Role of Accountants in Addressing Cybersecurity Risk

CA. Dayaniwas Sharma **CA. Manu Agrawal**

The authors are member of the Institute. They can be reached at dayaniwas@gmail.com and eboard@icai.in

In today's interconnected digital environment, technology plays a profound role in shaping the global risks landscape for citizens, governments and businesses. The World Economic Forum's Global Risks Report, 2019 ranked cyberattacks among the top-five risks. At a global level, cybercrime causes multibillion dollar losses to business; the average cost of cybercrime for an organisation has increased from $11.7 million in 2017 to $13.0 million. Read on to know more...

Cyber Threat Landscape

"Cyber vulnerabilities can come from unexpected directions, as shown in 2018 by the Meltdown and Spectre threats, which involved weaknesses in computer hardware rather than software. They potentially affected every Intel processor produced in the last 10 years. Last year also saw continuing evidence that cyberattacks pose risks to critical infrastructure. In July the US government stated that hackers had gained access to the control rooms of US utility companies. The potential vulnerability of critical technological infrastructure has increasingly become a national security concern. The second most frequently cited risk interconnection in this year's GPRS was the pairing of cyber-attacks with critical information infrastructure breakdown." States Global Risks Report 2019[1]

As per market reports, the value of the cybersecurity market is estimated to grow from $120 billion in 2019 to $300 billion by 2024. Further, it is more surprising that, while efforts and investment to improve cybersecurity continue to grow, security developments lag behind the pace of the malicious use of digital technologies. Increasing incidents show that cyber threats are escalating in frequency, impact and sophistication.

The European Union Agency for Network and Information Security (ENISA) Threat Landscape Report 2018[2] mentions, the main trends in the 2018's cyberthreat landscape are:

- Mail and phishing messages have become the primary malware infection vector.

1. *"The Global Risks Report 2019 – 14th Edition" published by World Economic Forum*
2. *ENISA Threat Landscape Report 2018 – 15 Top Cyber threats and trends*

- Exploit Kits have lost their importance in the cyberthreat landscape.
- Cryptominers have become an important monetisation vector for cyber-criminals.
- State-sponsored agents increasingly target banks by using attack-vectors utilised in cyber-crime.
- Skill and capability building are the main focus of defenders. Public organisations struggle with staff retention due to strong competition with industry in attracting cybersecurity talents.
- The technical orientation of most cyberthreat intelligence produced is considered an obstacle towards awareness raising at the level of security and executive management.
- Cyberthreat intelligence needs to respond to increasingly automated attacks through novel approaches to utilisation of automated tools and skills.
- The emergence of IoT environments will remain a concern due to missing protection mechanisms in low-end IoT devices and services. The need for generic IoT protection architectures/good practices will remain pressing.
- The absence of cyberthreat intelligence solutions for low-capability organisations/end-users needs to be addressed by vendors and governments

Frameworks to Assist Management in Implementing and Evaluating a Cybersecurity Risk Management Program

- National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity. A 2013 Presidential Executive Order called for the creation of a voluntary, risk-based cybersecurity framework that would provide a set of industry standards and best practices for all organisations. The resulting NIST framework came together with collaboration between industry and government. Organisations can turn to the Voluntary Program, which was created to help organisations use the NIST Cybersecurity Framework to improve their cyber resilience. According to the United States Computer Emergency Readiness Team, the program connects organisations with public and private sector resources that align to the NIST Framework's five functional areas: Identify, Protect, Detect, Respond, and Recover.
- ISO/IEC 27001/27002 - Published by the International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC), this group of standards is intended to be used as guidance for securing financial information, intellectual property, employee data, and other information entrusted to the organisation by third parties.
- SEC Cybersecurity Guidelines -The SEC has published cybersecurity guidance for registered investment companies and investment advisers, including steps to consider to address cyber risk.
- Trust Services Criteria (TSC) The TSC align to the 17 principles presented in COSO Internal Control—Integrated Framework. The TSC, as developed by the AICPA's Assurance Services Executive Committee, are designed for use in evaluating the suitability of the design and operating effectiveness of controls relevant to the security, availability, or processing integrity of information and systems, or the confidentiality or privacy of the information processed by the systems at an entity, a division, or an operating unit of an entity or a particular type of information processed by

> A Computer Security Institute (CSI) survey ranked internal cybersecurity audits as the strongest weapon in preventing and detecting cybersecurity vulnerabilities.

one or more of an entity's system(s) or one or more systems used to support a particular function within the entity.

A Computer Security Institute (CSI) survey ranked internal cybersecurity audits as the strongest weapon in preventing and detecting cybersecurity vulnerabilities. An effective internal security audit identifies cybersecurity risks and assesses the severity of each type of risk. Following the audit, preventive controls need to be instituted for the major risks that were identified. Some best practices that can help management develop those controls include:

- Proactively patching vulnerabilities, including vulnerable software.
- Using least-access privileges and other sound logical access controls to help remediate crimes perpetrated internally; for external threats, sound perimeter controls such as firewalls, intrusion prevention systems (IPS) and intrusion detection systems (IDS) are critical to protection.
- Monitoring systems, technologies and access with associated controls varying based on the threat level (also a detection strategy); for example, use various logs created by technologies for those activities.
- Data backups, including offline versions.

> Accountants should, using their skills and expertise, play a role in helping organisations protect data and information, as well as reporting on a company's cybersecurity risk management program and controls.

Role of Accountants in Cybersecurity Risk Management

Organisations should develop a holistic risk management rather than piecemeal approach in dealing with cyber security that spans across people, processes and technology across the business. It is suggested that accountants gain a clear and overall understanding of the major threats, risks, costs and other related factors posing risk to cybersecurity of an organisation. Accountants should using their skills and expertise play a role in helping organisations protect data and information, as well as reporting on a company's cybersecurity risk management program and controls. They should help the board of directors/ audit committees in identifying suitable preventive measures. They need not assume role of cybersecurity expert, but they should remain informed and aware of cybersecurity risks and wherever required engage security professionals. Accountants should gain knowledge in relevant IT systems and technology environment, understand IT processes and controls and their evaluation, awareness of various cybersecurity frameworks, understanding of various cybersecurity risk an organisation is more exposed to and other related areas.

IFAC "*Cybercrime Threatens Trust in Business – How Accountants Can Help*" mentions that supporting smaller businesses is an important opportunity for firms to provide useful business

advice. The professional accountant advisor can be particularly important in:

- Helping clients assess their governance and risk management - smaller businesses tend not to have strong risk management and control expertise. Accountants can ensure adequate business continuity and disaster recovery planning, particularly in the face of ransomware threats;
- Helping clients quantify risks and return on investment based on cost of breaches and stolen data and factors that impact cost; and
- Helping to mitigate risks with effective controls.

In order to effectively manage cyber risks, organisations should adopt a cyber risk management programme and the accountants should verify whether it is comprehensive and covers following major aspects[3]

- Have we performed a cyber business risk assessment to identify our key business risks?
- How do we know where to invest to reduce our cyber risks?
- What would be the disruption to our business from a cyber attack? How would it affect our business, brand, and reputation?
- How much revenue would we lose if our business processes were impacted by a cyber event?
- Have we identified our most critical business assets and do we understand their value to our adversaries?
- Have we looked at the value of these assets and business processes through the lens of the various threat actors?
- Do we have a cyber incident capability that will allow us to quickly respond to a cyberattack?
- How do we establish cyber risk tolerance to the organisation?
- How do we communicate about cyber risk to the Board and other stakeholders?
- Is my business resilient enough to survive a cyber attack?

Accountants can play a crucial role in enabling management to consider adoption of best practices

> The National Institute of Standards & Technology (NIST) Cybersecurity Framework (CSF) classifies the major functions of an information security program into five categories: identify protect, detect, respond and recover.

based on most commonly used control and cyber frameworks. Risk assessment would help to identify control weaknesses in various areas of the organisation. The National Institute of Standards & Technology (NIST) Cybersecurity Framework (CSF) classifies the major functions of an information security program into five categories: identify protect, detect, respond and recover. Accountants should make sure organisations are not focused solely on protection but also building the capability to detect when their organisation has been breached, and thus can respond and recover. Cybersecurity risk being one the most significant threat to organisations and accountants should share responsibility with board of directors and senior management in navigating cybersecurity threat landscape.of an information security program into five categories: identify protect, detect, respond and recover. Accountants should make sure organisations are not focused solely on protection, but also building the capability to detect when their organisation has been breached, and thus can respond and recover. Cybersecurity risk being one of the most significant threat to organisations and accountants should share responsibility with board of directors and senior management in navigating cybersecurity threat landscape.■

[3] *"Analytics and Cybersecurity: The shape of things to come" – CPA Australia*