AMMINISTRAZIONE IN CAMMINO
Rivista elettronica di diritto pubblico, di diritto dell'economia e di scienza dell'amministrazione a cura del Centro di ricerca sulle amministrazioni pubbliche "Vittorio Bachelet"
Direttore Professor Giuseppe Di Gaspare
ISSN 2038-3711

The new challenges of cybersecurity for economic operators: the American case

di Andrea Chiappetta

5 dicembre 2019

Summary: 1. Introduction. – 2. Cybersecurity experts on the board of companies in the United States. – 3. Disclosure of cyber expertise board. – 4. Cybersecurity' board oversight. – 5. The board of directors and cybersecurity. – 6. Cybersecurity experts on the boards of the companies. – 7. Conclusion.

1. Introduction

It is crucial to know whether the board of directors have cybersecurity expertise before investing in a certain company. The responsibility of the board of directors is to take control of the entire organization's governance, and its responsibilities include making the right decisions in ensuring the well-being and profitability of the enterprise. A distinctive member of the board is chosen based on the experience and skills needed by the boards to make decisions.

The cybersecurity topic is one of the topics that the board looks to experts to understand better the position of the organization on the cybersecurity's state (Cowley & Greitzer, 2015). Cybersecurity is a growing concern for the board, and it a topic that takes up the discussions of the board majority.

Various companies are at bigger risk for cyber threats and attacks, for instance, industries healthcare and financial services or businesses that conduct their important business online. The cybersecurity expert board member can assist the management team in making crucial decisions regarding risk management and increasing cybersecurity awareness and general knowledge levels on board of directors (Fraser, 2016.). Whether the company adds an expert on cybersecurity or not, the company should ensure that they have enough cybersecurity expertise access. The experts in the board of directors should be capable of understanding cyber-attacks as well as have asses capability of management of dealing with the issues which are related to cyber threats and attacks (Rothrock, Kaplan & Van Der Oord, 2018).

A company with a strong environment of technology with solid information technology leadership, it is possible for the companies to implement cyber controls that are more robust. This will ensure that the precise tactical decisions for cyber become

AMMINISTRAZIONE IN CAMMINO
Rivista elettronica di diritto pubblico, di diritto dell'economia e di scienza dell'amministrazione a cura del Centro di ricerca sulle amministrazioni pubbliche "Vittorio Bachelet"
Direttore Professor Giuseppe Di Gaspare
ISSN 2038-3711

easier. Organizations need someone who has knowledge of cybersecurity and is an expert who is able to understand the issues of cyber. The professionals of cybersecurity who have a bigger understanding of risks associated with technology and the impact of the business are well-suited to be on the board of governance of any company.

2. Cybersecurity experts on the board of companies in the United States

It is a known fact that the US is a global guide on cybersecurity issues and their implications.

The boards' cybersecurity experts have the proper cybersecurity expertise to advise the board on the nest tools, resources, and processes to keep the company safe from cyber-attacks. Adding experts of cybersecurity to the board gives the other members of the board a strong direction on the prefect techniques to assign spending for cybersecurity (Price, 2018). The cybersecurity expert has knowledge and experience, and expertise to guide discussions of the board on how they should spend on both the front end and backend prevention for managing crises (Wirth, 2017). The boards' experts of cybersecurity are the key resource individuals for identifying novel developments in the information technology as novel technologies advances. The experts can also assist the board of directors to be able to know how to categorize risks best and how to create strategies that are comprehensive for protection against cyber-attacks (Rothrock, Kaplan & Van Der Oord, 2018).

3. Disclosure of cyber expertise board

The United States Senate in the year 2017 (Cybersecurity Disclosure Act of 20171) introduced a bill that requires the publicly traded businesses to disclose whether they have experts of cybersecurity on the board of directors in that company.

The new version of the Cybersecurity Disclosure Act of 2019 show a small change of wording to the Cybersecurity Disclosure Act approved in 2017, introducing three new acts as described below:

1) Cybersecurity expertise at board level, and the nature of that expertise, in the organization's annual report or annual proxy statement to the Securities and Exchange Commission (SEC).

2) There is now more focus on the existing cybersecurity posture and a 'person' to be involved.

[1]https://www.congress.gov/bill/115th-congress/senate-bill/536/text?q=%7B%22search%22%3A%5B%22Cybersecurity+Disclosure+Act+of+2017%22%5D%7D

AMMINISTRAZIONE IN CAMMINO
Rivista elettronica di diritto pubblico, di diritto dell'economia e di scienza dell'amministrazione a cura del Centro di ricerca sulle amministrazioni pubbliche "Vittorio Bachelet"
Direttore Professor Giuseppe Di Gaspare
ISSN 2038-3711

3) The third paragraph in both versions of the act says the FTC should consult with NIST, with reference to the NIST SP 800-181 Cybersecurity Workforce Framework[2], to "define what constitutes expertise or experience in cybersecurity... using commonly defined roles..." Substantially the new act will increase the pressure on organizations to have a named CISO with a voice on the board as the most efficient way of fulfilling the legal requirement.

Generally, businesses should solidly consider having an expert on cybersecurity on their bodies (McLaughlin & Anderson, 2016). The importance of the cybersecurity expert in the body will enable the company to develop strategies on how to handle matters concerning cyber-attacks and any other risks Imposed on the company. The expert will ensure that that there is concrete security regarding protecting the personal information of their clients and provide guidelines on implementing crucial policies of guiding security access to information systems of the company. The structure of the cybersecurity team of the enterprise is crucial for making sure that the organization operates in an effective and efficient manner (Wirth, 2017). The board's cybersecurity expert is required to have cybersecurity and technical expertise, and executive and operational level of experience. It is an obligation for the board members to make sure that their companies strike a balance between meeting requirements of compliance effectively and establishing a cyber-program that is risk-based, which addresses vulnerability areas unique to the business (Securities and Exchange Commission, 2018).

4. Cybersecurity' board oversight

Breaching of cyber is going string still, and every year is seen to be a novel year of the breach. One of the most priority problems is cybersecurity for public company directors and executives.

Cyber breaches pose material into risk and have a critical impact on various companies. The regulators and experts heightened attention recently in light of incidents of cybersecurity at main companies indicate that cybersecurity is not just an information technology issues but is the company's important component and of the wide risk management of the enterprise that necessitates expert oversight of the cybersecurity threats (Mitchell, 2018).

The attention of the company to cybersecurity should well extend beyond compliance's regulatory. In the global business environments, today ensures that corporate networks' security and sensitive data is a crucial driver of the businesses and hence, a critical component of financial value and development. Business partners, regulators, investors, and customers are paying attention to programs and risks of

[2] https://csrc.nist.gov/publications/detail/sp/800-181/final

AMMINISTRAZIONE IN CAMMINO
Rivista elettronica di diritto pubblico, di diritto dell'economia e di scienza dell'amministrazione a cura del Centro di ricerca sulle amministrazioni pubbliche "Vittorio Bachelet"
Direttore Professor Giuseppe Di Gaspare
ISSN 2038-3711

cybersecurity to mitigate and address those risks. Various companies should consider the security protocols and risk profile of probable acquisition targets, and the necessary preparedness and oversight of cybersecurity must be the main factor in determining combinations of potential business.

The proper oversight of the board requires the management to be fully aware of the current cybersecurity measure's effectiveness and the importance of cyber incidents that have happened if any (Wong, 2014). Disclosure of procedure and controls should assist the business to identify incidents and risks of cybersecurity, analyze and assess consequences on the business of the company, evaluate the importance related with incident and risks, enhance open communication between disclosure advisors and technical experts, and finally make disclosures that are timely regarding those incidents and threats. The businesses should assess themselves to determine whether they have enough disclosure procedures and controls to make sure that cybersecurity incidents and risks are identified at the right time, evaluated, and then reported to the appropriate management personnel and board at large (Mitchell, 2018).

The oversight board requires the directors to understand the cybersecurity risk's nature and prioritize cyber disclosure, response, and detection. The board is required to receive updates from the management and other expert advisors of cybersecurity matters on the compliance of the company with applicable standards. The board should be given reliable information so that they can determine the right action to take in regards to cyber-attacks and risks. It is crucial to have an expert on cybersecurity on the board members, and also it is considerate to add a technical expert to their disclosure and sub-certification committee procedures.

There are various considerations that should take place for structuring cybersecurity's board oversight. Those considerations include tailored oversight, oversight structure, tools of measurement, incidence response plan, and the team of crisis management, and red flags.

Tailored oversight

From one company to another, cybersecurity risks vary, and it must tailor its approach to its certain business that includes data of which it should be responsible for and risks to that data.

Structure of oversight

The cybersecurity's oversight of the boards can be attained in various ways. The audit committee in several companies retains primary cybersecurity risk oversight. Some companies have developed a designated committee on cybersecurity, and the entire board maintains the responsibility of oversight (Lanz, 2014). Any structure of the oversight should comprise regular meetings with the information security officer of the company, and there must be the right protocols for uplifting information on crucial incidents and risks of cybersecurity.

- Measurement tools

AMMINISTRAZIONE IN CAMMINO
Rivista elettronica di diritto pubblico, di diritto dell'economia e di scienza dell'amministrazione a cura del Centro di ricerca sulle amministrazioni pubbliche "Vittorio Bachelet"
Direttore Professor Giuseppe Di Gaspare
ISSN 2038-3711

The committee or the board should determine the cybersecurity risks of the company and its controls efficiency to address risks. By the use of the right benchmarks to regulatory and standards requirements of the industry, and ever-changing state awareness of the cybersecurity technologies art and best practices.

- Incidence response plan and the team of crisis management

An effective strategy on cybersecurity needs expediency in responding to resiliency and breaching in recovering and addressing from the breach. Having in place a crisis management team that includes representatives from information technologies, management, legal, and investor relations allows the business to respond to matters concerning cyber-attacks mare quickly and effectively. The companies should always seek advice from the cyber counsel who is qualified so as to test, update, formalize, and organize the incident response adequacy and the plan of data breach notification. The experts should evaluate the disclosure procedures and controls of the company concerning information on cybersecurity that includes the right restrictions on corporate insider trading when management is investigating a breach that might occur.

- Red flags

The cybersecurity experts in the board should mind about cyber incidents at critical vendors and peer companies that can offer insights into types of cyber-attacks the company my experience and highlight potential supply chain and systems vulnerabilities that should be taken into account. The work of the board is to oversee the potential risk that might occur and look for the best tactics to address the issues.

5. The board of directors and cybersecurity

Cybersecurity is a financial risk, reputational, and legal issue, which is increasing prominently for companies and consequently for the board of directors. Over two-thirds of the corporate directors that are 69 percent reported concerning their board being involved more with cybersecurity according to the 2015 report, and it had been in 12 months earlier. Several directors stated that their organizations had not taken crucial and solid steps with respect to cybersecurity while the boards were involved in issues of cybersecurity (McLaughlin & Anderson, 2016).

It is not an exaggeration to say that the landscape of legal in accordance to cybersecurity is growing in the geographic landscape as well as in complexity. In the United States, all the 47 states have laws which need the companies to provide notice to affected individuals by a breach of security (Riggi, n.d). The handful of states requires the entities to implement security measures that are reasonable to protect particular data types. Massachusetts dictates that business that handles personal information should implement an information security program which comprehensively written to address various security basics, for instance, regular security of information program audits and employee training.

AMMINISTRAZIONE IN CAMMINO
Rivista elettronica di diritto pubblico, di diritto dell'economia e di scienza dell'amministrazione a cura del Centro di ricerca sulle amministrazioni pubbliche "Vittorio Bachelet"
Direttore Professor Giuseppe Di Gaspare
ISSN 2038-3711

Due to increased cybersecurity attacks as well as increasing calls in the private sectors for transparency, the public organizations need to disclose to the United States Securities and Exchange Commission whether they have security professionals on the board during their periodic filings. Cybersecurity Disclosure Act of 2019, which is pending, is part of the developing trend of enhancing oversight cybersecurity of the private sector by the Securities and Exchange Commission. Originally the cybersecurity act was introduced in the year 2017 and reintroduced in 2019 by three senators, and they are Susan Collins (R-ME), Mark Warner (D-VA), and Jack Reed (D-RI). The Act was later supported by Doug Jones (D-AL) John Kenney (R-LA), who were novel Democratic and Republican co-sponsors. This proposed disclosure is almost similar to the Sarbanes-Oxley Act of 2002, which requires the public organization to identify members who are financial experts of its audit committee annually during their disclosure (Sandstrom, 2019).

Cybersecurity Disclosure 2019 Act directs the Securities and Exchange Commission to give last rules requiring an issuer who is registered to

- To disclose in its annual statement of proxy or mandatory yearly report whether there is any member in their board of directors has experience or expertise in cybersecurity and;
- In case there is no member who is expertise or has the experience, the company has to describe other company cybersecurity aspects that were considered by the person in charge of evaluating and identifying candidates for the governing board (Sandstrom, 2019).

Senator Jack Reed (D-R.I.) proposed that companies that do not have such members on their body to explain in filings to the Securities and Exchange Commission how other efforts of cybersecurity are absent (Merken, 2019).

Various federal regulators in the United States have affirmed authority within the space of cybersecurity beyond the requirements of the state laws. Various agencies of federal in the United States have shown interest in regulating issues of cybersecurity. The agencies include Health and Human Services, Securities and Exchange Commission, Department of Energy, and Federal Communications Commission. For instance, the Securities and Exchange Commission requires the companies to disclosure under its guidelines to file a notice of security issues, if any. This agency has come up with investment advisors and broker-to-dealers enforcement actions for not having proper procedures and actions in place which were developed to protect against expected hazards or threats to the customer information security (Fontaine & Stark, 2018). Cybersecurity has become one of the critical issues in various organizations, and it has to be looked into clearly. The experts can give away forward on how to deal with certain matters that may cause cyber threats to the companies due to ever-changing cybersecurity threats' nature (Larcker, Reiss & Tayan, 2017).

Rules concerning notifications and cybersecurity around cyber breaches have resulted in a larger discussion as well as awareness on this cybersecurity issue.

AMMINISTRAZIONE IN CAMMINO
Rivista elettronica di diritto pubblico, di diritto dell'economia e di scienza dell'amministrazione a cura del Centro di ricerca sulle amministrazioni pubbliche "Vittorio Bachelet"
Direttore Professor Giuseppe Di Gaspare
ISSN 2038-3711

Industries like utilities, telecommunications, and financial services are subject to increased cases of cyberattacks and have regulatory requirements that are strict for cybersecurity. The regulatory and government agencies across the globe have tightened requirements concerning breach notification. Therefore, a body would benefit from having a board member who is able to identify the strategy of the company and the cybersecurity (Donlon, 2018).

Companies with Cybersecurity experts	Name of the expert
LPL Financial	Corey Thomas
Snap	CEO of McAfee, Chris Young
Goldman Sachs' bank	Phil Venables
Spirit Airlines, Popular Inc., and CMS Energy	Myrna Soto
Deutsche Bank	Gerhard Eschelbeck

*Table 1: cybersecurity experts on the board of directors (*Mehta, 2019*).*

6. Cybersecurity experts on the boards of the companies

Cybersecurity threats issues are ever-changing every year with new breaches being witnessed. Publicly traded companies have experienced 60 breaches, and 2016 was no difference with 2017, and the pace of breaching always surpass the previous. These breaches are not only small annoyances, but also they come with a cost.

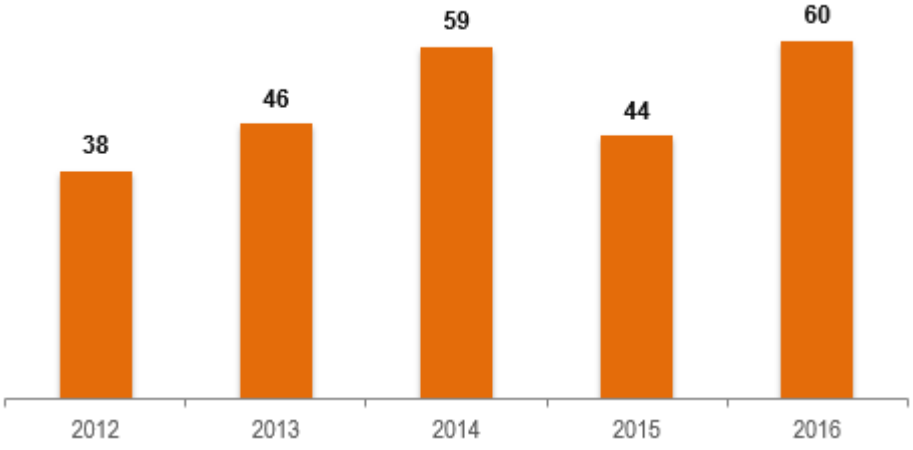

Fig 1: cybersecurity breaches number (Coleman, 2017).

The data breach cost is averagely totaled to 3.62 million USD, and 24,089 records were disclosed according to the data breach cost study of 2017. The companies can be able to curtail cost when the threats occur by personal data encryption, creating a response team of the incidents, coming up with bora-level involvement, and taking part

AMMINISTRAZIONE IN CAMMINO
Rivista elettronica di diritto pubblico, di diritto dell'economia e di scienza dell'amministrazione a cura del Centro di ricerca sulle amministrazioni pubbliche "Vittorio Bachelet"
Direttore Professor Giuseppe Di Gaspare
ISSN 2038-3711

in threat sharing. Companies are adopting cybersecurity protocols based on the novel directors' appointment (Coleman, 2017).

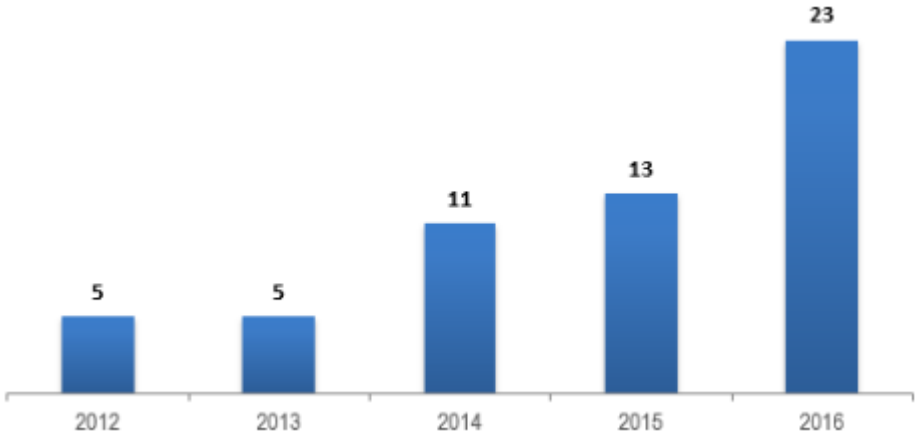

Fig 2: cybersecurity experts' appointment (Coleman, 2017).

Over the past years, the number of persons with cybersecurity experience has been selected as the boards to public companies has increased tremendously. This shows that the experts will be able to analyze the required tools and methods to deal with cybersecurity issues. The experts take a look at possible loopholes available in the company and come up with a team that will tackle the problems and thus prevents any threat which is likely to occur — as per the study of Ponemon, having involvement of board-level reduces the breach cost by 3 percent totaling to 123000 USD. Also, having the involvement of the board-level can lead to bigger results. A knowledgeable and committed board of cybersecurity and cyber safety can play a critical role in implementing a response team of an incident and take part in sharing risks, and the two actions can result in a reduction of the average breaching cost by 13 percent and 5 percent respectively. The average reduction cost of the two actions is 193,000 USD for participating in risks sharing 468,000 USD for implementing the incidence response team (Coleman, 2017).

A bilateral group of senators has suggested a bill that requires each public company to disclose to its directors' cybersecurity. The sponsors of the bill want to promote transparency as well as give the public and investors a precise understanding of whether companies that are publicly traded are prioritizing cybersecurity, and they are able to protectors customers and investors against cyber-attacks (Cowley & Greitzer, 2015). This disclosure law does not expect the public companies to have an expert on cybersecurity on their bodies. A company can disclose if it has a board member who has cyber expertise or can decide to go for cyber consultants from outside and it can boost the staff's cybersecurity expertise instead of hiring a director who has certain knowledge and experience of cybersecurity (Larcker, Reiss & Tayan, 2017).

AMMINISTRAZIONE IN CAMMINO
Rivista elettronica di diritto pubblico, di diritto dell'economia e di scienza dell'amministrazione a cura del Centro di ricerca sulle amministrazioni pubbliche "Vittorio Bachelet"
Direttore Professor Giuseppe Di Gaspare
ISSN 2038-3711

The cybersecurity committee of the board can manage a wider arrange of issues related to cyber issues that the public companies face, which includes plans of the business community, incident response plans, insurance of the cyber, bad leaves, and insider threats. In case the board does not have a cybersecurity expert, the board can hire an external expert to take the position of the cybersecurity director on the boards. Without an experienced as well as qualified cybersecurity expertise on the board, the board can leave a crucial enterprise risk which is unchecked. The company itself can expose to finger-pointing if it fails to follow the guidance of 2018 as well as failure to attain its obligations. The notion of boards to have an expert on cybersecurity has picked up grip not only from the regulatory point of view but also as a federal law matter (Cowley & Greitzer, 2015).

There is a need for boards of directors to have knowledge of cybersecurity. It should have enough access to the expertise of cybersecurity, and discussions concerning risk-management should be discussed in the board meeting. The bodies should consider having expertise in information technology access at the board level, and instead of depending on other business parts, clear responsibility allocation for cybersecurity oversight (Balbi, 2015). Various companies consider adding information technology security or cybersecurity expert to the board directly through recruiting novel directors. But also, the board can consider increasing its security expertise access as the board can develop a system of a check-and-balance by looking for advice from cybersecurity experts.

7. Conclusions

A good oversight board needs the board to be informed fully on the effectiveness of the existing measures of cybersecurity and the importance of any incidents of cyber that have occurred, both in public and private companies. Controls, as well as disclosure, should allow businesses to identify incidents and risks of cybersecurity, analyze and analyze the impact on the business of the company, assess the importance associated with those incidents and risks, enhance communication between advisors of disclosure and technical experts, and make disclosures which are timely concerning those risks and incidents, and if it possible also provide an estimation of the damages (financially and reputationally). The cybersecurity (independent) expert importance in the body will enable the business to develop strategies on how to handle matters about cyber-attacks and any other risks imposed on the enterprise. The cybersecurity experts have a mandate to inform the entire board of directors when a cyber-incident has been identified (Balbi, 2015). The experts in the board of directors should be capable of knowing cyber-attacks as well as assess the capability of management in dealing with the matters which are connected to cyber threats and attacks. The board is required to receive updates from the management and other expert advisors of cybersecurity

matters on the compliance of the company with applicable standards. The significance of the cybersecurity professional in the body will assist the company in developing tactics on how to handle matters regarding cyber-attacks and any other risks imposed on the business

The board of governance should have a cybersecurity expert as a member of the board who can assist them in making critical decisions concerning cybersecurity matters and giving them guidelines on how to go with cyber-attacks (Balbi, 2015). An oversight board concerning cybersecurity audits should include a comprehensive assessment of security and risk review, reports of penetration testing, and any other subsequent efforts of remedial or corrective measures that are implemented afterward (Lanz, 2014). The oversight panel obliges the directors to realize the cybersecurity risk's nature and prioritize cyber disclosure, response, and detection.

The board needs to know that they have to be informed concerning cybersecurity and therefore keeping up with cybersecurity in the world of information technology which is complex and rapidly changing, where of course the role of the regulator it is fundamental to improve and protect the competitiveness of a nation, and indirectly their impact on foreign direct investments.

References

Balbi, A. (2015). Discussing cybersecurity at the board level. *Strategic Finance*, *96*(7), 22.

Coleman D., (2017). *Cybersecurity Experts on the Board of Directors.* Retrieved from https://blog.auditanalytics.com/cybersecurity-experts-on-the-board-of-directors/.

Donlon, J.(2018). Boards Increasingly Challenged By Oversight Of Cyber Threats. Retrieved from https://boardmember.com/boards-increasingly-challenged-oversight-cyber-threats/

Fontaine, D.R. & Stark, J.R. (2018). Cybersecurity: The SEC's Wake-up Call to Corporate Directors. Retrieved from https://corpgov.law.harvard.edu/2018/03/31/cybersecurity-the-secs-wake-up-call-to-corporate-directors/

Fraser, J. R. (2016). The role of the board in risk management oversight. *The Handbook of Board Governance: A Comprehensive Guide for Public, Private, and Not-for-Profit Board Members*, 283.

McLaughlin, P. & Anderson M, (2016). *Cybersecurity and the board of directors*. Retrieved from

https://www.financierworldwide.com/cyber-security-and-the-board-of-directors#.XX8ZACgzbIV

Merken, S. (2019). Senators Call for Board-Level Cybersecurity Expert Disclosure. Retrieved from https://news.bloomberglaw.com/privacy-and-data-security/senators-call-for-board-level-cybersecurity-expert-disclosure

Lanz, J. (2014). Cybersecurity governance: The role of the audit committee and the CPA. *The CPA Journal*, *84*(11), 6.

Larcker, D. F., Reiss, P. C., & Tayan, B. (2017). Critical Update Needed: Cybersecurity Expertise in the Boardroom. *Rock Center for Corporate Governance at Stanford University Closer Look Series: Topics, Issues, and Controversies in Corporate Governance No. CGRP-69*, 17-70.

Mehta, T. (2019). Corporate Boards Are Snatching Up Cybersecurity Talents. Retrieved from https://www.forbes.com/sites/abb/2019/07/11/a-quiet-and-emissions-free-transport-of-the-future/#fac46852139f

Mitchell B. R. (2018). *BOARD OVERSIGHT OF CYBERSECURITY.* Retrieved from https://www.expertguides.com/articles/board-oversight-of-cybersecurity/arfoqroc

Price, N., (2018*). Why Cybersecurity Requirements Are Growing for Board Members.* Retrieved from https://www.boardeffect.com/blog/cybersecurity-requirements-board-members/

Riggi, J. (n.d). *The executive board's role in cybersecurity.* Retrieved from https://ethicalboardroom.com/the-executive-boards-role-in-cybersecurity/

Rothrock, R. A., Kaplan, J., & Van Der Oord, F. (2018). The board's role in managing cybersecurity risks. *MIT Sloan Management Review*, *59*(2), 12-15.

Sandstrom, T.(2019). Congress Considers Requiring Public Companies to Disclose Board Member Cybersecurity Expertise in SEC Filings. Retrieved from https://georgetownlawtechreview.org/congress-considers-requiring-public-companies-to-disclose-board-member-cybersecurity-expertise-in-sec-filings/GLTR-06-2019/

Securities and Exchange Commission. (2018). Commission Statement and Guidance on Public Company Cybersecurity Disclosures. *February 26*, 2018.

Wong, V. C. (2014). Cybersecurity, Risk Management, and How Boards Can Effectively Fulfill Their Monitoring Role. *UC Davis Bus. LJ*, *15*, 201.

Wirth, A. (2017). The Economics of Cybersecurity. *Biomedical instrumentation & technology*, *51*(s6), 52-59.