INSTITUTE OF SINGAPORE CHARTERED ACCOUNTANTS

Cybersecurity Risk Considerations in a Financial Statements Audit

June 2018

Global Mindset, Asian Insights

Preface

Cybersecurity risk is a business threat that is becoming increasingly common and can pose immense challenges to entities in the current business environment. Over the years, cyber attacks have continued to proliferate, escalating in frequency, severity and impact, and impacting every industry.

This leads to the question of whether cybersecurity risk is relevant to the audits of financial statements, and the extent of the financial statements auditor's role. Does the financial statements auditor need to consider the cybersecurity risk of their client when planning and performing the audit?

This publication demonstrates how cybersecurity risk and cyber attacks can impact an entity's financial statements and its related audit. It also provides guidance on how cybersecurity risk considerations can be incorporated as part of risk assessment during audit planning, as well as the appropriate audit responses to the cybersecurity risk identified and cyber incidents that have occurred.

This publication is issued to provide practical guidance to financial statements auditors. It does not amend or override the Singapore Standards on Auditing (SSAs). Further, this publication is not meant to be exhaustive and reading it is not a substitute for reading the SSAs.

Contents

1 The Cyber Age, Sharing of Real Cases 3

2 Relevance of Cybersecurity Risk and Cyber Attacks to Financial Statements Audits 5

3 Cybersecurity Risk Consideration and Assessment 7

4 Audit Responses to Identified Cybersecurity Risk 12

5 Audit Responses to Cyber Attacks 13

6 Auditor Vigilance Towards Undetected Cyber Attacks 15

7 Key Learning Points 16

1 The Cyber Age, Sharing of Real Cases

As we move into the cyber age, technology has become a huge part of both our everyday lives and today's business environment, as more and more businesses increase their online presence and digital exposure by leveraging on technology in almost every conceivable aspect, be it as a revenue-generating measure or a drive towards raising productivity.

Take Amazon for example, which started from merely selling books through its website to becoming the world's largest e-commerce behemoth that offers almost everything including digital content. Its Web Services arm is a provider of cloud-based services for millions of business customers around the world. Another global technology pioneer, Alibaba, uses technologies such as artificial intelligence, virtual reality, cloud computing and mobile Internet technologies to power the global retail platform that connects millions of merchants and shoppers around the world.

Not just the big names, but many small start-ups are also using the engine of e-commerce to do business too.

But just as technology offers opportunities to many businesses, it also presents threats and challenges.

Over the years, cyber attacks have continued to proliferate, escalating in frequency, severity and impact. Existing prevention and detection methods appear largely ineffective against increasingly sophisticated cyber attacks. These cyber incidents[1] have impacted every industry, from financial services, retailers, entertainment, to healthcare providers.

For example, in the biggest known breach of a company's computer network, state-sponsored hackers attacked all three billion user accounts of Yahoo! in 2013, and made off with names, birth dates, phone numbers and passwords of users that were encrypted with security that was easy to crack. Following the disclosure of the cyber attack, Yahoo's Internet business was acquired by Verizon Communications at a substantially-reduced price that was US$350 million lower than the original US$4.8 billion agreed price.

Common Cyber Attack Techniques[2]

- Malicious software or ransomware, downloaded to a target computer, which can do anything from stealing data to encrypting files and demanding ransom
- Phishing emails crafted to trick victims into giving up passwords and other credentials or taking some other malicious action
- Denial of Service (DoS) attacks, which overwhelm a server, system or network with bogus traffic
- Man in the middle attacks, which fool the target computer into joining a compromised network

These techniques can be used in tandem. For example, the malicious attacker uses phishing emails to trick users into downloading malware or ransomware in hope to demand ransom over encrypted files.

[1] As defined in the Cybersecurity Bill, a cybersecurity incident is an act or activity carried out without lawful authority on or through a computer or computer system that jeopardises or adversely affects its cybersecurity or the cybersecurity of another computer or computer system.

[2] Josh Fruhlinger. *"What is a cyber attack? Recent examples show disturbing trends"*. CSO, IDG Communications Inc, March 2018.

1 The Cyber Age, Sharing of Real Cases

Elsewhere, criminals gained access to certain files in Equifax, a credit rating agency's system, by exploiting a weakness in its website software, resulting in a data breach involving highly sensitive and personal information belonging to 148 million customers. Its Chief Financial Officer said in November 2017 that this had cost the US credit bureau nearly US$90 million, a figure that was set to rise further. Health service entities in the United Kingdom were hit by the WannaCry ransomware attack in 2017, which scrambled data on computers and demanded payments of US$300 to US$600 to restore access, affecting the delivery of healthcare services.

In Singapore, the scale of the WannaCry ransomware attack was much smaller, affecting only certain shopping malls and stores. In 2017, a breach in an Internet-connected system at the Ministry of Defence resulted in the theft of the personal data of 850 national servicemen and employees. Earlier in 2014, the personal data of over 300,000 karaoke company K Box's customers were leaked as a protest against the government's announcement to match Malaysia's toll hikes at the Causeway. K Box was ordered by the Personal Data Protection Commission (PDPC) to pay a fine of S$50,000; PDPC's investigations had shown that the company did not have a sufficiently robust IT system.

Undeniably, cyber attacks can have a huge impact on businesses. This in turn begs the question whether financial statements auditors need to consider cybersecurity risk in the audits of their clients. What do you think?

The next section discusses how cybersecurity risk and cyber attacks are relevant to financial statements audits.

Impacts of Cybersecurity Breaches

Depending on the industry, the timing and duration, the extent of impact of a cyber attack on an entity could differ. Some of the common impacts include:

- Theft – loss of customer data, intellectual property, corporate information
- Financial losses – Loss of customers or revenue due to personal data loss (for example, payment information, healthcare data, or personal identifiable information), regulatory penalties for breaching data privacy legislation. Monetary losses can also be in the form of lost revenue due to extended period of downtime and cease of business operations.
- Reputational damage – loss of customer and stakeholder trust, leading to a loss of business. It can also impact the ability to attract suppliers and investors.
- Lawsuits and settlements – While most lawsuits happen in the first few years following the cyber attack, litigation can continue for years, creating huge unexpected costs, especially in severe breaches.

2 Relevance of Cybersecurity Risk and Cyber Attacks to Financial Statements Audits

Cybersecurity risk is relevant to every entity, except entities that run entirely on manual processes without any technology intervention or Internet connectivity which is very rare nowadays. Otherwise, cybersecurity risk will come into play albeit in varying degrees.

For an entity operating with a traditional business model with no online presence, intuitively, one may think that cybersecurity risk does not apply. But this cannot be further from the truth. A small mom-and-pop provision shop, for instance, could be using a point-of-sales system and technology to monitor its inventories and hence, is also exposed to cybersecurity risk.

While most of the victims of reported cyber attacks are big renowned businesses, small businesses also suffer from attacks. For small businesses, the likelihood of experiencing cyber attacks is just as high, if not higher, as their defences are typically less sophisticated. In fact, the impact could be more devastating, or attacks may even go undetected. While larger businesses will likely have the resources to recover, the chances of making a full recovery for smaller businesses are much lower. Potentially, it could even put them out of business.

Cybersecurity risk is hence relevant to almost every entity, be it big or small, and with or without an online retail platform.

This leads to the question of whether cybersecurity risk is relevant to the audits of financial statements. Do financial statements auditors need to consider the cybersecurity risk of their clients when planning and performing the audits?

Just as auditors would consider, as part of risk assessment, an entity's business risks in a financial statements audit, cybersecurity risk is an equally important risk area that cannot be ignored. As highlighted in the previous section, cyber incidents can result in financial consequences and therefore, have an effect on the financial statements. The financial impact on businesses can be massive and can cause fundamental enterprise-wide damage to entities. Cyber attacks can even go undetected, resulting in financial implications to the entity that may not have been reflected in the financial statements.

As such, cybersecurity risk is an essential consideration in every financial statements audit. Auditors should consider and assess the impact of such risk to the financial statements audit and where necessary, the extent of audit response required to address the risk.

Cybersecurity risk can affect different areas of a business: financial related as well as non-financial related.

For financial statements audit, the auditor only needs to consider those risks that could impact the financial statements and an entity's assets.

2 Relevance of Cybersecurity Risk and Cyber Attacks to Financial Statements Audits

Similarly, for actual cyber incidents. Let's look at some examples:

Case Study 1

Theft of New Technology

A technology company experienced a cyber attack which resulted in the theft of its patented new technology. This patented technology is recognised as an intangible asset and the amount is material. The theft indicates potential impairment issues that need to be further assessed by the company. Clearly, this incident has a financial impact to the company, and is likely to result in consequential effects on its future earnings and cash flows.

If the company does not have robust intrusion and detection controls, it may not even be unaware of the theft at year end, resulting in an undetected impairment issue and other potential costs not reflected in the financial statements.

Case Study 2

Deletion of Financial Reporting Data

A manufacturing company was subject to a cyber attack, which deleted some of its financial reporting data. Without appropriate data backup and recovery controls, the company may not be able to present complete and accurate financial information.

Case Study 3

Loss of Customer Information

A financial institution experienced a cyber attack which resulted in the loss of sensitive customer information (credit card information). There appear to be no direct impact to the financial statements or the entity's assets. However, there may be other consequences arising such as penalties for breaching data privacy, potential lawsuits from affected customers, reputation damage, or even potential impairment and going concern issues, especially when the breach is material.

Case Study 4

DoS Attack to Online Retail Platform

An online retailer experienced a distributed DoS attack to its online retail platform, an attack to make the online service unavailable by overwhelming it with traffic from multiple sources. This resulted in customers being unable to place online orders for an extended period. This represents a business risk to the retailer with an opportunity cost of lost revenue when the system is down rather than a direct impact to the financials of the entity.

Case Study 5

Connected Internal System

Similar circumstances to the above online retailer example. However, the retailer's online system is connected to its internal system that stores its confidential data and information. The retailer's confidential information may have been compromised from the attack and there could be an impact to the retailer's assets and financial information.

Case Study 6

Attack Detected by Intrusion System

A company experienced repeated rogue attacks on its network devices. However, this was stopped at the perimeter network by the company's intrusion detection system and hence the systems and applications that house financial statements related data were not affected. This represents a cyber attack with no real implications to the company.

The next few sections provide guidance on the identification and assessment of cybersecurity risk as part of risk assessment during the planning stage, and the appropriate audit responses to the risks identified and the cyber attacks that have occurred.

3 Cybersecurity Risk Consideration and Assessment

Risk assessment is critical in a financial statements audit. It is a key fundamental process which must be performed in the planning phase of every audit. Singapore Standard on Auditing (SSA) 315 (Revised)[3] requires the auditor to identify and assess the risks of material misstatement in the financial statements, through understanding the entity and its environment, including the entity's internal control. With an in-depth understanding of the entity's business and environment, it enables the auditor to identify the risks, and to design and implement appropriate audit responses to address those identified risks.

Incorporate Understanding the Cyber Environment of an Entity as Part of Risk Assessment

With technology driving today's businesses, the cyber environment of an entity is an area that the auditor should have a sufficient understanding on. Depending on the nature of the entity, cybersecurity risk may or may not be identified as a business risk that may result in risks of material misstatement, whether at the financial statement level or at the assertion levels.

The considerations detailed in the table below are designed to assist auditors gain a better understanding of an entity's cyber environment[4]. Some of these considerations may have already been included as part of understanding the entity and its environment, but may need to be expanded to specifically address cybersecurity risk. Depending on the extent to which the entity uses technology, the auditor should exercise professional judgement in determining which of these considerations are relevant to their client. For highly complex cyber environments, the auditor should consider involving subject matter experts.

Area	Considerations
Entity's Risk Assessment Process	If the entity has established its internal risk assessment process for financial reporting purpose: • Has the entity identified cybersecurity risk as a risk relevant to its financial reporting objectives? • How does the entity define cybersecurity risk for its business? Do any of these defined risks impact the internal controls relating to financial reporting? • Is the risk assessment conducted periodically to identify cyber threats, asset vulnerabilities, and potential business impacts, including those related to outsourced functions, third parties and business partners?

[3] SSA 315 (Revised), *Identifying and Assessing the Risks of Material Misstatement through Understanding the Entity and its Environment.*

[4] The considerations are **not** meant to serve as a cybersecurity readiness diagnostic whose objective is to assess the effectiveness of existing cybersecurity measures and/or to assess the entity's preparedness/readiness in managing cybersecurity risks. A cybersecurity readiness diagnostic is a much more extensive exercise, often involving specialists with deep expertise and is focused on cybersecurity risk, processes and controls of the entity as a whole and would include, amongst other things, testing the operating effectiveness of controls which mitigate cybersecurity risk, including operational and other matters not relevant to financial reporting.

3 Cybersecurity Risk Consideration and Assessment

Area	Considerations
Entity's Risk Assessment Process (Cont'd)	• Are there any cybersecurity risk assessment findings that could impact the financial statements? What actions has the entity taken as a result of its risk assessment? • Has the entity established risk-based cybersecurity programmes and controls to mitigate specific cybersecurity risk identified, or that otherwise help to prevent, deter and detect cyber incidents? • Does management monitor those programmes and controls and how is this done? • Is the entity's cybersecurity programme based on a recognised standard[5]? • Has the entity invested in, or plans to invest in, security products? For example, intrusion prevention and detection systems, anti-malware and firewalls.
Roles and Responsibilities	• Has the entity established roles and responsibilities over cybersecurity? Who is responsible? • Has the Board of Directors, management or Audit Committee discussed about cybersecurity? If yes, has the entity taken any actions as an outcome of those discussions?
Safeguarding of Assets	• Are there material digital/electronic assets on the balance sheet which are subject to cybersecurity risk? For example, intellectual property, patents and copyrighted material. • If so, has management implemented a formal process for identifying, classifying and reviewing these assets and prioritising their protection based on data classification, criticality and business value? • Does the nature of the business of the entity require collection of personal data? • Has the entity created an inventory/register of its information assets that require protection? For example, customer database, trade secrets, key projects information and financial data.

[5] For example, the National Institute of Standards and Technology (NIST)'s Cybersecurity Framework, and Information Security Standard 27001. NIST is a non-regulatory agency of the United States Department of Commerce.

3 Cybersecurity Risk Consideration and Assessment

Area	Considerations
Safeguarding of Assets (Cont'd)	• Has the entity designed and implemented policies and procedures that consider cybersecurity risks? What is the entity's formal security administration process to grant, modify or remove access to data and systems in a controlled manner? Does the entity perform access reviews on a periodic basis to ensure that access is commensurate with job roles and responsibilities, including privileged access? • Does the entity periodically maintain and test backups of critical data and systems? • Does the entity provide training to employees concerning information security risks and responsibilities? For example, periodic security awareness training programme, personal data protection law and policies training, and guidance on use of social media for all employees. • How does management monitor whether there has been unauthorised access to digital/electronic assets and assess the impact on financial reporting?
Security Breaches	• Does the entity have a mechanism designed and implemented to detect anomalous cyber activity or cyber incidents? • Has the entity been subject to cyber incident or data breach? For example: - Malware detected on entity's devices - Access to systems was blocked or impaired by a DoS attack - Availability of entity's web or network resources was impaired by a software or hardware malfunction - Breach by an unauthorised user - Theft of data - Compromise of a third party system used to remotely access the entity's network. For example, web services company which is given the access to an entity's network in order to build and maintain the entity's website, was compromised. - Compromise of a third party system that stores and/or processes the entity's digital/electronic assets - Fraudulent activities, for example, fund transfers, related to cybersecurity breach • If yes, what was the nature of this incident? For example, summary of incident, root cause analysis, impact and remedial measures. Did this incident impact financially significant systems and/or data? • Does the entity have an IT security incident response plan that is tested and updated on a periodic basis? • Does the entity have any crisis management and communication plan in place?

3 Cybersecurity Risk Consideration and Assessment

As part of planning the approach for understanding ITGCs in a financial statements audit, an IT system is considered to be in-scope for the financial statements audit when IT dependencies (i.e. automated controls) are identified to be relevant to financial reporting. For example, the daily batch job posting of journal entries from the inventory system to the general ledger system; and the classification of receivables into appropriate aging categories by an accounts receivable application, would be in-scope.

The auditor should obtain an understanding of the ITGCs, evaluate their design and determine whether the ITGCs that are relevant to the audit have been implemented. The IT systems and/or data that are relevant to the audit are usually a subset of the aggregate IT systems and data used by an entity to support its overall business operations and may be separately managed or controlled. The auditor's responsibilities do not encompass a comprehensive evaluation of the risks and controls across the entity's entire IT environment.

With a robust understanding of the entity and its environment, including the entity's cyber environment, the auditor would be able to identify specific risks arising that may result in risks of material misstatement. The auditor should also determine whether any of the risks identified are, in the auditor's judgement, significant risks that require special audit consideration.

Case Study 7

Weak Security Process to Grant, Modify and Remove Access to Data and Systems

A company has no formal process in place to grant or modify system access and the controls to ensure appropriate access to financial reporting databases and applications are weak. Employees are given access to systems/applications which they do not require for their work (for example, the accounts receivable officer's access rights include the right to record journal entries into the general ledger). This represents a risk that may result in material misstatement to the financial statements. The auditor may also determine that the risk is significant that requires special audit consideration.

Case Study 8

Material Information Assets with Weak Control Environment

An advisory company holds a huge database of client confidential information. The company does not have a data protection officer to develop and implement data protection policies. Control of access to client information is weak and unused accounts are not disabled. This represents a business risk to the company. However, the auditor may not necessarily identify this as a risk of material misstatement in the financial statements. Nevertheless, the auditor should remain alert of potential breaches, for example, leakage of client confidential information, that may have occurred that can bring about financial implications to the company.

3 Cybersecurity Risk Consideration and Assessment

Case Study 9

Cyber Attack Resulting in Significant Risks Identified

A technology company experienced a cyber attack resulting in the theft of material patented new technology, which is recognised as an intangible asset. Arising from this, the auditor determines that assessment of impairment of the intangible asset will be challenging and is subject to significant estimation uncertainty and requires management to exercise significant judgement and develop subjective assumptions. The auditor hence identifies a significant risk related to the valuation assertion of the intangible asset.

In addition, upon obtaining an understanding of the company's cyber environment, the auditor notes that the company's systems are inter-connected, and its controls and security measures are generally weak and not kept up-to-date. The attack could have compromised other confidential data of the entity, including financial data that are housed together. In such circumstances, the auditor may determine that the risk is pervasive to the financial statements as a whole, and can potentially affect many assertions.

The next two sections discuss possible audit responses to the risks identified in each of the above scenarios.

Re-Assessing Cybersecurity Risk Every Year

Changes in the risk environment and the ways in which businesses operate mean that business risks do not remain constant. In one year, cybersecurity risk may not have been identified as a key business risk that may result in risks of material misstatement, but this does not mean that the same will apply for the next year. Significant and rapid changes in information systems, incorporation of new technologies into production processes, or expansion of operations can bring about new cybersecurity risk. Take the example of a brick-and-mortar retail shop selling fashion apparel which switches to a predominantly online retail platform – the extent of exposure to cybersecurity risk would have increased drastically with the change in its business model; it is hence important that cybersecurity risk be assessed from year to year.

4 Audit Responses to Identified Cybersecurity Risk

Based on the auditor's understanding of the entity and its environment, the auditor shall design and implement audit responses to address the assessed risks of material misstatement at both the financial statement and assertion levels.

Help Tips

Consider involving IT specialists if risks are identified

If the auditor identifies cybersecurity risk that may result in risks of material misstatement at the financial statement level, the auditor should take guidance from SSA 330[6] to design and implement overall responses. This may include assigning more experienced staff or those with special skills such as IT specialists to the engagement, incorporating additional elements of unpredictability in the selection of further audit procedures to be performed and modifying the nature of audit procedures to obtain more persuasive and corroborative audit evidence.

When ITGCs are tested in the financial statements audit, the auditor will assess whether the operating effectiveness of relevant IT dependencies/automated controls can be relied upon. Where deficiencies are identified, the auditor should consider compensating controls that the entity has in place to reduce the impact of the ITGCs deficiencies, for example, management review of logs to detect potential errors and anomalies.

In addition, the auditor should carefully consider the results of the tests of ITGCs and the identified deficiencies, if any, and evaluate the pervasiveness of the deficiencies across the entity. This may have an impact on the audit. The auditor would have to determine whether continued reliance can be placed on the IT dependencies/automated controls in the audit; consider the need to revise the initial risk assessment, and the impact to the nature, timing and extent of other planned audit procedures. The auditor would have to respond to the ineffective IT control environment by for example, obtaining more extensive audit evidence from substantive procedures.

If the auditor identifies cybersecurity risk that may result in risks of material misstatement at the financial statement level or the risks identified are, in the auditor's judgement, significant risks that require special audit consideration, the auditor should consider the use of subject matter experts. The auditor may suggest management to engage external IT consultants to perform a cybersecurity readiness diagnostic, which is a much more extensive exercise, involving specialists with deep expertise and is focused on cybersecurity risk, processes and controls of the entity as a whole and would include, amongst other things, testing the operating effectiveness of controls which mitigate cybersecurity risk.

Audit Response to Case Study 7 in Section 3:

The company with no formal process in place to grant or modify system access. In particular, the accounts receivable officer's access rights include the right to record journal entries into the general ledger. To respond to the risk identified, the auditor may lower the materiality level and/or modify the nature and extent of journal entries to examine or adjustments to be made throughout the period. The auditor could also consider testing all journal entries.

Audit Response to Case Study 8 in Section 3:

For the advisory company with weak protection of its client information, the auditor can design overall responses such as engaging its internal IT specialists to look at key controls and emphasising to the engagement team the need to be alert to events or conditions that may indicate a possible breach.

[6] SSA 330, *The Auditor's Responses to Assessed Risks.*

5 Audit Responses to Cyber Attacks

As can be seen in the previous sections, entities that fall victim to successful cyber attacks may incur substantial costs and suffer significant damage. As such, auditors should understand the nature and cause of the incident, carefully consider the costs and any adverse consequences arising from the cyber incident, and evaluate the impact to the financial statements audit.

Help Tips

Consult the experts, especially for significant breaches!

Some cyber incidents clearly have an impact to financial reporting, for example, those that relate to unauthorised access to financial reporting applications, data and digital assets recorded on the balance sheet. For example, Case Study 9.

Audit Response to Case Study 9 in Section 3:

The technology company which experienced a cyber attack resulting in the theft of its patented technology - the auditor would have to design procedures that specifically respond to the risk identified which could include:

- Understanding management's process to review and assess the impact of the theft of its patented technology. This will include direct financial losses and potential damage to its competitive advantage, future earnings, etc;
- Critical assessment of the assumptions, estimates and judgements made by management in ascertaining the impairment of the intangible asset;
- Sensitivity analysis of possible changes in the estimates that may result in material impact to the financial statements;
- Consideration of the impact to the company's other assets;
- Assessment of the impact of the attack on the entity's future revenue, potential litigation expenses, cybersecurity protection costs, etc and future cash flows, which will affect any impairment assessment; and
- Assessment of whether the breach may indicate going concern issues for the entity.

5 Audit Responses to Cyber Attacks

Many of the common cyber attacks are those that involve the theft of customers' personal data. While it may not appear to have a direct impact on the financial statements or the entity's assets, the auditor would still have to consider:

- Remediation costs that the entity would have to incur, such as costs to repair the system damage and compensation offered to customers to maintain business relationships;
- Regulatory inquiries and punitive penalties for breaching data privacy;
- Potential lawsuits from affected customers and associated legal fees;
- Reputation and brand damage, and its impact to revenue, value of inventories, intangibles (impairment issues); and
- Going concern issues.

It is also important to recognise that the impact of cyber attacks may not be limited to or contained within a single component of a system or network. Potential systemic risks may be created and the impact of security breaches to businesses may be more extensive than it initially appears to be.

6 Auditor Vigilance Towards Undetected Cyber Attacks

Cybersecurity risk may not have been identified as a key area of focus by the auditor as part of risk assessment, but this does not necessarily mean that no breach has occurred.

Auditors should still maintain their professional scepticism when carrying out their audit as there could be events or conditions that may indicate a possible breach. Some businesses with weak IT programmes and controls may not even realise that they have been the subject of a cyber attack. Auditors should hence conduct their audit with a mindset that recognises the possibility that an actual cyber attack may have happened, regardless of any past experience with the entity and regardless of the auditor's belief about the entity's cybersecurity defence abilities.

During the course of the audit, the auditor should also inquire management regularly about whether management has knowledge of any cyber incident or suspected cyber incident affecting the entity. Through the performance of the usual audit procedures, it is still possible to identify undetected cyber incidents or incidents not disclosed to the auditor.

Case Study 10

A traditional manufacturing company has no online presence. The auditor performed a risk assessment and did not identify cybersecurity risk as giving rise to risks of material misstatement in the financial statements. Accordingly, the auditor obtained an understanding of the ITGCs, designed appropriate procedures and performed testing over the relevant ITGCs. IT specialists were not engaged to perform additional work on cybersecurity testing.

During the course of the audit, while performing substantive testing of the revenue accounts, the auditor noted exceptions. There were goods delivered with supporting delivery notes and acknowledgement by customers. However, the sales transactions were not in the general ledger and accordingly not reflected in the financial statements. Upon enquiries and further investigations by the company, it was then discovered that it had been the subject of a cyber attack by a disgruntled employee who deleted some of its sales transactions. As there was no management review of logs in place to detect potential errors, anomalies or malicious attacks, the incident went undetected even to the company itself.

In this situation, the company would also have to assess if unauthorised changes had been made to its other financial records. Further, in such scenarios where financial records have been altered, if entities do not have appropriate backups and recovery contingency plans, they may not be able to present complete and accurate financial information.

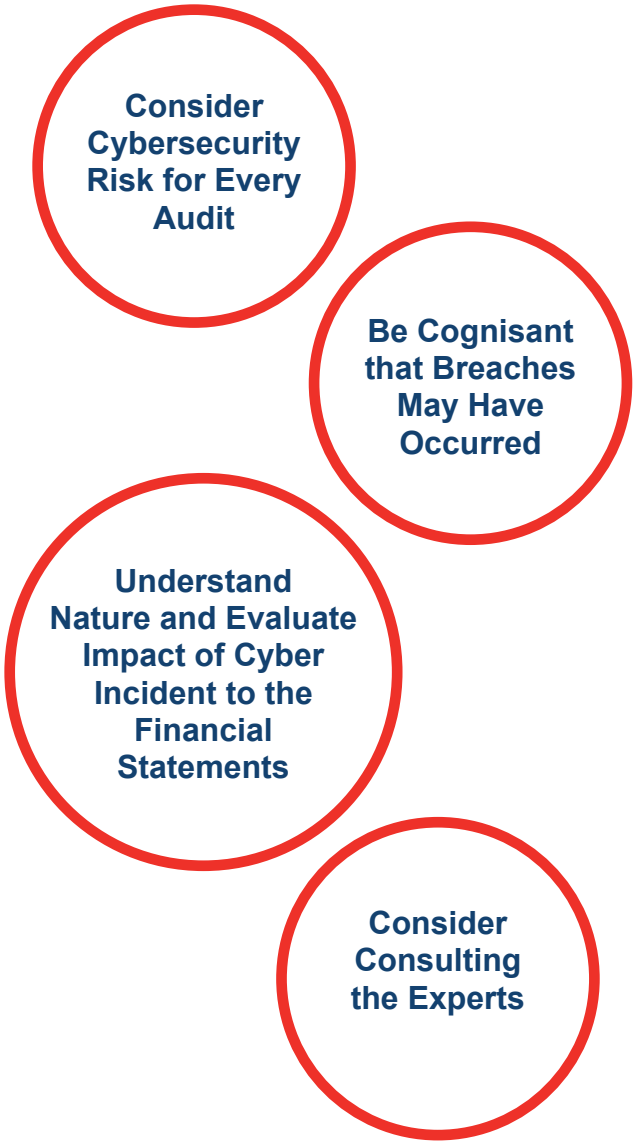
Although it is not the responsibility of the auditor to detect every cyber incident that results in alteration to the financial records of an entity, unauthorised material changes to financial records have a good chance of being detected from the performance of robust and appropriate audit procedures. Auditors should hence be more vigilant, if the auditor is aware that the entity does not have robust IT systems and controls in place or when a higher cybersecurity risk has been identified.

7 Key Learning Points

Financial statements auditors should consider and assess cybersecurity risk as part of risk assessment for every audit. The conclusion may be that cybersecurity risk is not an area that requires special audit attention, but the assessment is still required nonetheless to make such a determination. Auditors should also be cognisant that breaches may have occurred but remained undetected.

In addition, it is important to note that risk assessment continues throughout the engagement. New information or audit evidence may be obtained during the audit which would have changed the auditor's risk assessment if such information was available when the initial assessment was made, for example, the auditor was subsequently made aware of a past cyber incident. The auditor should revise the assessment and modify the audit plan and procedures accordingly.

Where cybersecurity risk has been identified as a key business risk that may give rise to material misstatement of the financial statements, the auditor should consider involving subject matter experts. When a cyber incident has occurred, the auditor would have to understand the nature and cause, determine whether additional audit procedures or an alteration in audit approach is necessary, and evaluate the impact to the financial statements. Where necessary, the auditor should also consider involving subject matter experts.



About the Institute of Singapore Chartered Accountants

The Institute of Singapore Chartered Accountants (ISCA) is the national accountancy body of Singapore. ISCA's vision is to be a globally recognised professional accountancy body, bringing value to our members, the profession and wider community. There are over 32,000 ISCA members making their stride in businesses across industries in Singapore and around the world.

Established in 1963, ISCA is an advocate of the interests of the profession. Possessing a Global Mindset, with Asian Insights, ISCA leverages its regional expertise, knowledge, and networks with diverse stakeholders to contribute towards Singapore's transformation into a global accountancy hub.

ISCA is the Administrator of the Singapore CA Qualification and the Designated Entity to confer the Chartered Accountant of Singapore - CA (Singapore) - designation.

ISCA is a member of Chartered Accountants Worldwide (CAW). CAW brings together 12 chartered accountancy bodies connecting and representing the interests of over 1.7 million members and students globally.

For more information, visit www.isca.org.sg.

Contributor

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 158 countries with more than 236,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.

60 Cecil Street,
ISCA House,
Singapore 049709
TEL +65 6749 8060
FAX +65 6749 8061
EMAIL isca@isca.org.sg
WEBSITE www.isca.org.sg