Cybersecurity Description and Control Criteria to Strengthen Corporate Governance

Hugh Grove
University of Denver

Mac Clouse
University of Denver

Laura Georg Schaffner
University of Strasbourg

The dangers of not properly focusing upon cybersecurity risks were emphasized by recent, notorious attack and hack examples. With guidance from key sources, like the AICPA Cybersecurity Guide, cybersecurity strategies can be developed by corporate executives and Board of Directors to help thwart such attacks. An immediate trend for data security is the General Data Protection Regulation adopted by the European Union in 2018 as well as quantum computing. If all of this is accomplished, the entity's corporate governance would be strengthened by corporate executives and Boards of Directors who are the key gatekeepers for protecting and enhancing the investments of company stakeholders.

INTRODUCTION

A Chartered Global Management Accountant survey found that 68% (852 of 1,253) of the Chief Financial Officer and Controller respondents were moderately or significantly concerned with the threat of cyberattacks to their companies (CGMA 2015). "Cybersecurity threats are escalating, thereby unnerving Boards of Directors, managers, investors, and customers of businesses of all sizes---whether public or private," observed Sue Coffey, The American Institute of Certified Public Accountants (AICPA) Executive Vice President of Public Practice. She also said: "While there are many methods, controls, and frameworks for developing cybersecurity risk management programs, until now there hasn't been a common language for companies to communicate about, and report on these efforts" (Tysiac 2017).

Accordingly, the AICPA issued in May 2017 a Cybersecurity Guide, Reporting on an Entity's Cybersecurity Risk Management Program and Controls. This Guide assists CPAs and others who are engaged to examine and report on an entity's cybersecurity risk management program. It defines criteria as the benchmarks used to assess and evaluate the subject matter. To enable the preparation and evaluation of cybersecurity information, two distinct yet complimentary sets of criteria are used in an examination of cybersecurity risk management. Description criteria are used to prepare and evaluate the

description and presentation of an entity's cybersecurity risk management program. Control criteria are used to evaluate the effectiveness of controls to achieve an entity's cybersecurity objectives (AICPA 2017). An immediate need for data security is the General Data Protection Regulation (GDPR), adopted by the European Union (EU) in 2016 and enforced on May 25, 2018 (McCallister, Zanfir-Fortuna, and Mitchell 2018).

To strengthen corporate governance for cybersecurity, this common communication language of AICPA description and control criteria could be used by Boards of Directors to assess the cybersecurity programs of their companies. Boards could either set up a separate Cybersecurity Committee or expand the Audit Committee's duties. Such attention to cybersecurity is essential as emphasized by this quote: "Once again in 2016, experience seemed to verify that there are only two kinds of companies—those that know they've been hacked and those that have been hacked but just don't know it" (Castelluccio 2017). The rest of this paper covers the topics in the following sections: EU General Data Protection Regulation, cybersecurity risks and recent notorious hacks, description criteria for cybersecurity, control criteria for cybersecurity, threats from quantum computing, and summary.

EUROPEAN UNION GENERAL DATA PROTECTION REGULATION

This new Cybersecurity Guide is timely as the EU GDPR went into effect on May 25, 2018. It affects all companies that use personal data of persons in the EU to provide services, sell goods, or monitor their behavior, even if those companies don't have an office in the EU. Such companies must have an appointed representative for EU enforcement purposes. The GDPR is a comprehensive law that applies to businesses handling personal data of individuals in the EU, even when no transaction takes place and regardless of whether a business is physically located in Europe. The GDPR provides for fines, which can go up to 20 million euros or 4% of annual global turnover, or revenue, for the previous year and is much more comprehensive than the 1995 EU Data Protection Directive.

Many U.S. companies have been working on implementation plans for GDPR since it was passed in 2016 but other U.S companies are still determining whether the GDPR even applies to them. The GDPR does apply to companies that are not established in the EU as long as they provide services or offer goods to persons in the EU or they monitor the behavior of persons in the EU, such as Facebook's EU subscribers. Thus, all such U.S. companies are subject to the EU's GDPR. Examples include cloud-based businesses, companies that market to international client bases, pharmaceutical and medical-device companies, hotels, universities, international professional organizations, and all companies with EU-based customers or their data. Also, should a personal data breach occur, companies must notify the supervising authority of the breach within 72 hours of becoming aware of the event and they must notify impacted individuals "without undue delay," not waiting months while insiders sold their common stock in the Equifax data breach (McCallister, Zanfir-Fortuna, and Mitchell 2018).

If an organization already has good data protection measures, complying with GDPR should require tweaks, rather than an overhaul. The Institute of Chartered Accountants of Scotland (ICAS) has provided six steps to comply with GDPR (Huber 2018):

1. Review your data
2. Update your notifications about data privacy
3. Make someone responsible for data protection
4. Train staff in data protection
5. Check your suppliers and contractors if they handle personal data on your customers
6. Double-check your organization compliance with new data protection rights for individuals.

Similarly, completion of the following four items concerning GDPR is recommended (Kalinich 2017):

1. EU GDPR Readiness Assessment: Companies need to identify, prioritize, and remediate gaps in compliance programs and mitigate data protection risks.

2. Cyber Impact Analysis: Companies need to model the financial statement impact from data breaches and provide a comprehensive understanding of the cyber exposures facing the company.
3. EU GDPR Insurance Endorsement: Companies are required to address defense costs, expert cyber services, and regulatory defense costs.
4. Incident and Claims Response: Companies are asked to recruit post-event advisory services, including incident response, digital forensics, and claims handling to lower the total cost of risk.

CYBERSECURITY RISKS AND RECENT NOTORIOUS HACKS

There are numerous, recent 2017 and 2016 examples to emphasize attack and hack cybersecurity risks. Equifax, a U.S. credit-monitoring company, disclosed a data breach from hacking on September 7, 2017 where hackers may have stolen the personal information of 143 million Americans, one of the largest hacks ever. The company said that it had learned of the hacking on July 29 but did not disclose this hack publicly until September 7. A required Securities and Exchange Commission (SEC) report for executive trading showed that on August 1 and August 2, Equifax's Chief Financial Officer (CFO) sold shares worth $946,374, the President of Equifax's U.S. information solutions division sold shares worth $584,099, and another divisional President sold shares worth $250,458 for a total of almost $1.8 million (Riley et al 2017). In the following week from the public disclosure on September 7 through September 13, the Equifax stock fell from $142.72 to $96.66, a 32% drop of $46.06, which destroyed $5.5 billion in market capitalization. By early October, 2017, the stock had recovered to $107.83 which represented a $4.6 billion market cap destruction of 26% in one month. As of early 2018, the stock only had a minor recovery to $115.44.

An ongoing U.S. Justice Department investigation, aided by the U.S. Federal Bureau of Investigation, found Equifax had learned about a major breach of its computer systems even sooner in early March. Using this earlier timeline, the CFO sold shares on May 23 for $1,910,160 and on May 21 for $6,455,346. If either of the investigations by the U.S. Justice Department or the SEC finds that company executives knew about this hack by February 28, then the Chief Executive Officer (CEO) and other executives could be in trouble. On this date, the CEO sold 74,346 shares worth $9,742,299 and six other executives sold 41,913 shares worth $6,424,595 (MarketWatch 2017). None of these executives had pre-determined stock sale plans to mitigate insider trading allegations (Koren 2017). Equifax's Chief Information Officer and Chief Security Officer both resigned on September 15. The CEO resigned on September 26 but may still get $18.4 million in retirement payouts and possibly millions more, including lifetime health coverage (Surane and Melin 2017).

Over twenty-five lawsuits have subsequently been filed against Equifax and forty U.S. states have joined a probe of its handling of the data breach. The U.S. Federal Trade Commission and a U.S. Congressional committee with subpoena power are also investigating. The U.S. Senate Democratic Leader, Chuck Schumer of New York, compared Equifax to Enron: "It's one of the most egregious examples of corporate malfeasances since Enron" and called Equifax's treatment of consumers afterward disgusting and its inability to protect data deeply troubling. He said Equifax's CEO and Board of Directors might need to resign if the company does not immediately take concrete steps to protect consumers and testify before lawmakers and federal regulators (Thomson/Reuters 2017). Another U.S. Senator, Elizabeth Warren of Massachusetts, called on the Equifax executives to return some of their compensation (Surane and Melin, 2017).

Another recent hack was similarly reported in September 2017 but was also first discovered in March 2017 although it may have occurred as early as October 2016. This cyberattack hit the entire email system and all administrative accounts of the global accounting company, Deloitte. The hack compromised a range of clients' data, including large Fortune 500 multinational companies and U.S. government departments. The breach occurred because one administrator did not have two-factor authentication, just

requiring a single password to sign in. Deloitte is one of the largest private U.S. companies and one of its lines of business is offering cybersecurity advisory services to major governments and large multinationals (CBS News 2017).

Another recent hack was also reported in September 2017 by the SEC. The 2016 hacking was on its online database of corporate filings, called the test Edgar system, which lets startup companies unfamiliar with filling out SEC forms get comfortable with the process before they do public announcements. These cybercriminals may have stolen corporate secrets and profited from having inside information ahead of public disclosures. This SEC hack disclosure was just two weeks after the Equifax hack disclosure and is triggering a renewed call for U.S. federal agencies and companies to do more to secure data. The SEC chairman said that the agency is working to increase public awareness of the "substantial systemic risks" associated with cybersecurity. A U.S. Senator, Mark Warner of Virginia, commented: "Information has become one of our country's most valuable resources and control of that information comes with significant responsibility." (Bain and Robinson 2017).

The May 2017 WannaCry ransomware cyberattack was worldwide, affecting over 300,000 computers in 150 countries in one day. It was linked to the Lazarus group of hackers who have links to the North Korean regime which has an army of 6,000 hackers. This attack used a ransomware crypto-worm which targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the bitcoin cryptocurrency. This attack led to losses of four billion dollars and suggested that North Korea is now using state-sponsored hackers to raise revenue to help counter its economic sanctions (Burton 2017). Shortly after the attack began on Friday, May 12, 2017, a web security researcher discovered an effective kill switch which slowed the spread of the infection and Microsoft issued a security update as well. As of May 19, 2017, the attacks had slowed down and are probably extinct although a newer virus version could be released (Wikipedia 2017).

In October 2016, a massive DDoS (distributed denial of service) attack slowed Amazon, Twitter, Netflix, Paypal, online newspapers, and many other websites to a crawl. The weapon was a Mirai botnet that was mostly made up of IoT (Internet of Things) devices, like security cams. In April 2016, the Russian hacker, Guccifer 2.0, hacked the servers of the Democratic National Committee (DNC). He then created a WordPress page and posted emails, memos, and other information from the DNC files which Wikileaks also published. Subsequent investigations by the FBI and various U.S. Congressional committees continue to this day (Castelluccio 2017).

In August 2016, almost 120,000 bitcoin worth $78 million were stolen from Bitfinex, an exchanged based in Hong Kong. In March 2016, about $81 million of Bangladesh's money disappeared out of its account at the Federal Reserve Bank of New York which used the SWIFT international bank messaging system, billed as a super-secure system that banks use to authorize payments. This attack was also attributed to North Korean hackers (Burton 2017). In contrast, it took the notorious American bank robber, Willie Sutton, 40 years to steal $2 million.

DESCRIPTION CRITERIA FOR CYBERSECURITY

Since description criteria can be used to explain an organization's cybersecurity risk management program, such criteria would be a common communication language and good starting point for an Audit Committee or a Cybersecurity Committee of the Board of Directors to assess the cybersecurity risks in their companies. The AICPA organized nineteen description criteria by nine general categories: nature of business and operations, nature of information at risk, cybersecurity risk management program objectives, factors that have a significant effect on inherent cybersecurity risks, cybersecurity risk governance structure, cybersecurity risk management process, cybersecurity communications and quality of cybersecurity information, monitoring of the cybersecurity risk management program, and cybersecurity control processes. These general categories and description criteria are elaborated as follows:

Nature of Business and Operations

1. The nature of the entity's business and operations, including the principal products or services the entity sells or provides and the methods by which they are distributed.

Nature of Information at Risk

2. The principal types of sensitive information created, collected, transmitted, used, or stored by the entity.

Cybersecurity Risk Management Program Objectives

3. The entity's principal cybersecurity risk management program objectives related to availability, confidentiality, integrity of data, and integrity of processing.
4. The process for establishing, maintaining, and approving cybersecurity objectives to support the achievement of the entity's objectives.

Factors that Have a Significant Effect on Inherent Cybersecurity Risks

5. Factors that have a significant effect on the entity's inherent cybersecurity risks, including the (1) characteristics of technologies, connection types, use of service providers, and delivery channels used by the entity, (2) organizational and user characteristics, and (3) environmental, technological, organizational and other changes during the period covered by the description at the entity and in its environment.
6. For security incidents that (1) were identified during the 12-month preceding the period end date of management's description and (2) resulted in a significant impairment of the entity's achievement of its cybersecurity objectives, disclosure of the following (a) nature of the incident; (b) timing surrounding the incident; and (c) extent (or effect) of these incidents and their disposition.

Cybersecurity Risk Governance Structure

7. The process for establishing, maintaining, and communicating integrity and ethical values to support the functioning of the cybersecurity risk management program.
8. The process for Board oversight of the entity's cybersecurity risk management program.
9. Established cybersecurity accountability and reporting lines.
10. The process used to hire and develop competent individuals and contractors and to hold those individuals accountable for their cybersecurity responsibilities.

Cybersecurity Risk Management Process

11. The process for (1) identifying cybersecurity risks and environmental, technological, organizational, and other changes that could have a significant effect on the entity's cybersecurity risk management program and (2) assessing the related risks to the achievement of the entity's cybersecurity objectives.
12. The process for identifying, assessing, and managing the risks associated with vendors and business partners.

Cybersecurity Communications and Quality of Cybersecurity Information

13. The process for internally communicating relevant cybersecurity information necessary to support the functioning of the entity's cybersecurity risk management program, including (1) objectives and responsibilities for cybersecurity and (2) thresholds for communicating identified security events that are monitored, investigated, and determined to be security incidents requiring a response, remediation, or both.
14. The process for communicating with external parties regarding matters affecting the functioning of the entity's cybersecurity risk management program.

Monitoring of the Cybersecurity Risk Management Program

15. The process for conducting ongoing and periodic evaluations of the operating effectiveness of key control activities and other components of internal control related to cybersecurity.

16. The process used to evaluate and communicate, in a timely manner, identified security threats, vulnerabilities, and control deficiencies to parties responsible for taking corrective actions, including management and the Board of Directors, as appropriate.

Cybersecurity Control Processes

17. The process for developing a response to assessed risks, including the design and implementation of control processes.
18. A summary of the entity's IT infrastructure and its network architectural characteristics.
19. The key security policies and processes implemented and operated to address the entity's cybersecurity risks, including those addressing the following:
    a. Prevention of intentional and unintentional security events
    b. Detection of security events, identification of security incidents, development of a response to those incidents, and implementation activities to mitigate and recover from identified security events
    c. Management of processing capacity to provide for continued operations during security, operational, and environmental events
    d. Detection, mitigation, and recovery from environmental events and the use of back-up procedures to support system availability
    e. Identification of confidential information when received or created, determination of the retention period for that information, retention of the information for the specified period, and destruction of the information at the end of the retention period

The eighth description criteria emphasized the Board of Directors' oversight of the entity's cybersecurity risk management program, as elaborated with three key points: 1) the extent of the Board of Directors cybersecurity and IT experience or access to external cybersecurity and IT expertise or both, 2) identification of the Board committee designated with oversight of the entity's cybersecurity risk management program, if any, and 3) the frequency and detail with which the Board or committee reviews or provides input into cybersecurity-related matters, including Board oversight of security incidents. These three points can be used to enhance corporate governance, concerning the Board of Directors' oversight of cybersecurity.

Also, to further strengthen corporate governance, the sixteenth description criteria is relevant: the process used to evaluate and communicate, in a timely manner, identified security threats, vulnerabilities, and control deficiencies to parties responsible for taking corrective actions, including management and the Board of Directors, as appropriate. Finally, the nineteenth description criteria with its five key potential risks can be used as an excellent cybersecurity review and executive summary by the Board of Directors.

CONTROL CRITERIA FOR CYBERSECURITY

Control criteria can be used to evaluate and report on the effectiveness of the controls within an organization's program. Such criteria would be a common communication language and comprehensive program for an Audit Committee or a Cybersecurity Committee of the Board of Directors to assess the cybersecurity risks in their companies after the description criteria have been assessed. The AICPA has developed control criteria, generally based upon its Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy. It used five general categories: control environment, risk assessment, control activities, communication and information, and monitoring activities which were elaborated by seventeen control principles from the Committee of Sponsoring Organizations of the Treadway Commission's (COSO) 2013 Internal Control—Integrated Framework. Finally, the AICPA used six additional cybersecurity control categories: logical and physical access controls, systems operations, change management, risk mitigation, availability, and confidentiality, which were not

specifically covered by the COSO internal control principles. All these general categories and COSO principles are elaborated as follows:

Control Environment

1. The entity demonstrates a commitment to integrity and ethical values.
2. The Board of Directors demonstrates independence from management and exercises oversight of the development and performance of internal control.
3. Management establishes, with Board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
4. The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
5. The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

Risk Assessment

6. The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
7. The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.
8. The entity considers the potential for fraud in assessing risks to the achievement of objectives.
9. The entity identifies and assesses changes that could significantly impact the system of internal control.

Control Activities

10. The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
11. The entity also selects and develops general control activities over technology to support achievement of objectives.
12. The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.

Communication and Information

13. The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.
14. The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
15. The entity communicates with external parties regarding matters affecting the functioning of internal control.

Monitoring Activities

16. The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
17. The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the Board of Directors, as appropriate.

Logical and Physical Access Controls

1. The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.
2. Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.

3. The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.
4. The entity restricts physical access to facilities and protected assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.
5. The entity discontinues logical and physical protection over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.
6. The entity implements logical access security measures to protect against threats from sources outside its system boundaries.
7. The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.
8. The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.

System Operations

1. To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.
2. The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.
3. The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.
4. The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.
5. The entity identifies, develops, and implements activities to recover from identified security incidents.

Change Management

1. The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.

Risk Mitigation

1. The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.
2. The entity assesses and manages risks associated with vendors and business partners.

Additional Criteria for Availability

1. The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.
2. The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up process, and recovery infrastructure to meet its objectives.
3. The entity tests recovery plan procedures supporting system recovery to meet its objectives.

Additional Criteria for Confidentiality

1. The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.
2. The entity disposes of confidential information to meet the entity's objectives related to confidentiality.

Corporate governance is strengthened by the second COSO control principle: the Board of Directors demonstrates independence from management and exercises oversight of the development and performance of internal control. The AICPA provided an additional point of focus for this second control principle: the Board of Directors supplements its expertise relevant to security, availability, processing integrity, confidentiality, and privacy, as needed, through the use of a subcommittee or consultants.

Corporate governance is also strengthened by the third COSO control principle: management establishes, with Board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives. The AICPA provided two additional points of focus for this third control principle: 1) management and the Board of Directors consider requirements relevant to security, availability, processing integrity, confidentiality, and privacy when defining authorities and responsibilities and 2) management and the Board of Directors consider the need for the entity to interact with and monitor the activities of external parties when establishing structures, reporting lines, authorities, and responsibilities. A brief summary of an entity's monitoring responsibility for cybersecurity is provided by the seventeenth COSO control principal: the entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the Board of Directors, as appropriate.

THREATS FROM QUANTUM COMPUTING

IBM now has three quantum computing systems that are online and open source at ibm.com/IBMQ for use by companies, universities, and other researchers. One IBM quantum computer researcher commented that quantum computers, with their exponential processing power, will be able to crack most encryption systems without breaking a sweat. Quantum computers will be able to crack sophisticated encrypted codes where you need to try a massive number of variables with an exponential number of possibilities (Friedman 2018).

For example, the Rivest-Shamir-Adleman (RSA) algorithm, which protects almost all e-commerce, relies on the simple math strategy of multiplying large prime numbers together. When the code numbers are much bigger, the problem scales polynomially in computer science terms. For hacking such a large number or code, you have to work the process in reverse to find which prime numbers or factors should be multiplied together to produce the code. Making the numbers or code bigger makes the problem much harder to solve as it scales exponentially. However, the power of a quantum computer could crack such a code or cipher that uses the RSA algorithm or an elliptic curve (EC) algorithm almost immediately (Kielpinski 2014 and Wood 2011).

Another quantum computing expert observed that quantum computing will instantly change the world of encryption and when someone has a quantum computer, no one is really going to feel safe anymore: "Your encryption will be useless against hackers with quantum computers. Forget about worrying if you need to change a password at a particular group of websites. Everything you send over the wire will be readable by the entity that gets a quantum computer first" (Cox 2014).

On August 16, 2016, China did launch the first quantum space satellite (QUESS). Its stated purpose is to build a worldwide network that can send messages that can't be wiretapped or cracked through conventional methods. A hacker trying to crack the message changes its form in a way that would immediately alert the sender and cause the message to be altered or deleted. QUESS will relay transmissions between two ground stations, one in China and the other in Europe with the Austrian Academy of Sciences providing optical receivers for European ground stations. Since government, military, corporate, and financial networks are appealing targets for espionage, as well as online shopping

hacking, quantum encryption promises to provide a level of potentially unbreakable encryption for such systems and a sure-fire method to detect any hacking attempts (Merchant 2016; Lin, Singer, and Costello 2016).

Raising the question of who's responsible for cybersecurity, two cybersecurity researchers observed: "Cybersecurity isn't a one-and-done task for the manufacturer, but a responsibility shared among everyone operating the device" (Rohrer and Hom 2017). Such responsibility extends to all the previously mentioned networks of government, military, corporate, and financial, as well as any online systems.

Accordingly, all the stakeholders involved in corporations and corporate governance should be responsible. To help with such responsibility, especially with respect to quantum computing security threats, the related AICPA cybersecurity description criteria could be used to help provide guidance: monitoring the cybersecurity risk management program (two criteria, numbers 15-16) and cybersecurity control processes (three criteria (numbers 17-19). Similarly, the related AICPA cybersecurity control criteria would be used to help provide guidance: risk assessment (four criteria, numbers 6-9), control activities (three criteria, numbers 10-12) and monitoring activities (two criteria, numbers 16-17).

SUMMARY

The dangers of not properly focusing upon cybersecurity risks were emphasized by recent, notorious attack and hack examples of Equifax, Deloitte, the Securities and Exchange Commission, the Federal Reserve Bank robbery, several massive DDoS (distributed denial of service) attacks, the WannaCry ransomware, and the Democratic National Committee hacking. With guidance from key sources, like this AICPA Cybersecurity Guide, cybersecurity strategies can be developed by corporate executives and Boards of Directors to help thwart such attacks and hacks. The design and control criteria and related procedures recommended by this AICPA Cybersecurity Guide could be used for a cybersecurity questionnaire by an Audit Committee or a Cybersecurity Committee of the Board of Directors in order to determine if an entity's cybersecurity objectives are being meet. An immediate need for data security is the General Data Protection Regulation, adopted by the European Union in 2016 and enforced on May 25, 2018. Corporate stakeholders also need to pay attention to the new cybersecurity threat of quantum computing. Accordingly, corporate governance would be strengthened by corporate executives and Boards of Directors who are the key gatekeepers for protecting and enhancing the investments of their shareholders and other stakeholders.

REFERENCES

American Institute of Certified Public Accountants (2017, May 1). *Guide: Reporting on an Entity's Cybersecurity Risk Management Program and Controls*, AICPA.

Bain, B., & M. Robinson (2017, September 20). *Hackers May Have Profited From SEC Corporate Filing System Attack*. Retrieved from bloomberg.com

Burton, J. (2017, August 15). *Cyberspace Aggression Adds to North Korea's Threat to Global Security*. Retrieved from theconversation.com

CBS Mews (2017, September 25). *Deloitte Hack Reportedly Hit Corporate, Government Clients*. Retrieved from msn.com

Castelluccio, M. (2017, January 1). The Most Notorious Hacks of 2016. *Strategic Finance*.

Chartered Global Management Accountant (2015, December 1). CGMA Cyber Security Risks Survey Data, *CGMA*.

Cox, J. (2014, September 18). *Your Encryption Will be Useless Against Hackers with Quantum Computer*. Retrieved from motherboard.vice.com

Friedman, T. (2018, January 16). While You Were Sleeping. *The New York Times.*

Huber, N. (2018, April 15). Six Steps to Comply With the GDPR. *CA Magazine*.

Kalinich, K. (2017, February 10). Should U.S. CFOs Worry About EU Cyber Risk Rules? *CFO.*

Kielpinski, D. (2014, February 11). Q*uantum Computers Could Crack Codes But Create Others Much Harder to Break*. Retrieved from theconversation.com

Koren, J. (2017, September 8). Equifax Execs Sold Shares Before the Hack was Announced—But was it Insider Trading? *Los Angeles Times*.

Lin, J., Singer, P., & Costello, J. (2016, March 3). China's Quantum Satellite Could Change Cryptography Forever. *Popular Science*.

MarketWatch (2017, October 5). *Insider Actions for Equifax*.

McCallister, J., Zanfir-Fortuna, G., & Mitchell, J. (2018, January 1). Getting ready for the EU's Stringent Data Privacy Rule. *Journal of Accountancy*.

McKenna, F. (2017, October 3). *Equifax Auditors Are on the Hook for Data Security Risk Controls.* Retrieved from marketwatch.com

Merchant, N. (2016, August 16). *China's Launch of Quantum Satellite Major Step in Space Race*. Retrieved from phys.org/news

Riley, M., Sharpa, A., & Robertson, J. (2017, September 18). *Equifax Suffered a Hack Almost Five Months Earlier Than the Date It Disclosed*. Retrieved from bloomberg.com

Rohrer, K., & Hom, N. (2017, October 1). Who's Responsible for Cybersecurity? *Strategic Finance*.

Surane, J., & Melin, A. (2017, September 26). *Equifax CEO Richard Smith Resigns After Uproar Over Massive Hack.* Retrieved from bloomberg.com

Thomson/Reuters (2017, September 14). *Schumer Compares Equifax to Enron: Disgusting, Deeply Troubling*. Retrieved from newsmax.com

Tysiac, K. (2017, April 26). A New Cybersecurity Risk Management Reporting Framework For Management and CPAs. *Journal of Accountancy*

Wikipedia (2017, May 22). *WannaCry Ransomware Attack*.

Wood, L. (2011, March 21). *The Clock is Ticking for Encryption*. Retrieved from computerworld.com