Cyber Security: A Paradigm Shift in IT Auditing

How to Deal with Cyber Security Risks in the Financial Statement Audit

Michiel van Veen MSc RE CISA CISSP CRISC

With the fast increase of cyber crime, companies are regularly being compromised by hackers. In many cases this is to extract value (money, information, etc.) from the company or damage the company and disrupt business processes. These cyber security incidents not only impact the business, but also impact the financial auditor. After all, the financial auditor verifies the veracity of the financial figures as presented in the annual report. This article is to help both financial auditors and IT auditors to take account of *relevant* cyber security risks and determine the impact on the financial statement. "Cyber in the Audit" provides a framework and guidance for a structured approach and risk-based decision making for assurance.

Introduction

Each year cyber crime is growing stronger and stronger. This is clearly demonstrated by the increase of cyber security incidents, for example the increasing occurrence of ransomware. In addition, we see a further maturing and professionalization of cyber criminals, for example, by considering the emergence of cyber-crime-as-a-service business models that they use. In 2013 the global costs associated with cyber crime were around 100 billion dollars, increasing in 2015 to around 400 billion dollars. Continuing to rise steeply, the cyber crime cost prediction for 2017 is 1 trillion dollars, increasing to a staggering 6 trillion dollars in 2021 globally ([CybV16]). This is serious.

At board level, this trend does not go unnoticed. As such, we see that companies' boards include cyber security risks in their top five of most important business risks ([MTRe16]). After all, most companies are completely dependent on a continuously and properly operating IT environment. This not only applies to the availability of the IT environment, but it also applies to the confidentiality of sensitive data (e.g. intellectual property and data privacy) and the reliability of the (financial) data. A disruption of the confidentiality, integrity or availability of digital data has an increasing impact on the performance and operating income of the business. This is not limited to the classic office automation, but also needs consideration regarding automated production facilities (Industrial Internet of Things like SCADA environments) and consumer devices (e.g. healthcare and automotive), for example. It is estimated that a total of 6.4 billion devices will be connected by the end of 2016 ([Gart15]). That almost equals the amount of people on this planet. Because of this "hyper connectivity" trend, the traditional IT environment of companies is stretched further and further in the public internet through automated supply chains and sourcing partners. This makes adequately controlling the IT environment and its data inherently complex.

M. van Veen MSc RE CISA CISSP CRISC
is a senior manager at KPMG Cyber and a cyber security specialist.
vanveen.michiel@kpmg.nl

The Relevance of Cyber Security Risks for Financial Auditors

Cyber security risks not only impact the business, but also impact the financial auditor. After all, the financial auditor verifies the veracity of the financial figures as presented in the annual report. Just like the company itself, the financial auditor strongly relies on the continuity and reliability of automated data processing. Unsurprisingly, this has been part of the Dutch Civil Code (2:393.4) for decades: "*At least he (the auditor) shall make mention of his findings about the reliability and continuity of computerized data processing.*" ([DCC])

Traditionally, the financial auditor relies on the testing of so-called General IT Controls (GITCs). To thoroughly understand what IT auditors are actually testing, an exam-

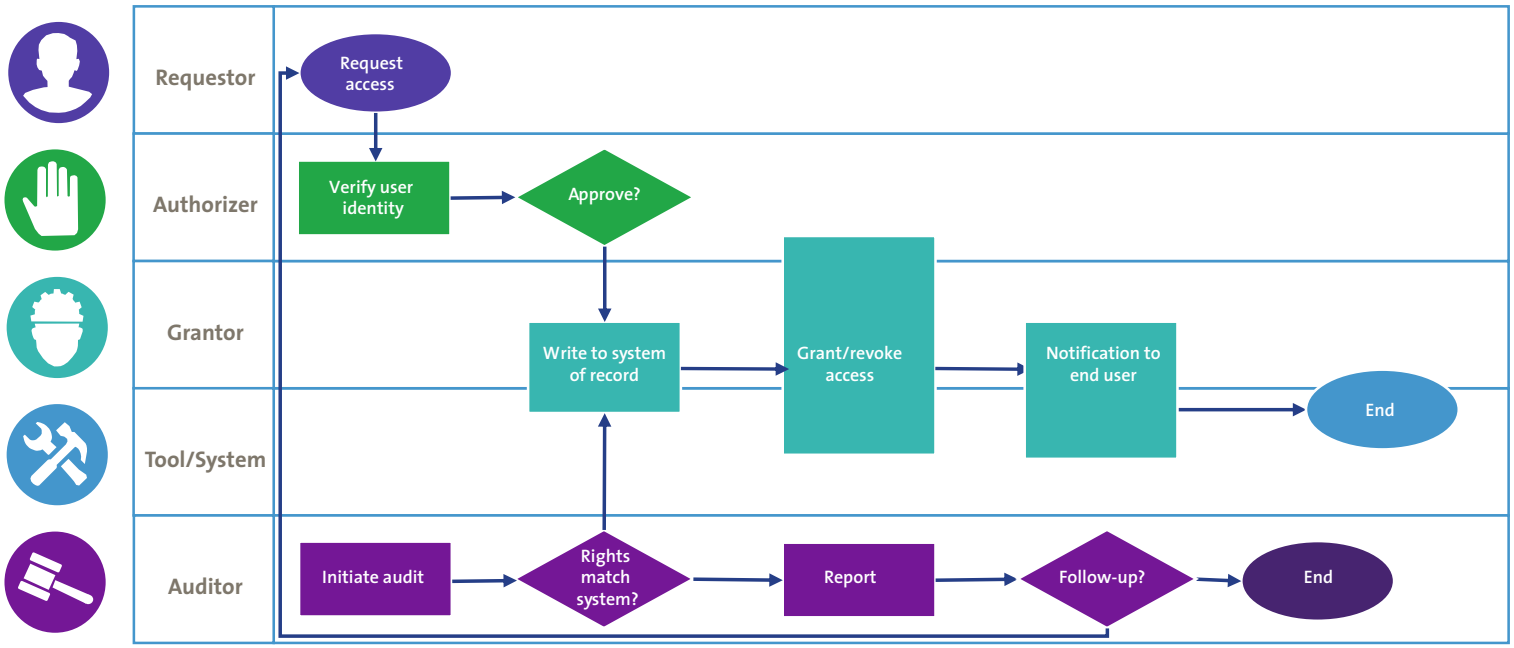

Figure 1. **User access management process example (ITIL).**

Figure 2. **Access management process of a cyber criminal.**

ple is provided in Figure 1 that illustrates the user access management process (ITIL in this example).

In Figure 1 one can identify the different roles in the access management process which execute IT controls, for example when a person requests access to the data in the IT environment. When conducting an IT audit, an IT auditor tests the controls in this process to determine their effectiveness in design and operation. If these controls are operating effectively, a financial auditor acquires additional reasonable assurance (on top of their own control testing in the financial processes) that the integrity of financial data is ensured.

However, here is the flip side: if we take a look at the approach that a cybercriminal would take to acquire access to the data in the IT environment, this is a very different process (see Figure 2).

It is clear that there are no controls in the process as shown above. Without any approval, registration and verification, a cyber criminal can acquire access to all IT applications and (financial) data in the IT environment. In fact, the cyber criminal bypasses all internal control measures implemented in the IT applications and IT infrastructure. In addition, a cyber criminal will cover (erase) its tracks to avoid being detected by audit logging & monitoring activities for example.

Financial auditors rely on the integrity of the data a cyber criminal can change. What does that mean for the integrity of financial data in this situation?

Acknowledging this risk, the PCAOB issued guidance on cyber security risks last year. Recently, the Netherlands Institute of Chartered Accountants (NBA) published a public management letter underpinning the importance

of considering this risk when perform FSAs. Furthermore, regulators are increasingly focusing on cyber security risks in their sector such as the Dutch Central Bank (DNB) in the financial sector.

In 2014, the AICPA (American Institute of Certified Public Accountants) issued CAQ Alert #2014-3 addressing the cyber security topic in the context of the External Audit ([CAQ14], [AICP14]). Unfortunately, no framework or practical approach was given. In addition, AICPA wrongly depicts the "typical access path to systems" and translates this into the wrong conclusion that the order of focus should be from application down to database and operating system, leaving out the network (perimeter). Instead, the auditor should consider the IT objects on the access path from an IT user (employee, hacker, etc.) to the data.

Just one month ago, AICPA started the "Cybersecurity Initiative", to develop criteria that will give management the ability to consistently describe its cyber risk management program, and related guidance to enable the CPA professional to provide independent assurance on the effectiveness of the program's design via a report designed to meet the needs of a variety of potential users ([Tysi16], [Whit16], [AICP16]). At the time of writing, the two criteria documents are still in draft. The proposal comes with an extensive list of cyber security related controls. The long list of controls is not efficiently tailored for an FSA.

At the same time, the IFAC (International Federation of Accountants) states that the effect on financial statements of laws and regulations varies considerably. As such the risk of fines for non-compliance (NOCLAR) increases. Non-compliance with laws and regulations may result in fines, litigation or other consequences for the company that may have a material effect on the financial statements ([IFAC16a], [IFAC16b]).

Such laws and regulations are proposed by the EU and implemented by the EU member states as well strengthening Europe's cyber resilience. In 2013 the Commission put forward a proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union. The Directive on the security of network and information systems (the NIS Directive) was adopted by the European Parliament on 6 July 2016. The NIS Directive provides legal measures to boost the overall level of cyber security in the EU ([EuCo16]).

The example as described and the current developments in the audit, legal and regulatory domains all concur in addressing cyber security risks as a major concern in general. As such, a financial auditor needs to consider relevant cyber security risks when conducting a financial statement audit (FSA). In addition to the traditional testing of GITCs, a financial auditor needs to assess the likelihood of GITC flip side as well.

Now, how do we address cyber security risks in the audit in a practical way? This article describes a practical approach called "Cyber in the Audit" (CitA). The approach contains the different activities to carry out, guidance for test activities and how to deal with companies that are already compromised. Finally, we address the impact of cybersecurity findings on the FSA.

A Practical Approach to Cyber in the Audit

When incorporating Cyber in the Audit activities in the traditional IT audit it is important to align these new activities as much as possible with the existing approach. This section explains the position of CitA in relation to other FSA activities and the CitA process.

Position of Cyber in the Audit

As shown in Figure 3, the IT audit supports the financial audit by testing the automated key controls. Likewise, CitA supports the IT audit, by testing the cyber security measures which prevent/detect the bypassing of the IT application and infrastructure controls.

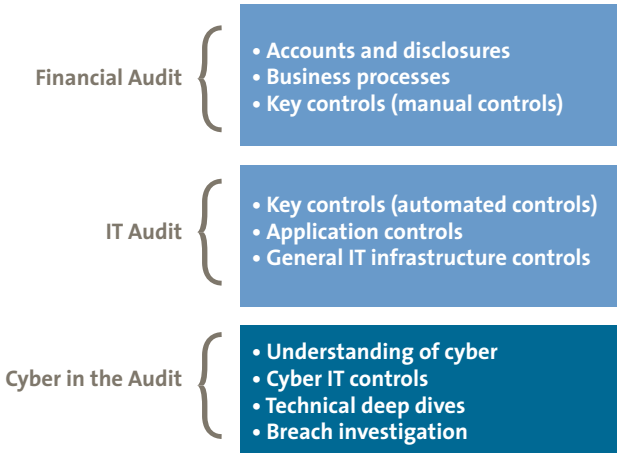

Figure 3. **Position of Cyber in the Audit.**

The CitA testing is an extension of the regular GITC testing and uses the same approach when it comes to control testing. The difference mainly lies in the topics to address and the use of technical deep dives for additional fact finding.

The CitA Process Step by Step

The flow chart in Figure 4 provides a workflow to help identify, assess and process cyber security risks in order to determine the impact on your financial statement audit. In each stage of the process, it can be decided to stop further fact finding if enough assurance on the state of cyber security controls is acquired. Each of the phases is further explained in the following sections.

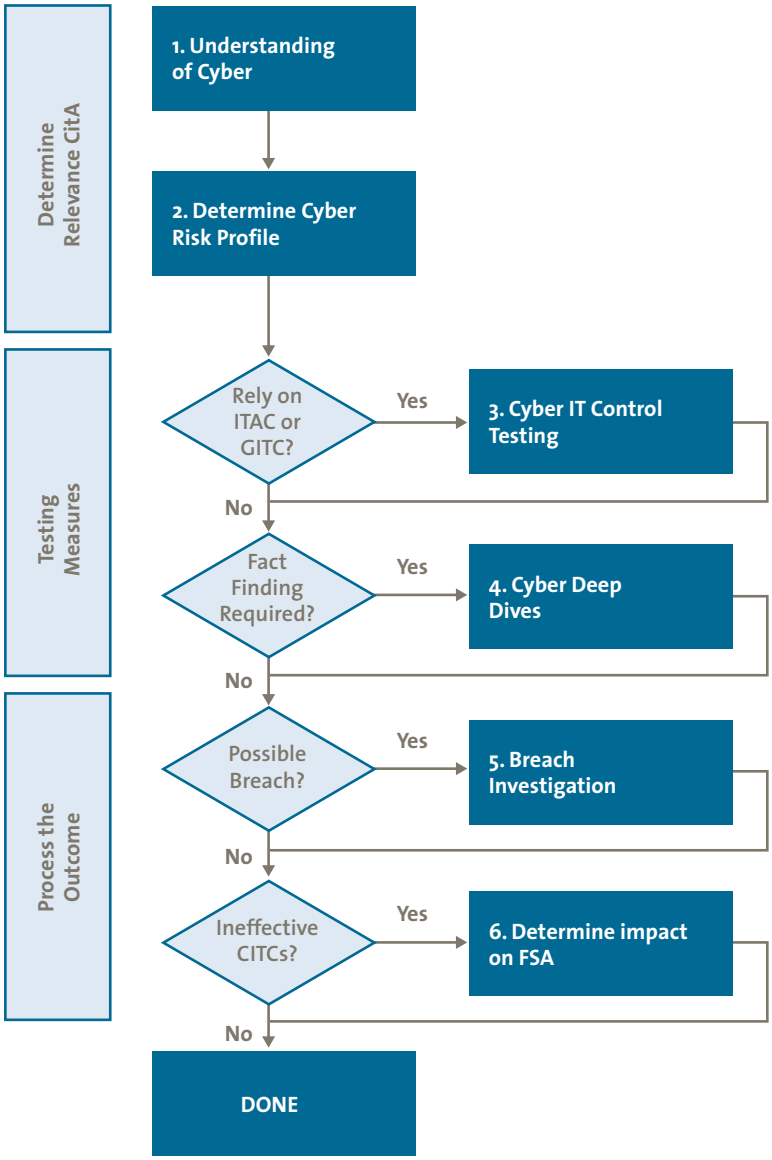

Figure 4. **CitA process flow.**

Determine the Relevance of CitA for the Financial Statement Audit

As part of the familiar "Understanding of IT" activities, we need to acquire an understanding of how cyber security risks are determined and controlled in the environment by extending this activity with "Understanding of Cyber". This should not only have a technical focus (e.g. implemented security in IT-systems), but also a focus on processes (e.g. response to a cyber security incident) and governance (e.g. who is steering/reporting and responsible for cyber security risks and measures). In addition, this approach is considered to be holistic, addressing topics like Legal & Compliance and Human Factors.

This is valuable input for further determining the need for further testing of any Cyber IT Controls and/or perform "deep dive" activities. In addition, this activity helps to identify weaknesses in the holistic cyber defense of the company, which can be reported through the management letter by way of concerns for business continuity or regulatory fines (e.g. data breach notification).

An overview of such topics are illustrated in Figure 5 which is based on KPMG's Cyber Maturity Assessment model. Of course other models can be chosen as well, such as those from ISF or NIST.

The cyber risk profile can be determined using the information from this analysis. Such a risk profile is a combination of the cyber threats the company is facing and the dependency on adequate cyber defense, which can be determined based on the understanding of cyber, but in addition on "trigger" questions such as those proposed by the NBA Public management letter ([NBA16]).

For cyber threats it is important to consider sector specific cyber threats, a high(er) chance of insider threats, primary revenue generated online, cyber fines and if the company has already been breached.

For cyber dependency it is important to take account of topics such as financial audit reliance on IT systems, most important assets (crown jewels), high level of automation, integrated supply chain and regulatory compliance.

When combined on two axis, the company is "plotted" based on the cyber threats and dependencies as shown

Leadership & Governance
Client's management, their due diligence, ownership, and effective management of risk within the context of the organization's goals, objectives and the external threat/risk landscape.

Human Factors
The level of security-focused culture that empowers and ensures the right people, skills, culture, and knowledge.

Information Risk Management
Client's approach to achieve comprehensive and effective risk management of information throughout the organization and its delivery and supply partners.

Business Continuity
Client's preparations for a security incident and its ability to prevent or minimize the impact through successful crisis and stakeholder management.

Operations & Technology
The level of control measures implemented within client to address identified risks and minimize the impact of compromise coming from both virtual or physical breach of security.

Legal & Compliance
Regulatory and international certification standards relevant to client.

Figure 5. **KPMG's Cyber Maturity Model.**

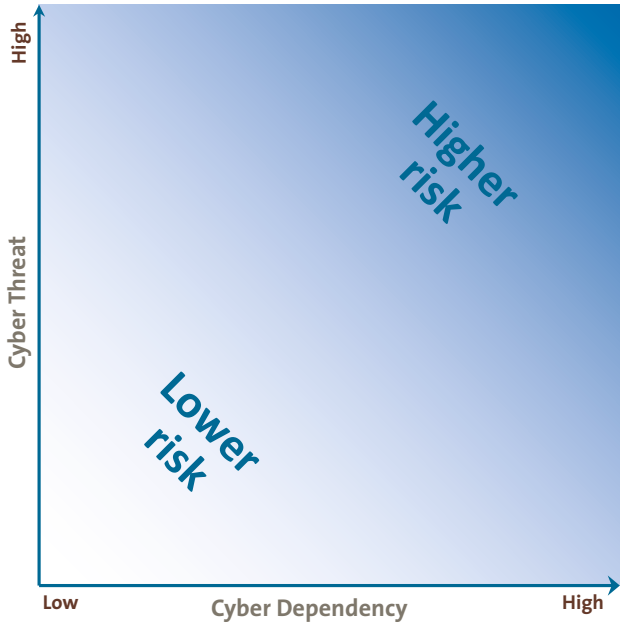

Figure 6. **Cyber risk profile plotting.**

in Figure 6. Such "plotting" has a close relationship with the sector the company is in. Typically, companies in the financial sector share common threats and dependencies (stealing money / integrity), which in itself differ greatly from for example the Manufacturing sector (sabotage/ availability).

This results in a relevance rating (for example low, medium, and high) based on the cyber dependencies and cyber threats the company is facing. The rating can also be used for further selection of Cyber IT Controls.

Testing Cyber Security Measures

The second phase consists of the actual testing of IT control measures specific to cyber security. Based on the just determined cyber risk profile, one or more Cyber IT Controls (CITCs) can be selected to test. The topics that the CITCs address are Cyber security Governance, Technical hardening and Cyber security Operations. These three topics cover the protect, detect and respond measures one would expect to be in place, for example: security monitoring, cyber incident response, security awareness and cloud security. The testing of these controls follows the exact same process as the testing of GITCs and can be seen as an extension to the default GITC set of controls.

As a result of ineffective CITCs, we know that security vulnerabilities may be present in the IT environment. As such, we need to select deep dive / fact finding topics which are applicable to the situation. Such deep dives can be, for example, Red Teaming, SAP Security, Phishing activities, SIEM reviews and Cloud Security Assessment, linking to the tested CITCs. The outcome of deep dives further clarify the impact of CITC deficiencies in terms of actual technical impact. Where CITCs may be ineffective, the technical implementation may not contain security vulnerabilities after all.

Breach Investigation

In the last phase, it is important to check if the company is aware of any cyber security breach having occurred in the financial year. In addition, tooling can help to determine this if the company is not able to provide evidence for this.

In the case the company is already aware that its IT environment has been hacked (or a hack is ongoing), or that this is discovered during the fact finding activities, the following steps are a guide to help determine the impact:

	Impact category	Guidance
1	**Impairment of asset value (e.g. Intellectual Property / sensitive data is stolen)** This is relevant, if the IP directly or indirectly influences the asset value on the balance. Would the represented value of the assets remain unchanged if the IP has been stolen by a competitor or has become common knowledge? In case an organization has placed a large part of its value into intellectual property, having this IP available to unauthorized users (or even the public) may cause significant devaluation of that asset.	In this case consider the following actions: • Assess what actor has stolen the IP / sensitive data to determine its motivation (hence impact). • Check the market place for related events (e.g. knock-off products for budget prices). • Check the stock market movements in case of stolen financial information (insider trading).
2	**Impairment of the banking system (cyber fraud / stolen cash)** In case fraudulent activity can be identified, not only do we have to formally report this, it can also directly impact the financial statement audit (the fraud amount should be accounted for).	In this case consider involving digital forensics regarding cyber fraud. Together you may consider determining the extent of the fraud via financial or technical analysis.
3	**Impairment of automated controls ("super user" bypasses all IT controls)** In case that the financial auditor relies on automated key (application) controls, scenarios in which it can be proven that these application controls can be circumvented or adjusted, directly impact the financial auditor's ability to rely on the figures resulting from an automated component.	In this case consider adjusting the financial or IT audit activities such that you acquire assurance through manual controls and/or data analytics, for example. In addition, you can consider further investigation if there are indicators that internal (IT) controls were actually bypassed at one point this year.
4	**Risk of contractual obligations (e.g. fines due to data privacy and breach notification act)** As of 1st of January 2016, organizations are required to notify the Dutch Data Protection Authority ("DPA") of data security breaches that have or are likely to have serious adverse consequences for the protection of personal data. Depending on the measures that the organization had in place to either prevent or detect such breach, they face penalties up to 10% of the organization's annual net turnover.	In this case consider if the company was actually compromised. If privacy sensitive data was compromised, it is required to notify the DPA. The DPA in turn can issue a fine. If they do, this fine needs to be included in the FSA. Given the size of the possible fine, this may have a material impact on the FSA. In addition, if the company is lacking too many cyber security measures, the risk exists that the company may be compromised in the coming 12 months. Hence, the DPA breach notification may be applicable then. As such, we can consider raising such an issue in the management letter / growing concern.
5	**Continuity risk / going concern** Major disruption of the IT environment from which an organization is unlikely to timely recover (and successfully counter a default). Most organizations' key business process relies on the correct functioning of IT. Cyber incidents may cause this major disruption (consider for example recent ransomware attacks).	In this case consider if the cyber security measures are not operating effectively to help prevent, detect and timely respond to cyber security incidents. If many of the cyber security measures are not operating effectively, chances are that operational disruptions may occur in the near future. Due to the hyper connectivity of modern IT networks, such disruptions (e.g. caused by ransomware) may disrupt many business processes through the occurrence of just one cyber security incident.

Table 1. **CitA Impact category and guidance.**

1. *Determine the threat actor.* What party/group/person is conducting the hack? Is this a state sponsored advanced persistent threat (APT) or just a "script kiddie"?
   This gives an indication of the magnitude and persistence of the actor.
2. *Determine the actor's motivation.* What is the goal of this hacker (group)? Are they looking to steal money, copy intellectual property / sensitive data (e.g. stock exchange data) or sabotage the production?
   This gives an indication of a possible impairment and points towards, for example, intellectual property (IP), stolen cash/fraud and/or operational sabotage.
3. *Determine actions until now.* What have they been doing before they were discovered? Are there any existing logging and monitoring capabilities to determine what actions this actor has already performed? Can the logging be trusted so that it has not been tampered with by this actor?
   This gives an indication of the damage incurred until now and it can be a source for answering the first two steps.

Consider involving digital forensic experts for the above mentioned process, to make sure that the correct actions and analysis is performed in such a way that this is still of value in court.

Determine the Impact of the CitA Findings on the FSA

The results of the CITC testing, deep dives and breach investigation are aggregated to determine potential FSA impact areas. This is fed into the financial audit process in

Do not fear cyber security – embrace it

order to determine the financial audit approach and choice regarding substantive testing, can-do/did-do analysis, etc. Table 1 can be used to determine how CitA findings relate to FSA impact categories.

Conclusion

With the ability to bypass all (effective) IT control measures, hackers pose a serious risk to existing accounting and internal control. With the increasing automation of our business processes and digital data becoming the single truth, financial auditors need to take these risks into account in relation to the financial statement and annual reporting. Hence, IT auditors need to change their approach and include the seeking of facts in the technical cyber security domain of their auditees.

The "Cyber in the Audit" approach explains the steps to do this, taking into account the relevance of cyber security risks for a company, the existing cyber defense capabilities and operating effectiveness thereof, and the possible breaches in the company's IT environment. In addition, a mapping of FSA impact categories with CitA findings provides guidance for the financial auditor translation.

Without wanting to add to the "cyber FUD" (fear, uncertainty and doubt) movement, it *is* crucial to understand what impact cyber security risks and incidents can have in our hyper connected digital world. Do not fear cyber security – embrace it.

References

[AICP14] AICPA, *CAQ Alert #2014-3*, March 21, 2014, https://www.aicpa.org/interestareas/centerforauditquality/newsandpublications/caqalerts/2014/downloadabledocuments/caq-alert_2014_03.pdf

[AICP16] AICPA, *AICPA Cybersecurity Initiative*, 2016, http://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/Pages/AICPACybersecurityInitiative.aspx

[CAQ14] Center for Audit Quality, *CAQ Alert #2014-03 - Cybersecurity and the External Audit*, March 21, 2014, http://www.thecaq.org/caq-alert-2014-03-cybersecurity-and-external-audit?s-fvrsn=2

[CybV16] Cybersecurity Ventures, *Cybersecurity Market Report*, Q3 2016, http://cybersecurityventures.com/cybersecurity-market-report/

[DCC] Dutch Civil Code, *Book 2, Title 2.9, Section 2.9.9 Audit*, http://www.dutchcivillaw.com/legislation/dcctitle2299aa.htm#sec299

[EuCo16] European Commission, *The Directive on security of network and information systems (NIS Directive)*, 2016, https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

[Gart15] Gartner, *Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015* (press release), November 10, 2015, http://www.gartner.com/newsroom/id/3165317

[IFAC16a] IFAC, *IAASB Amends Standards to Enhance Auditor Focus on Non-Compliance with Laws and Regulations* (press release), October 5, 2016, http://www.ifac.org/news-events/2016-10/iaasb-amends-standards-enhance-auditor-focus-non-compliance-laws-and-regulations

[IFAC16b] IFAC, *ISA 250 (Revised), Consideration of Laws and Regulations in an Audit of Financial Statements*, 2016, http://www.ifac.org/publications-resources/isa-250-revised-consideration-laws-and-regulations-audit-financial-statements

[MTRe16] MT Rendement, *Vijf belangrijke bedrijfsrisico's in beeld*, August 24, 2016, https://www.rendement.nl/nieuws/id18328-vijf-belangrijke-bedrijfsrisicos-in-beeld.html

[NBA16] NBA, *Van hype naar aanpak – Publieke managementletter over cybersecurity*, May 2016, https://www.nba.nl/Documents/Publicaties-downloads/2016/NBA_PML_Cyber_Security_(Mrt16).pdf

[Tysi16] K. Tysiac, *New path proposed for CPAs in cyber risk management*, Journal of Accountancy, September 19, 2016, http://www.journalofaccountancy.com/news/2016/sep/cyber-risk-management-201615199.html

[Whit16] T. Whitehouse, *CAQ: Audit's role in cyber-security exams*, September 15, 2016, https://www.complianceweek.com/blogs/accounting-auditing-update/caq-stumps-for-auditor-role-in-cyber-security-exams

About the Author

M. van Veen MSc RE CISA CISSP CRISC is a senior manager at KPMG Cyber. He has over a decade of experience in ethical hacking, IT infrastructure security, and technical IT auditing. He currently advises organizations about their cyber defense capabilities through cyber maturity assessments and improvement roadmaps. In addition, he increases the cyber security awareness of IT audit professionals and improves IT audit approaches. As such, he leads the Cyber in the Audit initiative in Europe for KPMG Netherlands.