

THE ROLE OF THE CHARTERED ACCOUNTANT IN DIMINISHING THE EFFECTS OF CYBER FRAUD

Elena-Simona Tache (Buzătoiu), Ph.D Student
IOSUD-SDSE Valahia University of Targoviste, Romania,
simona_buzatoiu@yahoo.com

Amalia-Magdalena Dănilă (Calafeteanu), Ph.D Student
IOSUD-SDSE Valahia University of Targoviste, Romania,
amaliacalafeteanu@gmail.com

1.

Monica-Mihaela Drăgan (Radu), Ph.D Student
IOSUD-SDSE Valahia University of Targoviste, Romania,
monicadraganradu@gmail.com

ABSTRACT: *In 2017, CERT-RO processed over 138 million cyber security alerts and an exponential increase in cyber fraud is expected. By its nature, the financial sector is in danger, registering an alarming growth in recent years, and about 70% of fraud remains undetected. When we talk about operations and security, financial organizations should use a multi-level, layered approach, focused on both the technical side and the human resource.*

Many financial institutions have been victims of cyber-attacks and social engineering. It is absolutely obvious that incidents are the result of human error, so prevention requires training, courses, awareness workshops.

In the context of the pandemic caused by the new coronavirus, most activities have moved to the online environment, both services, customer-company interactions (browser or application) and employee-company interactions (confidential databases).

In order to highlight the above, a comparative analysis is required between entities that have invested in cybersecurity and training of their own employees versus entities that have not been prepared for these exposures. In this sense, what would help the chartered accountant to play a significant role in diminishing the effects of cyber fraud?

Keywords: cyber security, human resources, professionalization, Social Engineering, digitalization, financial institutions, pandemic.

JEL Classification : M41, M53, M15.

INTRODUCTION

"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).

In 2017, CERT-RO processed over 138 million cyber security alerts and an exponential increase in cyber fraud is expected. By its very nature, the financial sector is in jeopardy, growing alarmingly in recent years, and about 70% of fraud remains undetected. When we talk about operations and security, financial organizations should use a multi-level, layered approach, focused on both the technical side and the human resource. Combining them is the new challenge for economic institutions as many financial institutions have been the victims of cyber-attacks and social engineering. It is absolutely obvious that incidents are the result of human error, so prevention requires training, courses, awareness workshops.

In the context of the pandemic caused by the new coronavirus, most activities have moved to the online environment, both services, customer-company interactions (browser or application), and employee-company interactions (confidential databases).

This material aims to bring into focus the imminence of cyber fraud attempts in the financial accounting sector and proposes solutions for professionals in the field of risk reduction, the vector being the human resource. The purpose of the article is to raise awareness of the importance of employees training and to transform them from victims of cybercrime into combatants by disseminating information.

In their roles as protectors and administrators of value, accountants need to be involved in cyber security solutions, whether acting as consultants to their clients, in a financial-accounting team or in a more general strategic or operational role.

Using new digital metrics should just be a reasonable learning extension for these competent and experienced people, as part of their learning process to stay relevant for the company executives whom they are overseeing and the investors whom they are representing (Grove, Georg and Clouse 2017).

REVIEW OF THE SCIENTIFIC LITERATURE

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).

Putting Malicious Cyber Activity in Context			
CRIMINAL ACTION	ESTIMATED COST	PERCENT OF GDP	SOURCE
GLOBAL			
Piracy	\$1 billion to \$16 billion	0.008% to 0.02%	IMB
Drug Trafficking	\$600 billion	5%	UNODC
Global cyber activity	\$300 billion to \$1 trillion	0.4% to 1.4%	Various
US ONLY			
Car Crashes	\$99 billion to \$168 billion	0.7% to 1.2%	CDC, AAA
Pilferage	\$70 billion to \$280 billion	0.5% to 2%	NRF
US- cyber activity	\$24 billion to \$120 billion	0.2% to 0.8%	Various

Figure no. 1 Estimated global loss on cybersecurity (%)

Source: Center for Strategic and International Studies, The Economic Impact of Cybercrime and Cyber Espionage

Global cyber-attacks in 2020, among which the costliest were reported in Computer Weekly:

- Currency exchange company Travelex has faced payment requests to decrypt the company's critical files after being hit by one of the most sophisticated ransomware attacks, known as Sodinokibi, which shut down IT systems on New Year's Eve.

The company, which operates in 70 countries, faced days of downtime after hackers made a devastating synchronized attack to hit the company when many of its employees were on vacation. According to security experts, the criminals requested a six-digit sum to provide Travelex decryption tools to recover the contents of files that have been encrypted by the virus.

- The criminal group responsible for the cyber-attack that disrupted banks and the foreign exchange chain Travelex for more than three weeks launched what has been described as a "massive cyber-attack" on parts manufacturer Gedia Automotive Group, with over 4,300 employees in seven countries, who said the attack would have far-reaching consequences for the company, which was forced to shut down IT systems and send staff home.

- The UK National Trust has joined a growing list of education and charities that have jeopardized the data of their graduates or donors in a two-month ransomware incident at US cloud software provider Blackbaud.

- IT services company Cognizant warns customers that a cyber-attack initiated by the ransomware group Maze has hit services to some customers. The IT services company, which has a turnover of more than \$ 16 billion and operations in 37 countries, provides IT services to companies in the manufacturing, financial services, technology and healthcare industries.

- Lloyds Bank customers were targeted by a phishing scam that hit mailboxes and text messages. The e-mail, which looks like an official correspondence from Lloyds Bank, warned its customers that their bank account had been compromised.

- Carnival cruise lines were hit by ransomware and customer data stolen.

- Hackers who launched the ReVIL or Sodinokibi redemption attack on law firms Grubman, Shire, Meiselas and Sacks (GSMS) have filed a \$ 42 million buybacks and threatened to release compromising information about US President Donald Trump.

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 Internet of Things devices, like security cams. In April 2016, the Russian hacker, Guccifer 2.0, hacked the servers of the Democratic National Committee. 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).

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 Coronavirus outbreak is now the biggest cyber security threat of all time. The total volume of phishing emails and other security threats related to the Covid-19 coronavirus has been found to be the largest around a single topic that has been seen for a long time and possibly ever, as Sherrod DeGrippe, senior director of threat research and detection at Proofpoint announced.

Recently, the CERT-RO team received notifications regarding a series of phishing messages coming from e-mail addresses from abroad, targeting BCR customers.

It is a phishing attack by which attackers try to extract card data from users, serving them a certain scenario. How this attack works: the message comes from an address with no connection to BCR, from various domains (.com, .fr) The text has spelling inaccuracies, a sign that the attackers could have used an automatic online translation tool in Romanian. Under the pretext that BCR has 'updated its online security system', the attackers seek to persuade potential victims to enter the card data. Of course, the user should realize that it is a fraud attempted, especially if he used the card without problems during the specified period and even more since BCR published on the website a series of anti-phishing information, where specific: BCR 'will never ask you to disclose, confirm or modify your personal and / or bank or card authentication data by accessing a link sent by e-mail, or to access the internet banking application via a URL sent by e-mail'.

Several others phishing attacks took place in online, using the image of important companies, such as DEDEMAN and OLX. The directions of the scam were either a one in a million sale, or their account being in danger and requiring a confirmation.

There is good news for Romania, though, coming from European Union. On 9 December 2020, Bucharest, Romania was selected by representatives of the governments of the EU member states as the prospective seat of the new European Cybersecurity Industrial, Technology and Research Competence Centre.

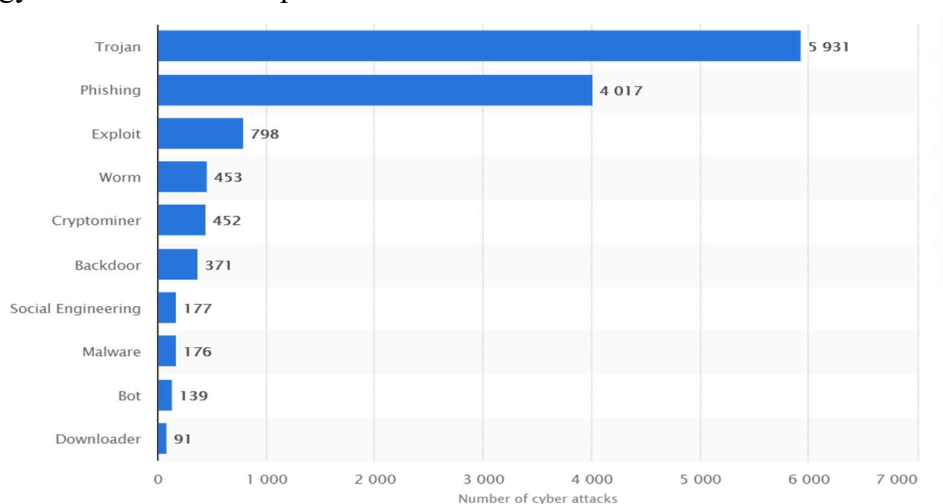


Figure no. 2 Number of cyber-attacks in Romania in 2019, by type

Source: www.statista.com

The Cybersecurity Competence Centre will improve the coordination of research and innovation in cybersecurity in the EU. It will also be the EU's main instrument for pooling investment in cybersecurity research, technology and industrial development.

The representatives of the governments of the 27 EU member states voted in the margins of a meeting of the EU ambassadors in the Council's Permanent Representatives Committee (Coreper).

Negotiations with the European Parliament on the proposed regulation establishing the Centre are ongoing.

Consequently, the investment in technology and collaboration with IT companies must happen organically in the next period on the software side, but the investment that requires the constant involvement and perpetual support of the company.

The reality is that technology seems to be advancing rapidly, and new consortiums have emerged to accelerate the definition of industrial standards and to foster collaboration (Kokina et al., 2017). New approaches to security and privacy controls are also emerging.

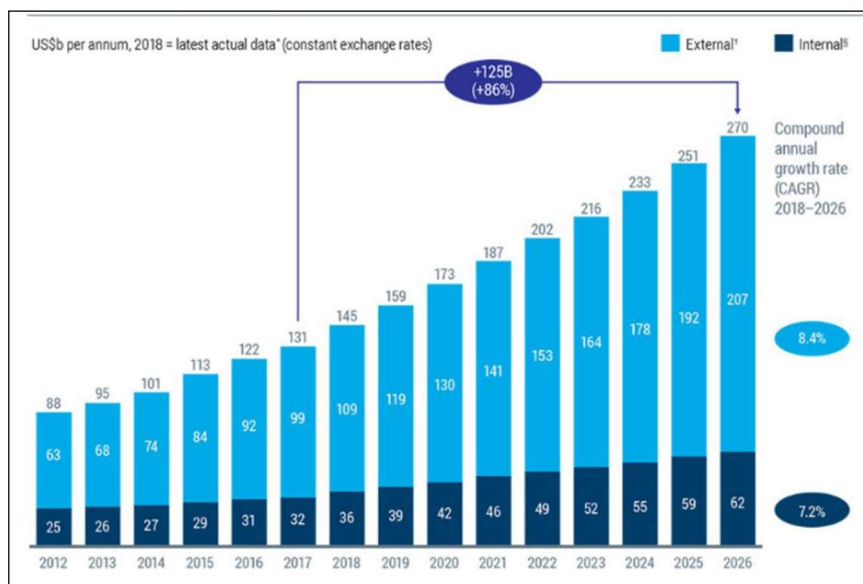


Figure no. 3 Estimated global spending on cybersecurity (%)

Source: Australian Cyber Security Growth Network, SCP - Chapter 1 - The global outlook for cybersecurity, 2020.

A recent report by the Alan Turing Institute in the UK emphasized that the terms "national security" or "cyber security" would become familiar. At the same time, it is clear that more attention needs to be paid to "epistemic security" - because without it, our societies will lose the ability to respond to the worst risks they may face in the future.

Focusing on the human factors involved with information security, Kevin Mitnick explains why all the firewalls and encryption protocols in the world will never be enough to stop a savvy grifter intent on rifling a corporate database or an irate employee determined to crash a system. He illustrates just how susceptible even the most locked-down information systems are to a slick con artist impersonating an IRS agent. Mitnick offers advice for

preventing these types of social engineering hacks through security protocols, training programs, and manuals that address the human element of security.

RESEARCH METHODOLOGY

We are using a meta-analysis, quantitative, in order to statistically analyse the results of a large collection of studies concerning cyber-security and the impact of the economic actors depending on the investments in professionalization.

Cyber security is a highly profitable investment for business leaders because it avoids the costs of a cyber-attack while exploiting the benefits of good security.

More and more companies classify cyber risk as a risk of legal non-compliance for the organization, taking, for example, non-compliance with the GDPR.

The NTT Security 2019 Risk Value report highlights the lack of investment in cybersecurity, especially in France. It also highlights the lack of awareness of companies on compliance, the persistent inability to provide critical data and increased recovery time after a security incident (+10 days compared to 2018). The performance of companies in France has deteriorated compared to India, which is today the best performing country in terms of cybersecurity, ahead of the United States and the United Kingdom.

France Vs. India - Comparative analysis of investments vs. loss

French companies and, more widely, those around the world are stagnating in their progress towards strengthening cyber security and seem paralyzed by the increasingly sophisticated techniques of cybercriminals. This is the conclusion drawn from the results of the Risk: Value 2019 report conducted with 2,256 business decision makers in 20 countries - including 200 French - commissioned by NTT Security, the security branch and the security excellence centre of the NTT group.

This year's results show that companies are aware of the dangers of cyber threats, placing cybersecurity and data theft among the top five risks to their business, certainly behind economic factors, but well ahead of other global issues such as the environment, barriers to international trade and political instability. The vast majority of survey participants - 78% for the French - believe that strong cyber security is good for their business. 90% even believe that cyber security has a major role to play in society in a broader sense.

Key fact: Indian companies, whose country is a newcomer to the study, are prosperous in the world in cybersecurity, ahead of their American and British counterparts. As the international media stagnates, the performance of companies in France, Germany and Singapore deteriorated last year, the same as financial services, telecommunications, chemicals, the pharmaceutical industry, oil and gas or healthcare facilities, questioning the soundness of critical national infrastructure.

The stagnation of French companies - and the situation worldwide

As last year, 44% of participants in the French survey consider all their critical data to be "fully secure" vs. 48% globally. Although 83% of French respondents consider it important to comply with the regulations, 1 in 5 do not know which one applies to their business.

Only 37% believe they are subject to the GDPR, while the regulation came into force a year ago and affects all companies with activities or customers in an EU Member State.

Security budgets do not keep pace with the increase in cyber risk: the increase in the percentage of IT budgets allocated to security is only 15% this year. Companies still lack

proactivity in terms of internal policies and processes. 49% of French companies - compared to 58% globally - have implemented a formal IT security policy, while 46% have an incident response plan - compared to 52%. Almost half of the French managers surveyed (46%) consider that cyber security "is the problem of the IT department and not of the company as a whole".

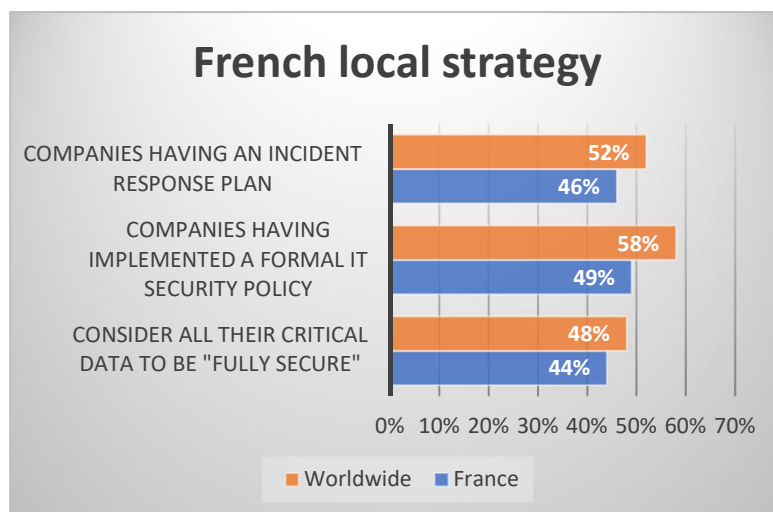


Figure no. 4 French local strategy

Source: Own diagram based on NTT Security records.

38% of French companies say they have no skills or resources. This finding remains unchanged from year to year, which seems to indicate that they need more assistance from an external security provider.

Security incidents: costs and time to restore growing activity

The Risk: Value 2019 report also shows that the recovery period of the business following a security incident continues to increase from year to year, which is estimated at 49 days on average in France, i.e., 10 additional days per year compared with 2018. Globally, this time is even longer with an average of 66 days, or 9 additional days compared to 2018. The estimated percentage of loss of turnover also increases each year by 10.4 % in 2019 in France and 12.7% worldwide.

The cost of resuming business following a security incident remains high, according to the report, reaching 690,000 euros in France, compared to 1 million euros (M€) on average worldwide. In the Nordic countries in particular, cost forecasts are much higher, reaching EUR 1.6 million in Norway and reaching a maximum in Sweden of EUR 2.7 million, more than double the world average. The oil and gas industry leads the sector in this area, with a resumption cost of EUR 2 million.

India and France on the 22nd of August 2019 concluded a path breaking road-map to make digital technology a transformative factor in their societies, to fight terror, to foster economic growth, sustainable development and secure enhanced internet access which is essential to bridge digital divide. The two countries signed an agreement on cooperation in the area of fight against cybercrime.

France and India recognize that cybercrime is a transnational crime that requires enhanced international cooperation to effectively bring cyber criminals to justice. As such, they plan to strengthen their cooperation in this area, with a particular view to facilitating

sharing of information, evidence collection, the identification of offenders, particularly malware developers, hosters / hosting platform providers or broadcasters. They also express their concerns regarding the security of electronic means of payment and confirm their commitment to the protection of consumers against online financial frauds including ATM cash outs. Finally, they plan to discuss the prevention of cybercrime with Service Providers, Social Media Companies to seek information sharing arrangements.

The two countries are willing to exchange technology and ideas, as they are complementary on these domains.

RESULTS AND DISCUSSION

The role of the chartered accountant in diminishing the effects of cyber fraud

Hacking and phishing attacks are often triggered by an employee innocently clicking on a link in an email.

Opening dubious email attachments is another common way for malware to enter an organisation. 'Word, Excel and PDF documents all present an easy way to embed a malicious code that can be exploited later,' says Greg Sim, chief executive of security technology company Glasswall Solutions.

In fact, while cyber-attacks are growing increasingly sophisticated, the main reason for security breaches is lax security awareness among employees. Bad password behaviour is one example. Research from password management firm Meldium shows that 90% of employee passwords are so predictable they can be cracked in six hours. Moreover, 18% of employees share their passwords with others.

Many employees also have their work emails automatically forwarded to personal email hosts. But hackers often look for corporate data through personal email, which is easily accessible to them because personal email services do not have the same security measures as corporate email services.

Cybercrime threatens trust and transparency in business and in government every day. As consumers, taxpayers, suppliers or other stakeholders, we wonder if we can trust organizations to ensure the effective protection of our data. The public is increasingly expecting greater openness to ethical issues related to cybersecurity breaches and how personal data is protected.

In their roles as protectors and administrators of value, accountants need to be involved in cyber security solutions, whether acting as consultants to their clients, in a financial-accounting team or in a more general strategic or operational role.

A recent article in the IFAC Global Information Network (www.ifac.org/Gateway) on Cyber Security presents relevant perspectives on the issues that accountants need to consider in relation to their role in cybernetic security. These include using their skills and knowledge to protect data and information, as well as reporting on the program and controls associated with managing a company's cyber security.

The cybersecurity landscape is changing rapidly as organizations store more data and hackers have more opportunities to break into systems. The consequences of security breaches, in the form of fines and legal action and, ultimately, the loss of customers, are also becoming increasingly significant.

A new study on the costs of cybercrime conducted by *Accenture* - a multinational management consulting company, technological solutions and outsourcing and the *Ponemon Institute* shows that information theft is the costliest consequence of cybercrime, while also

the fastest growing (although the data do not represent the only target). Companies do not think about ensuring their buildings, but in many situations, they are exposed to the loss and damage of the data they have. At best, stolen data, broken systems, and malware cause significant disruption to operations. In the worst case, reputation is damaged. Businesses must start from the premise that their security will be compromised. For boards and other stakeholders, cyber security must be treated as a significant business risk. People in supervisory or management positions therefore need more information on how organizations can manage cybersecurity as part of their risk management programs.

Given that cybersecurity is a complex, multidimensional business risk, it is important to involve executives and management in ensuring a comprehensive, business-oriented approach that integrates cybersecurity aspects into the entire decision-making process and all data operations and company information networks. Holistic risk management, rather than a fragmented approach, is the only effective way to deal with an ever-changing business environment as well as ever-evolving threats and risks targeting people, processes and technology across the enterprise. The involvement of all levels of an organization helps to ensure that there is a general framework that everyone understands and that the various lines of defence can manage and mitigate cyber security risks together at all times.

A proactive and pragmatic risk-based approach involves identifying gaps, concentrating resources to address key threats, and expanding cybersecurity activities beyond simple prevention, to include intelligence gathering, detection and response. Key steps include understanding cybersecurity roles and capabilities and identifying, mitigating, and monitoring specific risks, such as data privacy or cloud security risks. The identification and mitigation of cyber risks requires the mapping of key processes, systems and information flows and the assessment of the appropriate risk remediation plan and controls, as well as ongoing monitoring.

With regard to addressing the substantial gaps in cybersecurity levels, it is important to identify critical information assets and provide the appropriate foundations. For many organizations, this means addressing key security practices, including firewalls and Internet Gateways, secure configurations, access control, antimalware protection, and patch management. The core discipline involves reacting to new standards and regulations, understanding the weaknesses of traditional systems and identifying cases where investments in technology could be useful.

Supporting smaller businesses is an important opportunity for companies to provide useful business advice. The professional accounting consultant can be especially important in order to:

- help clients assess their governance and risk management - smaller businesses tend not to have a solid knowledge of risk management and control. Accountants can provide adequate planning for business continuity and disaster recovery, especially against ransomware threats;
- help clients quantify the risks and return on investment based on the cost of breaches and stolen data and the factors that affect the cost and help mitigate risks through effective controls.

The top costs of a company data breach, according to industry accountants.

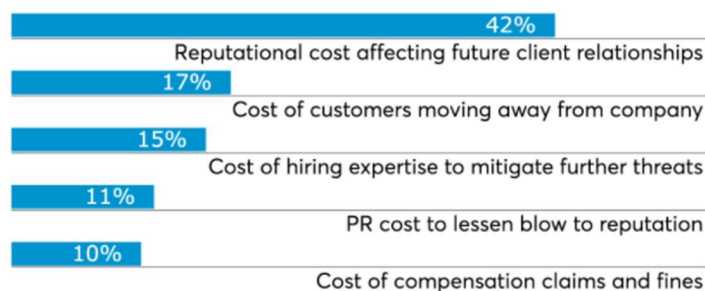


Figure no. 5 Cost distribution after a cyber-attack (%)

Source: *accountingtoday.com, Cyber-attacks threaten tax pros and accountants during coronavirus crisis*

An enhanced role in cyber security does require relevant knowledge, skills and experience. For accountants to effectively undertake cybersecurity risk management or attestation services, key areas of knowledge and skills include: relevant IT systems and technology, as well as the ability to keep current on changes in the technology and systems environment, understanding IT processes and controls and their evaluation, awareness and relevant experience with cybersecurity frameworks, understanding an entity's industry and business and whether it is subject to specific types of cybersecurity risks and establishing and engaging multidisciplinary teams, for example including information security professionals and auditors.

ICAEW (*The Institute of Chartered Accountants in England and Wales*) offers simple cybersecurity steps for smaller businesses. In the United States, *The American Institute of Certified Public Accountants* introduces *system and organization controls* (SOC) for cybersecurity, in order to assist accountants in managing and certifying risks and also provides the basis for transparent and consistent communication about the efforts of managing the cyber security risk in an organization. It also works to increase stakeholder confidence in the information provided by management on the organisation's cybersecurity efforts.

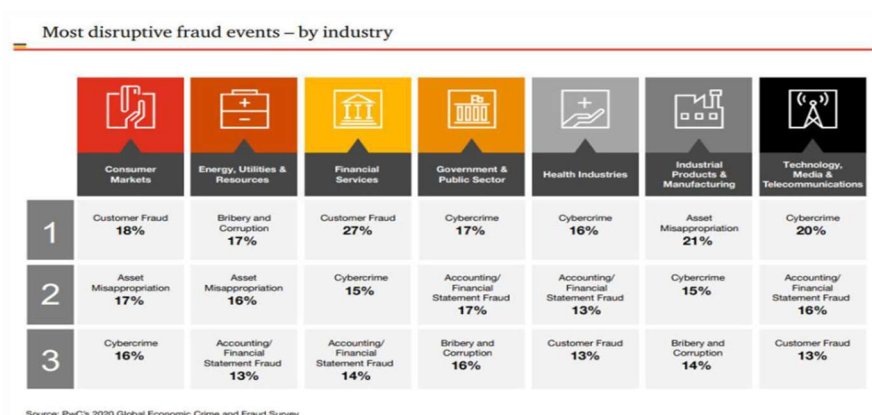
The general reporting framework for cybersecurity risk management, a key element of the SOC, includes the criteria that management should use to describe an entity's cybersecurity risk management program and the key components of the cybersecurity attestation report, which covers management's description of the entity's risk management program and its statement of the operational effectiveness of controls to ensure the achievement of cybersecurity objectives, as well as key components of the certification report and the professional accountant's report thereon.

In recent times, in Singapore, the Commercial Affairs Department (CAD) has seen cases where complainants, people who have approached CAD to report cases, these complainants observed financial irregularities, but they were not fully able to make sense of these irregularities. This changed only when audit or accounting firms came in to perform forensic accounting and digital forensics, which then led to firms being able to take action to strengthen their cyber defence.

Accountants can step beyond their traditional roles and help businesses fight cybercrime, as the Second Minister for Home Affairs Josephine Teo of Singapore says.

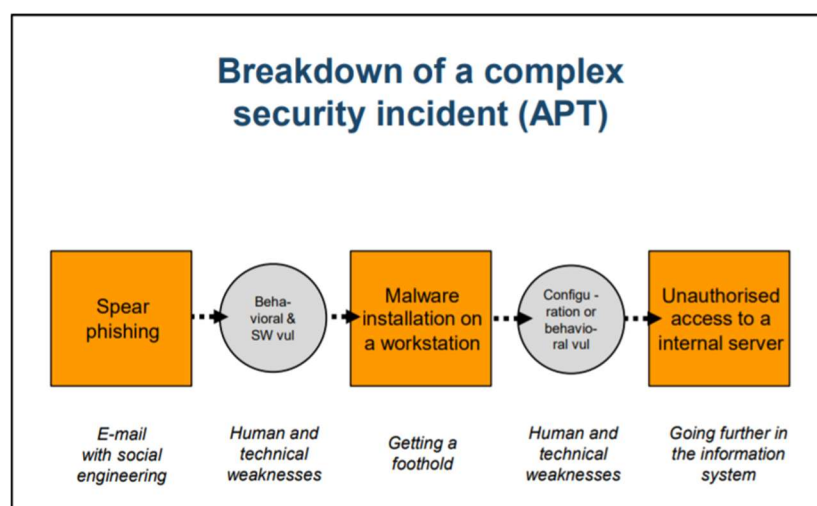
Accountants needed to hone their skills in three areas, said Mrs Teo. The first was forensic accounting, which she said was critical to help “uncover fraudulent activities from among voluminous transactional data”. The second capability would be digital forensics, as more transactions are becoming digital and mobile. Finally, accountants should also focus on financial crime compliance, which must evolve to keep up with new business models such as peer-to-peer lending.

Figure no. 6 Frequency of cybercrime by industry



Source: PwC, *Fighting fraud: A never-ending battle PwC's Global Economic Crime and Fraud Survey*

Figure no. 7 Description of a complex security incident



Source: ETSI GS ISI 002 V1.2.1 (2015-11) *Information Security Indicators (ISI); Event Model. A security event classification model and taxonomy*

CONCLUSIONS

In conclusion, once aware, the effects of cyber-attacks can be minimized by investing on the one hand in technology and on the other hand in improving human resources. In the age of digitalisation, the accountant is the link between the financial sector, software and the legal basis, which is a key player in avoiding cyber fraud. Accountants and finance professionals can, and should, play a leading role in defining key areas of a strategic approach to mitigating cybercrime risks. These include creating reasonable estimates of financial impact that different types of cybersecurity breaches will cause, so that a business can be realistic about its ability to respond to an attack and/or recover from it. Accountants and finance pros can also help organizations define a risk management strategy and set priorities for the digital resources they consider most valuable. Accountants are well placed to advise on the steps a business should take to protect itself – cyber security isn't just about technology and computers: it involves people, information, systems, processes and culture too. To be ready for the broad range of threats, accountants need to understand IT security policies at their firms, including policies and processes that they need to follow to ensure safe online practices, as well as procedures on reporting and dealing with breaches. Accountants may also need additional training on cyber awareness. Prevention, as with most things, is far preferable than cure.

REFERENCES

- [1] American Institute of Certified Public Accountants (2017). Guide: Reporting on an Entity's Cybersecurity Risk Management Program and Controls, *AICPA*, May 1, <https://www.wiley.com/en-us/Guide%3A+Reporting+on+an+Entity%27s+Cybersecurity+Risk+Management+Program+and+Controls%2C+2017-p-9781119449966>.
- [2] Castelluccio, Michael(2017). "The most notorious hacks of 2016." *Strategic Finance*, vol. 98, no. 7, 2017, p. 55+. Gale Academic OneFile, link.gale.com/apps/doc/A477203501/AONE?u=anon~b7ff1ba6&sid=googleScholar&xid=94fbf7f7. Accessed 4 July 2021.
- [3] CBS Mews (2017). "Deloitte Hack Reportedly Hit Corporate, Government Clients," msn.com, September 25, <https://www.cbsnews.com/news/deloitte-cyber-attack-reportedly-hit-corporate-government-clients/>.
- [4] Bain, B., & M. Robinson (2017, September 20). Hackers May Have Profited From SEC Corporate Filing System Attack. Retrieved from *bloomberg.com*, September 21, 2017, 6:39 AM GMT+3 Updated on September 21, 2017, 11:47 PM GMT+3.
- [5] Grove, H., Clouse, M., & Georg Schaffner, L. (2018). Digitalization impacts on corporate governance. *Journal of Governance & Regulation*, 7(4), 51-63. https://doi.org/10.22495/jgr_v7_i4_p6
- [6] Riley, M., A. Sharpa, and J. Robertson (2017). "Equifax Suffered a Hack Almost Five Months Earlier Than the Date It Disclosed," *bloomberg.com*, September 18.
- [7] Kokina, J., Mancha, R., & Pachamanova, D. (2017). Blockchain: Emergent industry adoption and implications for accounting. *Journal of Emerging Technologies in Accounting*, 14(2), 91–100.
- [8] Mitnick, K. D., & Simon, W. L. (2002). The art of deception: controlling the human element of security.

- [9] Tysiac , K. (2017, April 26). A New Cybersecurity Risk Management Reporting Framework For Management and CPAs. *Journal of Accountancy*
- [10] Website of Internet Security Centre (CIS), Available to: www.cisecurity.org
- [11] Free online security checks: <http://www.staysafeonline.org/stay-safeonline/free-security-check-ups>
- [12] Website of National Cyber Security Alliance for Local Users in Organizations, Available to: <http://www.staysafeonline.org>
- [13] Website of OnGuard Online, Available to: www.OnGuardOnline.gov
- [14] Website of SANS Institute (System Administration, Audit, Network, Security) – Vulnerabilities, Available to: <https://www.sans.org/emea/>
- [15] Website of Internet security critiques, Available to: www.sans.org/top20 Computer Weekly 2020
- [16] Website of IFAC's global information network, Available to: www.ifac.org/Gateway
- [17] Website of FORBES 2020 Magazine, Available to: <https://www.forbes.com/sites/louiscolumbus/2020/04/05/2020-roundup-of-cybersecurity-forecasts-and-market-estimates/?sh=1525a5cf381d>
- [18] Website of ENISA, Available to : <https://www.enisa.europa.eu/topics/cybersecurity-education>
- [19] Website of The global body for professional accountants, Available to: <https://www.accaglobal.com/vn/en/student/sa/features/cyber.html>
- [20] Website of Journal of Accountancy, Available to: <https://www.journalofaccountancy.com>
- [21] Website of CERT-RO, Available to : <https://cert.ro>