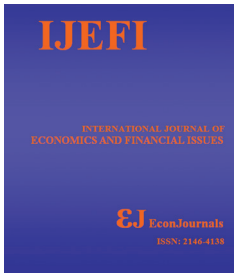

International Journal of Economics and Financial Issues

ISSN: 2146-4138

available at http: www.econjournals.com

International Journal of Economics and Financial Issues, 2020, 10(1), 27-32.

Emerging Technologies and Implications for Financial Cybersecurity

Sean Stein Smith*

City University of New York – Lehman College, American Institute for Economic Research, USA.
*Email: sean.steinsmith@lehman.cuny.edu

Received: 10 September 2019 **Accepted:** 24 November 2019 **DOI:** https://doi.org/10.32479/ijefi.8844

ABSTRACT

Emerging technology tools, such as blockchain, cryptoassets, robotic process automation, and artificial intelligence continue to change and influence the economic landscape at both a macro level and in different professional sectors. Pointedly, cybersecurity – far from being reduced in importance or relegated to secondary importance – continues to factor as a core consideration for management professionals. Accounting and financial services practitioners at large have long played a role in advising clients on technology matters as well as integrating technology into internal processes. As technology integration continues to accelerate, and fundamentally change how business processes function, practitioners must be able to assess and explain the implications of these tools on both internal and external processes. Written with both a practitioner and academic audience in mind, this research also leaves the door open for future research, analysis, and discussion.

Keywords: Blockchain, Cryptoassets, Robotic Process Automation, Artificial Intelligence, Cybersecurity
JEL Classifications: G, M

1. INTRODUCTION

As emerging technologies, which include but are not limited to blockchain, cryptoassets, robotic process automation (RPA), and artificial intelligence (AI) continue to permeate the business landscape and become increasingly integrated into mainstream business conversations the importance of implementing and establishing effective cybersecurity controls also continues to increase (EY, 2018). Possibly not a traditional area of expertise or competence for accounting and financial professionals, the importance of cybersecurity is difficult to overstate in the current business environment. Technology consulting has long played a role in the operations of accounting firms, but the focus on cybersecurity advice and guidance has become increasingly elevated in importance. Merely a cursory examination of headlines and other information connected to data management, consumer data, and the risks of hacks and other breaches reveals a plethora of instances in which cybersecurity protocols and controls have come to the forefront. Accounting and financial services professionals, already tasked with the maintenance and management of various internal systems and processes, continue to become immersed in both technology specific and business implications of technological change. This research and analysis, not meant to form an all-exhaustive nor all-inclusive analysis, should instead rather be used to form the basis of a more robust and comprehensive analysis moving forward.

2. EMERGING TECHNOLOGY AND CYBERSECURITY

Technology and technology integration are not anything new for the accounting and financial services profession; practitioners continuously have redefined and rebuilt policies and workflows across different industry lines. Given how disruptive the recent crop of technologies seems to be, however, it appears logical to

revisit the emerging technologies as well as how these tools are positioned to change the accounting conversation. Beginning with a brief definition of these tools and then continuing to the cybersecurity implications of these tools is a logical methodology through the technology and business implications can be examined. Regardless of whether or not a practitioner is employed within public accounting or private industry a core value proposition and accounting and financial services professionals is the control and custody services that are able to be offered (Brazina et al., 2019). It would seem that emerging technology tools, offering both the possibility of increases in automation and embedding encryption at the core of the product offering, reduce the need for a focus on cybersecurity. That said, it is worth pointing out that alongside the rise of said technology tools and platforms also is an increasing focus and importance placed upon cybersecurity control protocols.

2.1. Blockchain

Blockchain, widely discussed and analyzed across accounting and other industry verticals, is – at the core of the idea – a decentralized and distributed technology platform to store and share information between different network members. In addition to the decentralized underpinnings of blockchain, the encryption and consensus methodology commonly associated with blockchain form a core value proposition of why organizations seek to implement a blockchain or blockchain augmented platform. Given the strength of blockchain encryption and data security, there does appear to be some confusion as to how to correctly classify the status of this encryption; immutable versus tamper resistant. The original blockchain, the bitcoin blockchain that spurred the entire blockchain ecosystem, may indeed be thought of as an immutable record due to the fact that it has been not hacked or breached as of this research. A permissionless blockchain, such as the bitcoin blockchain, however, does not represent the iteration of blockchain that most commonly ends up being implemented at various institutions.

Permissioned blockchains, taking the form of either private or consortium blockchain models, are the most common application and version of blockchain that is implemented across industry lines. The differentiation becomes more important as blockchain technology and platforms are augmented and combined with other technology tools in a fast changing operational and regulatory landscape (Tashea, 2018). As the original blockchain code is edited, however, it is important to note and prevent the editing and tweaking of the blockchain code to accidentally undermine the core value proposition; data security and encryption. These edits and tweaks to the blockchain code are launched to improve the efficiency and speed with which data can be processed, but these business benefits also increase the risk of cybersecurity and operational failings.

- Blockchain cybersecurity takeaway. Even though blockchain is arguably most well know for (1) bitcoin, and (2) the encryption and security at the core of the technology platform, that does not mean that cybersecurity can take a back seat or reduced role. Rather, due to the technical complexity of many blockchain tools, and the lack of experience individuals and institutions have with connecting blockchains to other enterprise resource planning tools, blockchain may inadvertently increase cybersecurity. More to the point, colleagues and clients may not even realize some of the risks being undertaken due to the nascent and developing nature of the technology ecosystem. These risk, and potential misinformation that exists in the marketplace, presents an opportunity for practitioners to deliver quantifiable business benefits and insights to clients.

2.2. Cryptoassets

Cryptoassets are a related technological concept to blockchain technology and are possibly how most practitioners were first introduced to the blockchain ecosystem and marketplace. From an accounting perspective, there are also additional considerations that need to be factored into the analysis related to the accounting taxonomy conversation. Analyzing this question, both in the context of cybersecurity as well as on a standalone basis, also raises issues linked to custody and cybersecurity considerations especially from a risk mitigation perspective (Bruno and Gift, 2019). Regardless of what ultimately comes out of the accounting classification and taxonomy conversation, there is one core concept that needs to be resolved and finalized. Custody and provenance are both key considerations from a valuation and legalistic perspective but is also something that should be built into any cybersecurity conversation linked to cryptoassets.

Building on this fact, being able to prove and verify custody and provenance of certain assets is an imperative step toward building out a more comprehensive cybersecurity conversation. What makes this a key factor in the cybersecurity conversation and dialogue is the fact that cryptoassets – in addition to representing a hybrid or arguably a new class of assets – also do not have many characteristics of more traditional assets. Specifically, the fact that cryptoassets are bearer instruments increases the importance of developing and implementing robust cybersecurity policies. Put another way and given the reality that there are not widely available cryptoasset insurance policies, and that most cryptoassets are not eligible for FDIC or other types of investor protection, or even reporting these risks, the importance of cybersecurity in this context is increasingly important when it comes to safeguarding and protecting cryptoassets (Nallengara et al., 2018).

- Cryptoassets are perhaps the area in which cybersecurity is most directly impacted by emerging technology, because cryptoassets seem to have combined the issues connected to blockchain and the lack of legal finality in the emerging technology space at large. The lack of recourse in the case of losses, hacks, or breaches for many cryptocurrencies or cryptoassets also exposes individuals or institutions to direct losses with limited possibilities for reimbursement either now or going forward. Since many of the most high-profile breaches and hacks in the broader blockchain space have been focused in the cryptocurrency area, this is not a theoretical or academic concern. Interestingly, the very decentralized and distributed nature of many first-generation cryptocurrencies that generated so much initial interest also seem to be the very same reasons that new iterations and applications in the crypto space continue to develop.

2.3. RPA and AI

AI may represent the potential future of many business processes, but the underlying reality is that most organizations are not

prepared enough for a full-blown AI program. Some may suspect that this lack of preparedness is connected to the technical training or understanding of the tools themselves, and while that is a contributing factor, it is only a partial view of the situation. An important first step in the development and implementation of any automation program, be it connected to a specific theme such as RPA or more generally linked to automation, is the documentation that must precede any successful adoption or implementation. A realization such as this highlights just how important it is for financial professionals, including CPAs, to learn and understand AI applications and use cases (Cieslak et al., 2019). Appropriate documentation is, of course, important from a risk management perspective and point of view but is also something that should be noted through a cybersecurity lens and framework. Specifically, as ever larger components and pieces of processes are either automated altogether or augmented via the integration of automation technologies, there rises the risk of auditors and accounting professionals losing visibility into how these processes function.

Cybersecurity, however, is not simply connected to a specific new technology tool or platform that is being implemented at a number of organizations, but also focuses on how different technology systems and platforms interact with each other. Returning the focus of the conversation back to emerging technology tools, it does seem that many of the hacks, breaches, and data failures have not occurred at the epicenter of the tools themselves, but rather at the proverbial on-ramps and off-ramps enabling these differentiated tools and systems to connect with currently technology platforms. Drilling down to the implications of these trends, alongside the broader focus on automation that already exists, there appear to be several implications for auditing and accounting professionals that need to be incorporate into assurance and attestation practices.

- Cybersecurity takeaway. Automation is not a new force in the accounting or financial service space, but as the integration of said technologies continue to increase it does seem logical to revisit some of the cybersecurity implications of increasing automation. Most notably a key factor that should be incorporated into any risk management plan are the risks connected to the lack of transparency that can result. Stated another way, the documentation and check points surrounding a process and especially those in place at the beginning and ending of the process must be updated to help ensure that processes continue to operate as necessary.

3. IMPACT ON ACCOUNTING

It is important to, prior to an analysis as to how these emerging technologies are impacting cybersecurity and particularly how cybersecurity connects to attestation engagements, note that cybersecurity is broader term that might otherwise be construed. Not only does cybersecurity pertain to data security themes such as phishing and malware, but also are connected to must of the value delivered by accounting practitioner not employed in public accounting. Public accounting firms, particularly the Big 4 (Deloitte, PwC, EY, and KPMG) tend to drive numerous conversations forward in the broader accounting space, but these conversations and perspectives only represent one subset of the accounting field. Accounting practitioners employed within industry must contend with the operational reality as to how technology tools actually drive change connected to both organizational processes and how those processes are examined by external partners.

Arguably the most direct impact that emerging technologies will have on an organization and accounting functions within organization are by directly impacting that types of work completed by practitioners. For example, if distributed ledgers and different automation tools are integrated into how information is processed, this reduces the need for some work that includes, but is not limited to, reconciliations, confirmations, and affirming the valuation of various assets and information (Alarcon and Ng, 2018). The elimination, or reduction in importance of, some roles and tasks traditionally performed by accounting professionals, has caused some level of anxiety within the profession. From reducing the need for total accounting employment, to depriving new entrants into the profession of tasks necessary to build professional competence, to the rise of advisory firms headed by non-accountants handling some tasks, these fears are not completely unfounded. On the opposing side of this view, however, is the reality that for every tasks or process changed or augmented by emerging technologies, there are opportunities for motivated practitioners to develop new advisory opportunities.

A trend that must be acknowledged, however, and realizing that some new roles and opportunities will develop and emerge, is that the accounting and financial services landscape will change. Roles will be eliminated, firms will struggle, and there might even eventually be a reshuffling of the current order in terms of how certain firms engage with both regulators and other peers. It may, ultimately, result in a bifurcation of accounting and financial services organizations between those individuals and firms that embrace and utilize emerging technologies and those that do not. The sense of anxiety and angst common in some conversations and analyses is a realization of the numerous effects that increased automation, digitization, and efficiency will have on the broader economy. Weighing these potential negative effects against the opportunities and potential for increased growth provides a more complete picture and analysis of just what emerging technologies will drive to the forefront.

3.1. New Potential Roles

Prior to identifying potential best practices linked to cybersecurity it is important to realize that one potential impact of emerging technologies on the broader accounting and financial services space are the new roles that may eventually manifest in the marketplace. Notably, it is important to realize that some of the same technology tools – such as RPA and/or AI – can also assist in the design and implementation of cybersecurity policies and controls (Fearn, 2018). While it is difficult to forecast exactly how increased adoption of blockchain and other technologies will influence job creation and modification, there do appear to be several general areas in which practitioners will have new opportunities to deliver insights.

First, and especially as permissioned blockchains – be they private or consortium iterations – become more widespread in the

marketplace, these networks will require some additional controls and policies to assist in ensuring operational effectiveness. Since not every member of a permissioned network should have equal access, or full access, to the data stored and transmitted on the network itself, this requires a robust a set of controls. Notably, and even acknowledging that permissioned blockchains do tend to have higher level of trusts almost by the nature of these iterations, it is unlikely that members want to trust all monitoring to a fellow member. Even in the situation where an institution – such as Walmart or JP Morgan – originates and develops the idea, as the network matures it is reasonable for other members to expect some impartiality with regards to which institutions have access to network data. Accounting and attestation professionals have a unique opportunity to fill this role; serving as an independent auditor or consortium access lies within the wheelhouse of current professional competence while embracing the changing needs of the marketplace (Tysiac, 2016). From an operational point of view this could take the form of assisting in the creation and implementation of policies to (1) add members to the network, (2) remove certain members if necessary, and (3) grant and monitor which members have access to which subsets of information.

Second, and highlighting the importance of smart contracts to the success or failure of blockchain implementation at large, there does seem to be a need for increased standardization and clarification for how smart contracts interact with wide technology systems. It is worth remembering that no blockchain, whether or not it is permissionless or permissioned in nature, is not able to interact and transmit data by itself. Blockchains represent a static record of information or transactions that have previously occurred, but by itself a blockchain network is unable to interact or interoperate in a significant manner. Smart contracts, rather than the blockchain itself, represents the programmable and executable code language and tool that enables blockchains to take action, be utilized for enterprise applications, and interoperate with a wider array of technology systems (Stampone and Marcy, 2019). Contracts, no matter if they are considered smart or traditional in nature – all while realizing that smart contracts are translations and interpretations of traditional contracts – do occasionally suffer from an array of issues. Erroneous interpretation, disagreements as to how certain terms and items are executed, or even simple obsolescence due to the passage of time or other business facts can hamstring previously appropriate and accurate arrangements. Given the fact that smart contracts are designed to execute and fulfill agreements with limited human involvement and interaction, the importance of controls and policies to assist in ensuring successful implementation seems an appropriate role for accounting and attestation professionals.

No matter what specific tools and roles are developed, and remaining focused on blockchain implementation at this point, the importance of maintaining independence during the development and implementation of these policies is imperative. As accounting and attestation professionals continue to build out and develop necessary controls and protocols to document and secure blockchain augmented information, steps must be taken to prevent these protocols from encroaching on the prerogatives of management to make business decisions. While it is logical to conclude that accounting and attestation professionals will work with management to develop and implement necessary controls it is important to remember that the responsibility of said controls remains with management. Even in situations where attestation practitioners assist with arbitration or dispute resolution, care must be taken to ensure that the driving force behind this engagement remains with management and not the accounting or attestation partner.

3.2. RPA and AI Applications

Automation and driving process improvements do not represent new trends or themes in the financial services space, but the rise of increasingly sophisticated automation tools such as RPA and full blown AI suites is looking as if it will lead to an increased need for controls, protocols, and perhaps reworking of current processes. Specifically, for every process that is partially automated or augmented through increased integration of technology tools and platforms there is the possibility that these automated steps can operate incorrectly. Turning to practitioners employed within industry, the ability to maintain transparency and visibility into just how these tasks currently function – both before and after automation – is necessary to enable practitioners to not only answer application questions but to also continue producing reports and analyses (Banham, 2017). Practitioners employed in an external consultative role, on a related note, will have to test and develop new types of tests, analytics, and other substantive procedures to gain visibility and satisfaction with how this automation functions.

Coupled with the rise in the sheet quantity of information produced and generated by most enterprises, the opportunity of enhanced automation to facilitate accelerated decision making is tangible. By the same token, and as decision making is accelerated and increasingly automated, it is also worth realizing that the incorrect processes, or faulty documentation and workflow construction can hamstring even the most well-intentioned automation concepts and proposals. Given the importance of data protection and cybersecurity, while also realizing there is no one size fits all toolkit, preparing a checklist of factors to consider and integrate to a cybersecurity program makes sense both from a practitioner and client perspective.

4. CYBERSECURITY CHECKLIST

Emerging technology tools will inevitably have an impact on virtually every firm in the marketplace, regardless of whether or not any one specific institution is an active investor or early adopter of these technologies. Alternatively, and what is already beginning to occur to a certain extent, is that as larger organizations adopt and implement emerging technology tools, these platforms and processes are increasingly passed down through supply chains and other vendor relationships. Be it the implementation of blockchain by Walmart for fresh leafy green suppliers, the Interbank Information Network spearheaded by JP Morgan, or the TradeLens logistics blockchain developed in coordination between IBM and Maersk, the trend toward increased commercial blockchain adoption seems to be accelerating. In addition to the blockchain specific implementations, the rise of more affordable automation products in the RPA and full AI space are also creating

an environment where the increasing amounts of organizational data can be analyzed and reported on a nearly continuous basis. These questions and challenges, in addition to creating obstacles toward final implementation, also generate job and revenue opportunities for practitioners will to learn and evolve alongside the marketplace (Dickson, 2017). That said, it seems reasonable to assemble a checklist or proposed best practices that accounting and financial service professionals should take into account as the cybersecurity conversation and debate continues to evolve and develop. Not meant to be presented as an exhaustive or authoritative listing of factors, these items should form the basis for a more robust and comprehensive conversation going forward.

1. Identifying processes and certain tasks that can be streamlined, augmented, or otherwise improved via emerging technology tools. It is worth pointing out that not every process or task is going to as equally as good a fit for new technology tools as others. In fact, given the nature of some tasks – especially if they are bespoke or customized by nature, increasing the automation and data dependency of the processes may actually prove to be a hinderance rather than a benefit. Technically not connected to cybersecurity considerations or plans, being able to effectively pick out and select specific sub-processes to experiment with also provides an ancillary benefit. Limiting the exposure and scope of processes to be subjected to changing with new technology tools also means that, before and after the implementation, observations are able to be conducted consistently
2. Subsequent to identifying the specific processes, a critical next step for both the development of new technology policies as well as effective security measures associated with these technology platforms is the comparison of the process both before and after the changes. Processing data more efficiently does not always mean that the end result of the augmented task or workflow is superior to the previous one. In many cases an accelerated or more efficient data processing structure will be superior, but in order to (1) evaluate the effectiveness of the technology upgrade, and (2) understand the cybersecurity implications of this platform there must be an objective analysis as to how the task or function is actually performing on a before and after basis
3. Controls should be upgraded and updated to reflect the changing reality of cybersecurity in the face of new technology processes and option. By the very nature of how technology integrates with workflows and internal processes the development and rolling out new technology tools will have an impact on how information is treated from both an internal and external perspective. That said, as the processes themselves change and are modified as a result of technological integration it also seems logical and necessary to forecast that controls and control processes will also have to evolve
4. Core functionalities and service offerings will continue to evolve and change as cybersecurity becomes an increasingly high-profile topic and area of both concern and opportunity for organizations. For example, the entire premise of a SOC 1 and SOC 2 engagement – both attestation affiliated services that analyze internal controls, reporting functions, and technology systems – will evolve and mature by default in response to the changing needs and expectations of the marketplace. While some of the current functions and tasks that comprise these and other technology engagements will be automated to some extent, an underlying reality is that new ones will also have to be developed
5. Closing the loop on employee and client feedback. As with any new technological implementation there are going to be successes, failures, and opportunities for current iterations to be tweaked as adoption and implementation accelerates. Obtaining feedback from both front-line employees tasked with using new technology tools and processes as well as technology experts maintaining the systems on the back end is an important first step. Arguably more important, however, is the ability of practitioners to close the loop and address concerns – related to cybersecurity specific items or not – to help ensure that new technology tools and platforms operate as advertised.

5. ADDITIONAL CONSIDERATIONS

When proposing or hypothesizing new potential service or revenue opportunities it is important to realize that implementation and adoption of emerging technologies will occur at varying rates at different organizations. Despite this, practitioners do have a professional and fiduciary duty to understand both the technology itself as well as the implications these tools will have on internal processes. This variety of processes and implementation considerations do generate some headwinds for practitioners seeking to provide guidance, will also create additional opportunities for practitioners. For example, even if a small or medium size enterprise are not directly involved in a robust implementation or emerging technology tools these same enterprises might be part of supply chains led by larger organizations that are indeed doing just that (McLane, 2018).

Examples such as Walmart and JP Morgan are prime examples of how large multinational organizations are pushing adoption and implementation of these emerging technologies forward. Arguably the role that accounting and attestation practitioners can play in such a situation is more important than during a standalone implementation project. Since an enterprise is joining a pre-existing network or technology structure the themes of interoperability and controls between these different networks and systems are elevated to even higher levels of importance. Since many of the weak points in technology system lie at the joints or points of overlap between different technology systems it makes sense that integrating different organizations and technology systems would be an area of focus for both management and financial services practitioners.

Bridging the gap and making the pivot from compliance reporting and to more of an advisory role and capacity is a shift and change that has been oft repeated as the goal of many accounting and attestation firms. In fact, the fastest growing area for virtually every firm operating in the broader accounting space has been advisory services, and cybersecurity would certainly seem to fall into this category. Undertaking these projects, however, is not without risk for either the practitioner or firms that are leading

these engagements, not the least of because the standards and guidelines for cybersecurity practices are still evolving (Miller, 2019). Specifically, the lack of blockchain and cryptoasset insurance policies or coverage represents a significant risk, and financial exposure, for organizations seeking to offer services in this space. Even in more traditional areas such as cybersecurity services and offerings the importance of obtaining cybersecurity insurance policies is difficult to overstate (Shelhart, 2018). The numerous failings and other hacks and breaches that have occurred – both in emerging technologies as well as a more well-established firms and service lines – illustrates just how uncertain and nascent this type of service offering can become.

Clearly obtaining appropriate insurance, or even simply advising clients on the type of insurance and coverage to obtain as emerging technology is something that can deliver quantitative and qualitative benefits to the organization (Hayton, 2018). With the total global insurance market totaling trillions in total activity and value according to recent data this is not merely an academic or conceptual argument; it is core to how a business functions. Particularly as clients continue to embrace and implement emerging technology tools and platforms in different aspects of the business; front office, back office, and supply chain operations, understanding how these tools intersect with current functions is increasingly important. It is true that advising clients on either developing or purchasing appropriate cybersecurity policies, or insurance products linked to blockchain and cryptoassets, will most likely not form the majority of business operations it is worth illustrating the importance of having said conversations. Whatever the case may be, or how the interactions between certain firms and clients continue to develop, it seems clear that these conversations and engagements will need to evolve, develop, and become increasingly multi-faceted.

6. FUTURE DIRECTIONS

Emerging technology, by its very nature, is difficult to predict and forecast due to how fast moving and rapidly changing this tools and platforms are in terms of products and services. Accounting and financial services have a long track record of successfully integrating technology tools into service offerings and client advice, but the acceleration of technological integration does seem to provide an array of opportunities and challenges for both practitioners and organizations. Regardless of the specific tools analyzed and examined, however, the importance and implications of cybersecurity from both an operational and risk management perspective is difficult to overstate. Including a range of options, from relatively straight forward updating and improving of internal controls and cybersecurity policies, to the integration of blockchain into a supply chain network, generate numerous implications from a cybersecurity perspective. Accounting practitioners will, and already are, facing increased competition from a number of new entrants into this marketplace; this trend does not appear to be a passing fad but rather a fundamental change in the business landscape. Cybersecurity is a core business function in the modern economic landscape, and is something that the profession is realizing will create negative and positive second and third order effects. Embracing these technology tools, understanding how these tools function, and being to articulate this and other information to clients and colleagues will continue to be a differentiating factor moving forward. No matter how the emerging technology and cybersecurity conversation plays out, it is clear that cybersecurity is changing, the profession is changing, and there is a plethora of ideas and concepts to spur and support future research.

REFERENCES

Alarcon, J.L.J., Ng, C. (2018), Blockchain and the future of accounting. Pennsylvania CPA Journal, 2018, 3-7.

Banham, R. (2017), Cybersecurity: A new engagement opportunity: An AICPA framework enables CPAs with cybersecurity expertise to perform new services for clients. Journal of Accountancy, 224(4), 28-32.

Brazina, P.R., Leauby, B.A., Sgrillo, C. (2019), Cybersecurity opportunities for CPA firms. Pennsylvania CPA Journal, 2019, 1-5.

Bruno, D.T., Gift, L. (2019), How businesses can deal with cryptocurrency risks. Intellectual Property and Technology Law Journal, 31(3), 20-22.

Cieslak, D., Mason, L., Vetter, A. (2019), What's "critical" for CPAs to learn in an AI-powered world. Journal of Accountancy, 227(6), 1-6.

Dickson, B. (2017), Artificial Intelligence Creates New Job Opportunities. PC Magazine. p114-122.

EY. (2018), Understanding the Cybersecurity Threat: The Board's Role. Vol. 26. New York: Corporate Governance Advisor, 9-17.

Fearn, N. (2018), Tap the Seeing Power of AI for Cyber Defence. United Kingdom: Computer Weekly.

Hayton, R. (2018), Finally, a simple way to secure the internet of things: Blockchain and digital holograms™. Wireless Design and Development, 26, 8-9.

McLane, P. (2018), Cybersecurity: Every enterprise is at risk as attacks diversify and adversaries get smarter. Mix, 42(7), 10-48.

Miller, M. (2019), A new realm of auditing: Minimizing litigation risk in cybersecurity audits. Accounting Today, 33(5), 1-5.

Nallengara, L., Alsop, R., Halbhuber, H. (2018), SEC adopts interpretive guidance on cybersecurity disclosures. Computer and Internet Lawyer, 35(10), 18-25.

Shelhart, M. (2018), Why cyber defenses are worth the cost. Journal of Accountancy, 226(5), 1-8.

Stampone, A.L., Marcy, A.S. (2019), Emerging technologies will impact more than office duties. Pennsylvania CPA Journal, 2019, 11-13.

Tashea, J. (2018). What do AI, blockchain and GDPR mean for cybersecurity? ABA Journal, 104(12), 1-4.

Tysiac, K. (2016), New path for CPAs in cyber risk management. Journal of Accountancy, 222(5), 1-2.