk. By measuring the right things, and having adequate governance attention, corporations can better manage their risk environment.

Has management allocated sufficient resources?

Knowing how costly breaches can be in time, reputation, and money, boards should ask management what additional cyber risk management measures should be implemented, and at what cost. Kris Lovejoy, Global Cybersecurity Leader at EY, says that she hasn't yet met a management team that says it has sufficient resources to protect the company's key assets, and to detect a breach quickly enough. According to EY, approximately 74% of CISOs are also dealing with pandemic-related budgetary impacts.

The board should ask about how the next dollar would be deployed if additional budget monies were allocated. And, if a board hears that resources are lacking, ask why and determine if it is a misallocation problem.

> 'Cyber is part of risk management as with other marketplace risks that corporations face. Boards should understand the risks, and then manage or mitigate them.'

When and where should cyber considerations be built in?

Companies should build cyber risk management into product design and operations processes from the outset. Car companies don't manufacture and sell vehicles that go on the road, whereupon the safety engineers are then asked to 'add in' security features to make the cars safe. This analogy applies to how management incorporates cyber protection design into the introduction of new systems, vendor interfaces, and system integrations with merged companies, among others.

Planning to harden interfaces with each new technology system or vendor is an important step in deployment. Identifying potential backdoors and access-points is key to advance planning to detect hacking attempts and to prevent entry from bad actors seeking to infiltrate each of these new vectors.

Boards should remember that all connections are susceptible. A hacker used an IoT-connected fish tank to infiltrate a casino's high-roller database, exporting data through a tank thermostat. According to Hemu Nigam, founder, and CEO of Cyber Security Affairs 'this was one of the most entertaining and clever thinking by hackers I've seen'.

Furthermore, Greg Touhill, retired Brigadier General of the US Air Force and cyber security expert recommends that boards ask management if all corporate accounts use multifactor authentication. He says that relying on usernames and passwords is a high-risk approach in today's environment.

In sum, cyber security teams should engage before, not after, an organisation connects or rolls out new technology.

How to recover from a cyber attack?

Business continuity and crisis management are key components of risk management for cyber and other risks. Boards should ask management if and how the organisation could recover if an attacker breaches the perimeter and encrypts or wipes data. To recover well requires pre-planning and designating in advance who is to lead each element of the communication and response effort. After an incident occurs is not the time to consider hiring a crisis communication consultant or to designate who needs to be engaged in the response effort.

Boards can ask management to run tabletop exercises to stress test the crisis management plan, and to identify gaps. I participated in a tabletop on one of my boards that revealed that no one had included the Human Resource Manager in the communication flow – a fact that was painfully obvious once employee computer access was cut off (with no notice) during the damage assessment phase.

While extensive and expensive, recovery usually follows a similar pattern: invoking a cyber incident response plan, performing forensic damage assessment, preparing the recovery, removing the malware, or rebuilding systems, restoring the data into production environments, while communicating internally and externally, as appropriate.

In conclusion

- Directors should stay current regarding cyber security and ask management to prioritise assets and budget accordingly to protect them.
- Boards should ask management how they are designing and building in security on the front end of digital initiatives.
- Train board members and employees to recognise phishing emails, since this is not simply a technology issue. Cyber risk extends throughout the connected device network. Use independent third parties for penetration testing.
- Boards should ask management about pre-planning for a breach and recovery, including a communication plan, leadership plan, and other aspects of business continuity management.

Roberta Sydney is an independent board director and serves on the board of Plaxall, Inc. a Long Island City based real estate and manufacturing business where she chairs the compensation committee and serves on the governance committee. She also serves on the board of Azalea LLC, as well as Tiedemann Advisors, a $22B global wealth manager. She also serves as adviser to several real estate technoloagy start-ups. Her prior corporate experience includes senior roles with financial services institutions, including State Street Global Advisors and the Boston Company. She earned a BA in French from Wellesley College, an MBA from Harvard Business School, and an MS in Real Estate Development from MIT. She is an NACD Board Leadership Fellow and was named among the 2020 Directors to Watch by Private Company Magazine.

GOVERNANCE
www.governance.co.uk

Subscription form

Please complete this form and send by mail to:

**Subscriptions Department Governance Publishing and Information Services Ltd
The Old Stables, Market Street,
Highbridge, Somerset, TA9 3BP, UK**

**Tel: +44 (0) 1278 793300
Email: info@governance.co.uk
Website: www.governance.co.uk**

(Please tick one)

□ Yes! I would like to subscribe to Governance for one year

□ Or save with a 2 year subscription

Governance international subscription costs:

	£UK	Euro	US$
1Yr	325	450	490
2Yr	585	790	855

Governance can accept cheques in other currencies but an administration fee of £15 will be charged.

□ I enclose a cheque/bankers draft for

Currency Value

□ Please invoice me

Specify currency:

Order reference:

Title:

First name:

Surname:

Position:

Company/Organisation:

Address:

Postcode:

Email:

Tel:

Fax:

What our subscribers say

‘*Governance* is a great publication that I look forward to reading.’

‘I have found *Governance* to be a good resource for identifying and elaborating on emerging corporate governance trends.’

‘*Governance* provides a very useful summary of key issues.’

‘I enjoy *Governance* very much. The comprehensive range of topics covered keeps me up to date on corporate governance matters.’

‘*Governance* is a useful means of keeping up to date on developments in a field which is assuming greater importance by the day.’

‘*Governance* is the leading monthly publication covering major corporate governance issues. A most valuable source of information for investors, financial advisors, corporate board members and executives.’

Index

Organisations

People

Companies

Designed and printed by WithPrint
Riverside Studio, Gills Lane, Rooksbridge, Somerset, BS26 2TY
www.with-print.co.uk

ISSN 1358-5142

Governance Publishing and Information Services Ltd
The Old Stables, Market Street, Highbridge, Somerset TA9 3BP, UK
Tel: +44 (0) 1278 793300
Email: info@governance.co.uk Website: www.governance.co.uk