AICPA & CIMA

CGMA cybersecurity tool

Risk, response and remediation strategies 2021

Updated August 2021

About the Association

The Association of International Certified Professional Accountants® (the Association) is the most influential body of professional accountants, combining the strengths of the American Institute of CPAs® (AICPA®) and The Chartered Institute of Management Accountants® (CIMA®) to power opportunity, trust and prosperity for people, businesses and economies worldwide. It represents 650,000 members and students across 179 countries and territories in public and management accounting, and advocates for the public interest and business sustainability on current and emerging issues. With broad reach, rigor and resources, the Association advances the reputation, employability and quality of CPAs, CGMA® designation holders and accounting and finance professionals globally.

Acknowledgments

Ken Witt, CPA, CGMA, of the Association of International Certified Professional Accountants prepared the update of this tool and the original tool, which was based on a webcast series that Kenneth R. van Wyk, President and Principal Consultant of KRvW Associates LLC presented for AICPA & CIMA members.

Contents

2 Introduction

3 Understanding cybersecurity
- What problems do we face today?
- Who are the bad actors?
- Risk of security vulnerabilities

5 Cybersecurity fundamentals
- Cybersecurity objectives
- Data backup
- Security controls: protection, detection, response

10 Applied cybersecurity
Centralised management: desktops, laptops, mobile devices, networks and applications
- Centralised monitoring: SIEMs and SOCs

14 Advanced topics
- Forensic analysis
- Malware analysis
- Penetration testing
- Software security

16 Recent trends in cybersecurity
- Cyber actions and actors
- Data breach cost components
- Minimising financial and brand impacts

18 Cybersecurity and small business
- Small business incidents and impacts
- Small business resources

20 Cybersecurity governance, risk and reporting
- Privacy and Cybersecurity Regulation
- Risk management, reporting and oversight

22 Appendix I: Cybersecurity insurance

23 Appendix II: Cybersecurity risk management reporting framework

25 Appendix III: Center for Internet Security — CIS Controls v8

29 Appendix IV: CISA MS-ISAC *Ransomware Guide* – Part 2: Ransomware Response Checklist

31 Additional reading and resources

Introduction

Cyber risk has become a front-and-center issue in today's global economy. The media is rife with reports of cyberattacks ranging from major customer records thefts and health care records breaches, to political incidents. This increase in frequency and magnitude of cyberattacks, data breaches and ransomware requests has prompted public sector and private sector responses around the world

The United States formed a cross-government task force to oversee a range of initiatives, including defensive and offensive measures against ransomware attackers, tracking ransom payments on cryptocurrency platforms and coordinating activities with U.S. allies. Rewards of up to $10 million are also being offered for information that helps halt or punish hackers that lock up computers at vital U.S. industries and hold them for ransom.

The 2021 World Economic Forum Global Risks Report ranks 'cybersecurity failure' as ninth among the top ten likely risks. This characterisation is a combination of data fraud or theft, and cybersecurity attacks in previous rankings. Cybersecurity failure is defined as follows:

> *Business, government and household cybersecurity infrastructure and/or measures are outstripped or rendered obsolete by increasingly sophisticated and frequent cybercrimes, resulting in economic disruption, financial loss, geopolitical tensions and/or social instability.*

In addition to rankings, the 2021 WEF report surveyed the participants regarding their perceptions. When asked, 'When do respondents forecast risks will become a critical threat to the world?'

- 39% indicated that cybersecurity failure represented a 'clear and present danger' in the short-term (0–2 years), and
- 49% forecast cybersecurity failure as having 'knock-on effects', or medium-term risk (3–5 years).

A closely related new risk characterization in the WEF risk report is 'IT infrastructure breakdown', which is defined as:

> *Deterioration, saturation or shutdown of critical physical and digital infrastructure or services as a result of a systemic dependency on cyber networks and/or technology: AI-intensive systems, internet, hand-held devices, public utilities, satellites, etc.*

This risk was also projected to have medium term 'knock-on effects' by 53.3% of the respondents.

One global response to this ever-present global risk is the World Economic Forum's Centre for Cybersecurity, an independent and impartial global platform committed to fostering international dialogues and collaboration between the global cybersecurity community both in the public and private sectors.

The centre has three objectives:

- **Building cyber resilience** — Enhance cyber resilience by developing and scaling forward-looking solutions and promoting effective practices across digital ecosystems.
- **Strengthening global cooperation** — Increase global cooperation between public and private stakeholders by fostering a collective response to cybercrime, and jointly addressing key security challenges.
- **Understanding future networks and technology** — Identify future cybersecurity challenges and opportunities related to Fourth Industrial Revolution technologies and envision solutions which help build trust.

Understanding cybersecurity

Understanding cybersecurity in today's complex digital world begins with knowing what the most common threats are, who the potential 'bad actors' are, and what we can do to shore up our defenses.

What problems do we face today?

The most common threats to our cybersecurity include malware, including ransomware, botnets, malvertising, phishing and application attacks.

- **Malware** is the term used for malicious software intended to do any number of things ranging from stealing credentials, other information or money to the general wreaking of havoc, or denial of service. Some of the more typical types of malware include:
- **Ransomware** is a type of malicious software designed to block access to a computer system until a sum of money is paid.
- **Botnets** are networks of interconnected computers that are infected with a 'botnet agent' designed to do the attacker's bidding.
- **Malvertising** involves injecting malicious or malware-laden advertisements into legitimate online advertising networks and web pages. Malvertising is a serious threat that requires little or no user interaction.
- Phishing usually is an email designed to lure the reader into doing something ill-advised by masquerading as a trustworthy source or legitimate enterprise. Phishing requests to execute an attachment to the email or click on a link are designed to install malware on the user's computer, generally for the purpose of stealing money. Phishing can also involve more direct requests to provide private information, such as passwords, credit card account details or other sensitive data.
- Application attacks are increasingly common as application development is moving more and more to the web. In addition to complex business applications being delivered over the web, our personal mobile phone applications and our home devices connected to the internet via Internet of Things platforms that create widespread vulnerabilities.
- Application attacks, while varied in nature and design, usually have the same intents and purposes as malware attacks — stealing data from database servers, running attack scripts on other users' computers, stealing user credentials, etc.

Cost of doing business in the digital age

- **$5.52 million** — Average cost of a breach at enterprises of more than 25,000 employees
- **$2.64 million** — Average cost for organisations under 500 employees
- **39%** of the total cost attributable to lost business
- **80%** of breaches included customer personally indentifiable information (PII)
- **$150** — Average per record cost of customer PII

Companies that experienced breaches of more than 1 million records continued to see costs that were many times the overall average.

Ponemon Institute/IBM Cost of a Data Breach Report 2020

Who are the bad actors?

While the term 'hacker' may have had its origin as a term used to describe especially talented computer programmers and systems designers, and may still include those considered 'curious' hackers, the term has become much more widely used to describe computer intruders or criminals with less-than-desirable intent. In addition to basic thieves, these 'bad actors' can be outsiders, such as business competitors or nation states. They can also be insiders, such as disgruntled or otherwise malicious, employees.

Risk of security vulnerabilities

Cybersecurity vulnerabilities can be technical or procedural. Technical deficiencies that create exposure to sensitive functionality or information include software defects and the failure to use security protections, such as encryption adequately. Procedural deficiencies can be IT-related, including system configuration mistakes, or failure to keep up with software security updates. However, many procedural deficiencies are user-related, such as poorly chosen passwords.

Whatever the cause, when exploited, these vulnerabilities can be costly and result in:

- **Downtime** — Loss of business production or revenue generation opportunities
- **Tarnished reputation** — Company and brand value negatively affected
- **Customer flight** — Especially critical with increasing level of e-commerce
- **Legal consequences** — Fines, lawsuit costs and settlements can be staggering
- **Industry consequences** — Health care records breaches have been extensive

Cybersecurity fundamentals

Businesses must address these risks and implement security measures to protect their information assets and ensure the ongoing viability of their enterprise.

Cybersecurity objectives

As outlined in Appendix II, the AICPA has developed a cybersecurity reporting framework that organisations can use to demonstrate to key stakeholders the extent and effectiveness of an entity's cybersecurity risk management programme. A critical element of any cybersecurity risk management programme is the formulation of objectives by management.

Management establishes cybersecurity objectives that address cybersecurity risks that could affect the achievement of the entity's overall business objectives (including compliance, reporting and operational objectives). They vary depending on the environment in which the entity operates, the entity's mission and vision, the overall business objectives established by management, risk appetite and other factors.

Key cybersecurity objectives outlined in the framework resource Description Criteria for Managements Description of the Entity's Cybersecurity Risk Management Programme include:

- **Availability** — Enabling timely, reliable and continuous access to, and use of, information and systems
- **Confidentiality** — Protecting information from unauthorised access and disclosure, including means for protecting proprietary information and personal information subject to privacy requirements
- **Integrity of data** — Guiding against improper information modification or destruction of information
- **Integrity of processing** — Guarding against the improper use, modification, or destruction of systems

Data backup

These objectives are commonly referred to as the CIA of cybersecurity — confidentiality, integrity and availability. In this era where there is an extensive market for personal information on the dark web, along with the proliferation of ransomware attacks, ensuring the availability of data is key. You may not be able to totally prevent a breach. But if you back up your data, you may not have to consider paying a ransom. Since breaches can sometimes go undetected for quite some time, it is important to have multiple versions of backups, with some backups being stored off-site to preclude ransomware attackers from encrypting backup files as well as those that are currently active.

One common method for maintaining backup files of data is the 3-2-1 model. This model suggests that you need three copies of your data, two of which are backups on different media and one being stored off-site.

See Appendix III for a summary of key steps to take in the event of a ransomware attack, which include immediately isolating infected systems to minimise the impact.

Data backup 3-2-1

3 – Production copy plus two backups

2 – Backup copies on two different media

1 – backup copy off-site

Security controls: protection, detection, response

To achieve these security objectives and mitigate these risks, implement security mechanisms to protect information assets, detect malicious activity when (not if) it occurs and respond effectively to that malicious activity to minimise the impact on the business.

Different controls need to be implemented at different levels of the software, across the spectrum of components outlined:

Things we protect

- Servers
- Desktops
- Mobile devices
- Networks
- Data storage
- Business applications

How we protect them

- Policies and policy management
- Software updates
- Configurations
- Security products
- Application software controls

Protection — First and foremost, we try to protect our information assets and systems against attack. Protection strategies are our first line of defense and breaches usually are a failure of protection strategies.

Protective controls include:

- Identification — To have confidence in accountability for users, whether individuals or interactive system components, we need to have identification (e.g., usernames).
- Authentication — We also need to be able to authenticate that identification (e.g., passwords, fingerprints, etc.).
- Authorisation — In addition to authentication, we need to make sure user is authorised to conduct transaction — verify the user's level of authority for particular type of access or transaction.
- Protect secrets such as encryption of credit card information.
  - At rest while being stored
  - In transit while being transmitted

Strong identification

Common methods of identification and authentication that are easily implemented:

- Something you know, such as passwords; quality of passwords is increasingly important.
- Something you have, such as tokens that are sent to you via text message.
- Something you are, such as biometrics: fingerprint, facial, palm print scans.
- Two factor authentication (2FA) such as the combination of a password and token are increasingly in use today.

Certificates are a significant underpinning of security systems, especially where payments or particularly sensitive information is involved. Certificates are used for all kinds of practical applications, including the transmission of confidential information and the digital signing of documents.

Certificates are used in what is referred to as a 'handshaking' procedure to verify the identity of the sender, enable the transmission of encrypted confidential information privately, and also enable the receiver to know whether the information has been tampered with via the use of tamper-evident seals.

There is a public half and private half of a certificate. It is critical that the private half of the certificate be kept secure and not passed between parties. Within an organisation, certificates can be centrally managed to enable users to access the public certificate for someone to whom they want to send encrypted information. For external use, public certificates are issued by third-party certificate authorities that verify the identification of parties using them.

Man-in-the-middle attacks

Certificates are essential for circumventing man-in-the-middle (MitM) attacks. MitM is the term used for attacks in which the attacker independently makes connections with the victims and relays messages between them to create the impression that they are communicating with each other when, in fact, the attacker is controlling the conversation.

Machine Identity

One emerging trend with respect to identification and authorisation protocols is machine identity. Similar to the protective controls for individual access and exchange of data, internet-connected or IOT devices require credentials to authenticate and securely connect to other devices. Unfortunately, according to research done by Ponemon on behalf of Key Factor, these 'machine identities' are often left unmanaged and unprotected.

In the 2020 Hype Cycle for identity and Access Management Technologies, Gartner introduces a new category: Machine Identity Management. The addition reflects the increasing importance of managing cryptographic keys, X.509 certificates, SSH keys and other non-human identities.

Ponemon/Key Factor — State of Machine Identity Management 2021

Detection — In addition to protective or preventive strategies, it is also essential that entities employ detection strategies to identify when threats occur — essentially the computer equivalent of the security camera.

When an organisation is attacked, the key role of an incident response team is to serve as an advocate for the business and 'keep the patient alive.'

Common detection strategies include:

- **Event monitoring** — Documentation of events logged into files can be reviewed to look for unusual patterns of activity.
- **Intrusion detection and prevention systems** — Sophisticated applications are available that enable the ability to perform ongoing monitoring.
- **Threat monitoring** — Security community can study the tools and techniques that attackers use to develop 'threat intelligence' that can be used to inform the development of new controls.
- **User reports** — User reports can also help identify unusual activity.

Response — Part of the evolution of cybersecurity is the advent of Computer Incident Response Teams (CIRTs), sometimes referred to as Computer Security Incident Response Teams (CSIRTS).

The primary functions of the response team are to:

- Reduce losses
- Help the business get back into business as soon as possible
- Support investigations when necessary — law enforcement, forensic
- Provide decision support during incident-situational awareness, plan of action, informed decisions
- Facilitate crisis communications — customers, law enforcement, media, etc.

Breach identification and containment

The time to identify and time to contain a data breach have not varied much in recent years.

280 days – Average time to detect and contain a data breach

315 days – Average time to detect and contain a data breach caused by a malicious attack

$1.12 million – Average cost savings of containing a breach in fewer than 200 days vs. more than 200 days.

Ponemon Institute/IBM Cost of a Data Breach report 2020

Applied cybersecurity

Centralisation is an important element of cybersecurity with respect to implementing preventive and detective controls and responding to cyber breaches, especially when considering enterprise-level systems with huge numbers of desktop computers, laptops and mobile devices.

Centralised management

Desktops — Modern operating systems are fortunately rich in terms of security features. Centralised management is a key way to control and orchestrate key security features. The ability to 'push' security protocols, software updates and security update 'patches' to remote users enables the scalability of security for large enterprise-level systems. Centralisation also provides the ability to maintain a directory of user profiles that enables users to access their information from multiple locations.

Laptops — While many security features are common between desktop and laptop computers, the inherent mobility of laptops, especially the risk of lost or stolen devices, presents some unique challenges. Whole disk encryption, whether a feature of the operating system or an endpoint product, is an essential feature to ensure the security of data on laptop products.

Mobile devices — There are third-party mobile device management (MDM) products to facilitate the centralised management of such devices. Some companies consider it important to have company-owned devices and will implement a configuration profile that will prohibit the download of non-company applications.

Many companies have what are referred to as bring-your-own-device (BYOD) programmes. To ensure security for these employee-owned devices, they require employees to submit those devices for company-wide management, similar to laptops. To allow for flexibility in the implementation of security policies, companies can create different configuration profiles for different classes of users for their mobile devices.

Network configuration — Another critical component that companies use to enforce policies across the spectrum of corporate networks, including desktops, laptops and mobile devices, is network configuration. The value of these network-level controls is that they are exceedingly difficult to circumvent.

Network firewalls — Pre-defined policies about who can access what can restrict access to social media or other categories of websites. Access control lists implemented at the network level can provide people with access to sites that may not be allowed to others. The communications team, for example, may be authorised to have access to social media sites for company purposes.

Application firewalls — In addition to network data while activity is occurring — firewalls intended to restrict access to authorised individuals — application firewalls can also be used.

Antivirus and endpoint products — In addition to centralised management of security features, most organisations also commonly use 'endpoint products' to augment the features that the operating system provides. Endpoint products are especially valuable in ensuring security in enterprise-level systems that multiple users access from multiple locations with multiple devices. These products can ensure compliance with the organisation's policies and standards in addition to verifying the integrity of application products and detecting viruses, blocking activity if issues are found.

VIP travel: 'Throw-away systems'

Many companies with employees or executives travelling to remote locations set up 'traveler laptops,' especially for the trip. Whole disk encryption is used, and only the data necessary for the trip is set up on the device. When the executive returns, any files used on the trip are retrieved while the operating system and files are completely removed and reinstalled for future use.

Some companies travelling to particularly sensitive locations actually destroy the computer, rather than run the risk of compromising proprietary information.

Centralised monitoring

Fortunately, as enterprise systems with hundreds or even thousands of laptops have become the norm for organisations, centralised monitoring of systems activity has fortunately also evolved over time. Important components of centralised monitoring include:

Event logging and aggregation — All modern computer operating systems keep a ledger of their activity — who logged in? What programmes did they run? What files were accessed? What were the failures as well as the successes? The event logging on operating systems is largely superficial. However, it still is essential for administrative and accountability purposes as well as potential forensic use.

It's best to send logs to a central monitoring point, usually in the data center or security operations center (SOC). In addition to professional considerations, privacy considerations dictate that only security personnel view these 'logs.' While the logging of this information is critical for forensic purposes, the real value is to look at this data while activity is occurring.

Container applications: Creating a "world within a world"

Containerisation is very useful for securing data on mobile devices. It involves encapsulating an application in a container with its own operating environment. Containers allow you to put software written for your company environment in a container so employees do not need to use the device applications for company data. The container is entirely encrypted so you can keep your company data in the enclave and keep personal data out. These are popular for enterprise deployments, especially for basic services such as exchange email, calendar sharing, etc.

Security information and event management (SIEM) — SIEM systems have been developed to make this monitoring more effective. SIEMs analyse all of the available data and look for specific patterns in the data that might suggest a possible attack or security compromise.

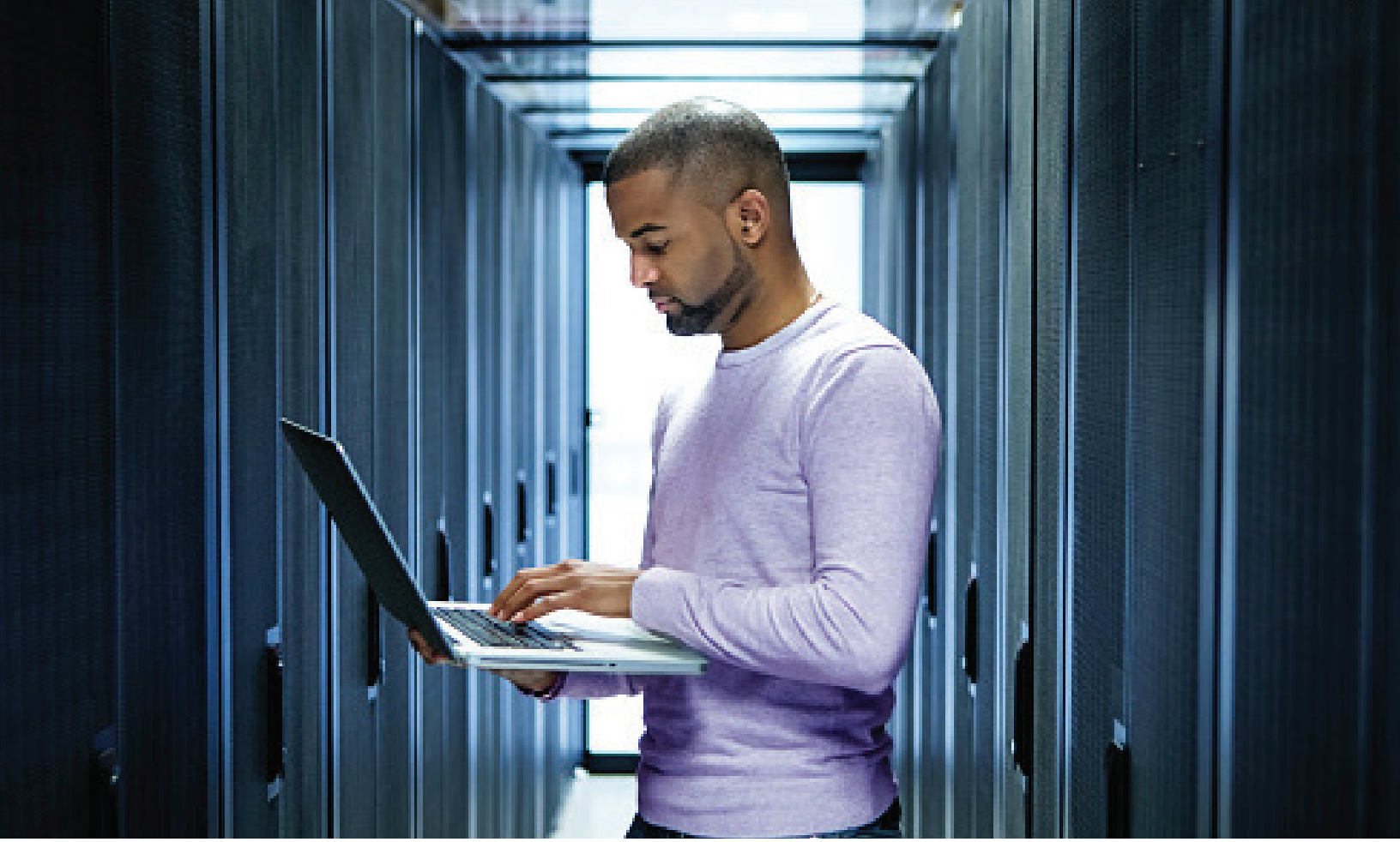
SIEMs dive deeply into possible incidents, automating the process of analysing what might be referred to as 'needle-in-the-haystack' scenarios.

Modern Security Operations Center (SOC) functions — SOC environments have matured over time and have a range of important teams, or functions:

- Incident response team — When the team monitoring the SIEM identifies a potential threat, it initiates an incident response process. The team's focus is on business continuity.

The incident response team is in effect the 'EMT' of the IT world.

Threat intelligence team — The mission of the threat intelligence team is to monitor current trends, especially in the specific industry sector in which the organisation is involved. Threat intelligence teams feed that information to the team that is responsible for monitoring activity via the SIEM.



- Hunt team — The mission of this team is to operate on the assumption that the organisation already has breached, but the SIEM team has not yet determined that the breach has occurred.

The role of the hunt team is to look for 'footprints in the sand' for possible intrusions.

Insider threat team — Research also has identified factors that are associated with employees involved in breaches, e.g., employees passed up for promotion, declining performance evaluations, financial challenges, etc. While some organisations have deployed insider threat teams, investigating for potential insider involvement has serious privacy and legal considerations.

Advanced topics

Prevention is the goal of any cybersecurity strategy, along with timely detection and an effective response to the inevitable intrusion. Equally important is gaining a deep understanding of the attack and an ongoing effort to continually improve your systems.

Forensic analysis

Forensic analysis, while using some of the same means and methods as the incident response team, has different objectives. In addition to determining what happened, and how a particular breach might be prevented, forensic analysis is the process of examining what is left behind that might be of value to investigators.

The three primary elements of forensic analysis include system-level analysis, storage analysis and network analysis.

System-level analysis — If we know a system has been breached, the first level of analysis would involve looking at the individual system that was compromised for 'footprints in the sand' to determine what changes were made.

Storage analysis — The size of today's databases and the advent of cloud environments complicate storage analysis greatly.

A particular complication of cloud environments with respect to forensic analysis involves the external ownership of the servers containing the data. While a subpoena can be issued to the owner of a hard drive containing data that you want to analyse, often the data that you may be interested in may have been deleted and overwritten.

Network analysis — Collecting and analysing network data 'traffic' provide different perspectives. While network monitoring does not provide information about the content of what is coming and going, it does provide information about who is coming and going.

Malware analysis

If malware is located on the system, especially if it is a piece of unauthorised software, it is important to deeply understand what the malware does.

Reverse engineering — The first step is to reverse engineer the piece of malware and determine how it works and what it does.

Penetration testing

The purpose of doing penetration testing is to find the weak points in your software before adversaries find them. If weaknesses are found, it may be possible to fix them. Otherwise, it may be possible to put in place a detection mechanism to block an intrusion.

The first step for penetration testing is to identify all of the network components. This would include all of the 'smart' devices including IOT components, and home computer system computers, printers, televisions and other devices that might serve as points of access for an intrusion.

Software security

Design review — This involves looking for design or architectural weaknesses. Particular areas of sensitivity are customer records, intellectual property and payment information.

Code review — This includes looking at key areas of sensitivity such as verification and authentication processes and common areas of programming weakness.

Security testing — While penetration testing involves testing the resilience against some set of known software vulnerabilities, security testing is diving deeply into software to verify that security requirements are being properly performed.

Recent trends in cybersecurity

Cyber actions and actors

According to the root-cause breakdown in the Ponemon Institute/IBM Cost of a Data Breach Report 2020, system glitches cause 25% of data breaches, including both IT and business process failures. Human errors, including negligent employees or contractors who unintentionally cause a data breach, accounted for another 23%. The balance of 52% were malicious attacks either hackers or criminal insiders caused.

In terms of motivation, 53% of these malicious attacks are financially motivated, which results in malicious attacks being the most expensive, with a cost nearly $1 million more than system glitches or human error. Nation-state actors were involved in 13% of malicious breaches. Only 13% were attributed to ''hacktivists'', with 21% unknown as to origin.

Stolen or compromised credentials were the most expensive cause of malicious data breaches.

For organisations in the 2020 study, the fully deployed security automation, the average total cost of data breach was $2.4 million to $3.58 million less than the average cost for organisations without security automation deployed.

Data breach cost components

The Ponemon report also analysed the key factors that comprise the cost of a data breach. In rank order, the cost amplifying factors included:

- Complex security systems enabling technologies create
- Cloud migration
- Security skills shortage
- Compliance failures
- Third-party breach
- Internet of things (IoT)/Operational technology (OT) impacted

Cost mitigating factors included an extensive list of technology factors that served to reduce the cost, including:

- Formation of an incident response team
- Performing incident response testing
- Threat intel sharing
- Vulnerability testing
- Security analytics
- Managed security services
- ID theft protection
- Data loss prevention.

Also included in the list of cost mitigating strategies included employee training, board involvement, business continuity and cyber insurance.

Minimising financial and brand impacts

IBM Security provided a number of steps in the Ponemon report that can help minimise the financial and brand impacts of data breaches, summarised as follows:

- Invest in security orchestration, automation and response (SOAR) to help improve detection and response times.
- Adopt a zero-trust security model to help prevent unauthorised access to sensitive data.
- Stress-test your incident response plan to increase cyber resilience.
- Use tools that help protect and monitor endpoints and remote employees.
- Invest in governance, risk management and compliance programs.
- Minimise the complexity of IT and security environments.
- Protect sensitive data in cloud environments using policy and technology.
- Use managed security services to help close the security skills gap

The mantra ‘train like you fight and fight like you train’ means developing and testing incident response playbooks to help optimise your business’ ability to respond quickly and effectively to attacks.

Cybersecurity and small business

Small business incidents and impacts

Unfortunately, another notable trend is that data breaches and cyberattacks involving small- and medium-sized businesses are on the rise, and addressing this risk is no longer an option.

In 2019, the Ponemon Institute also published a research report the 2019 Global State of Cybersecurity in Small and Medium-Sized Businesses, sponsored by Keeper Security Inc. Key takeaways from this report included the significant increase in SMBs experiencing data breaches and 66% saying their organisation had experienced a cyberattack in the past 12 months.

The financial impact of these events is severe. In 2019, the cost of dealing with damage or theft of IT assets and infrastructure for these SMBs was $1.24 million; the average cost of business disruption added another $1.9 million.

In terms of the type of attacks, 53% of respondents experienced phishing/social engineering attacks, followed by web-based attacks at 50%. General malware (39%) and compromised or stolen devices (37%) were also quite common.

Laptops (56%) and mobile devices (56%) were the most vulnerable endpoints or entry points, followed by IoT devices (45%), cloud systems (45%) and smartphones (41%). This is reflected in the finding that 49% of respondents feel that the use of mobile devices to access business-critical applications and IT infrastructure diminishes their organisation's security posture.

Almost half (47%) of SMBs have suffered an attack involving the compromise of employee's passwords. The average cost of each attack was $384,598. Unfortunately, while password policies can be very effective in mitigating this risk, 56% of respondents indicated their companies do not have, or were unsure of such a policy.

Clearly, SMBs struggle to maintain the effectiveness of their security posture, continuing to struggle with insufficient staffing and funding. When asked to identify the top three challenges that keep their security posture from being fully effective, responses yielded the following results:

77% — Insufficient personnel

59% — Insufficient budget

45% — No understanding of how to protect against cyber attacks

36% — Insufficient enabling security technologies

35% — Lack of in-house expertise

Other challenges included a lack of leadership, management not seeing cybersecurity attacks as a significant risk, or it not being a priority issue. Lack of collaboration with other departments was also cited, as was leadership in determining IT security priorities.

Small business resources

Appendix III provides a summary of the global Center for Internet Security Inc. (CIS®) framework of cybersecurity controls. The structure of this framework includes identification of controls by different Implementation Groups (IGs), with IG1 being enterprises that are 'small- to medium-sized with limited IT and cybersecurity expertise to dedicate towards protecting IT assets and personnel'. In addition to the CIS framework, there are other resources targeted to this audience.

In the U.S., the Cybersecurity and Infrastructure Security Agency (CISA) developed a Cyber Essentials Starter Kit: The Basics for Building a Culture of Cyber Readiness. CISA's Cyber Essentials is a guide for leaders of small businesses and small and local government agencies that is consistent with the NIST Cybersecurity Framework and can be used as a starting point for cyber readiness.

Building a culture of cyber readiness has six essential elements:

- **Yourself** — Drive cybersecurity strategy, investment and culture
- **Your staff** — Develop security awareness and vigilance
- **Your systems** — Protect critical assets and applications
- **Your surroundings** — Ensure only those who belong on your digital workplace have access
- **Your data** — Make backups and avoid loss of info critical operations
- **Your crisis response** — Limit damage and quicken restoration of normal operations

Reducing your organisations' cyber risks requires a holistic approach.

The Essentials Starter Kit also identifies 'Things to do first' including:

- **Backup data** — Employ a backup solution that automatically and continuously backs up critical data and system configurations.
- **Multi-factor authentication** — Require multi-factor authentication (MFA) for accessing your systems whenever possible.
- **Patch and update management** — Enable automatic updates whenever possible. Replace unsupported operating systems, applications and hardware. Test and deploy patches quickly.

The U.K. also has a government-backed Cyber Essentials certification program that has two levels. Cyber Essentials is a self-assessment option. Cyber Essentials Plus involves a hands-on technical verification.

The requirements for the U.K. Cyber Essentials certification are specified under five technical control themes:

- Firewalls
- Secure configuration
- User access control
- Malware protection
- Security update management

Cybersecurity governance, risk and reporting

Along with the ever-increasing frequency of breaches and compromised data, regulatory requirements and the demand for disclosure have also become part of the cybersecurity landscape.

Privacy and cybersecurity regulation

On the regulatory front, perhaps most notably, there have been significant 'press worthy' fines levied on global organisations in connection with the EU GDPR (General Data Protection Regulation). While there is not a similar national regulation in the U.S. protecting the privacy of data, there are a range of regulations that have resulted in fines levied on financial institutions, health-care providers and other enterprises for cybersecurity breaches involving compromised data.

In July 2019, the U.K. Information Commissioner clarified that the severity of fines under GDPR is based on the existence of adequate, reasonable, consistent and effective controls.

With respect to cybersecurity regulation, in the U.K. there is no overarching cybersecurity law. However, there are a number of specific legislative measures, including the Network and Information Security Regulations (the 'NIS Regulations) that require businesses to implement appropriate and proportionate measures to manage risks associated with the security of information systems.

In the U.S., an Executive Order on Improving the Nation's Cybersecurity was signed May 12, 2021. In addition to addressing cybersecurity in the federal government, it also makes an appeal to the private sector and includes provisions for the Secretary of Commerce and Federal Trade Commission to explore potential provisions for consumer labeling schemes.

It is the policy of my administration that the prevention, detection, assessments and remediation of cyber incidents is a top priority and essential to national and economic security.

Under these new requirements, defense contractors and subcontractors that make up the U.S. Defense Industrial Base will be required to demonstrate compliance with Cybersecurity Maturity Model Certification (CMMC) practices and policies by fiscal year 2026. In the U.K., the Cyber Essentials certification has been a requirement for contractors or subcontractors for any part of the UK central Government since 2014.

Risk management, reporting and oversight

In addition to this compliance risk, the business risks associated with cybersecurity from business interruption have escalated the level of concern on the part of governing boards, their audit and risk committees, investors, as well as customers and suppliers in the enterprise value chain.

As summarised in Appendix II, the AICPA developed a Cybersecurity Risk Management Reporting Framework as part of a collection of resources for both public accounting and management accounting Cybersecurity Resource Center. One resource available on the Resource Center, is the SOC for Cybersecurity Backgrounder, which provides an overview of Security and Organization Controls (SOC) assurance engagements.

With respect to governance and board oversight, the Center for Audit Quality, an autonomous public policy organisation affiliated with the AICPA, has developed the *Cybersecurity Risk Management Oversight*, which is a resource for board members.

This resource provides a range of guidance that board members can use to discharge their responsibilities with respect to cybersecurity risk. In addition to providing questions to ask that can develop understanding about the role of management and the financial statement auditor, it covers how CPAs can assist boards of directors in their oversight of cybersecurity risk management.

It also provides information and questions for board members to ask with respect to:

- Their companies' specific risk profile, particular vulnerabilities, and management's approach to managing these risks.
- The prioritisation of risk management practices, including supply-chain or third-party risks, in addition to internal personnel policies, training, access controls, etc.
- Incident response protocols, including thorough analysis of events, reporting to relevant parties, and potential disclosure requirements.

> The SEC has stated that disclosures regarding a company's cybersecurity risk management program and how the board of directors engages with management on cybersecurity issues allow investors to assess how a board of directors is discharging its risk oversight responsibility.
>
> CAQ Cybersecurity Risk Management Tool.

Appendix I:
Cybersecurity insurance

Since coverage for damages related to cybersecurity incidents is not included in most commercial insurance policies, a separate policy, or rider, is required. This is especially true for organisations that have significant customer or client personally identifiable information (PII) and process online credit card payments, or are otherwise highly dependent upon the web to conduct their business.

In addition to insurance that covers the losses relating to damage to, or loss of information from, IT systems and networks, policies generally include significant assistance with and management of the incident itself, which can be essential when faced with reputational damage or regulatory enforcement.

As outlined in a *Lloyds of London Quick Guide to Cyber Risk*, cyber risks fall into first-party and third-party risks:

First-party insurance covers your business's assets. This may include:

- Loss or damage to digital assets such as data or software programmes
- Business interruption from network downtime
- Cyber exhortation where third parties threaten to damage or release data if money is not paid to them
- Customer notification expenses when there is a legal or regulatory requirement to notify them of a security or privacy breach
- Reputational damage arising from a breach of data that results in loss of intellectual property or customers
- Theft of money or digital assets through theft of equipment or electronic theft

Third-party insurance covers the assets of others, typically your customers. This may include:

- Security and privacy breaches, and the investigation, defence costs and civil damages associated with them
- Multi-media liability, to cover investigation, defence costs and civil damages arising from defamation, breach of privacy or negligence in publication in electronic or print media
- Loss of third-party data, including payment of compensation to customers for denial of access, and failure of software or systems

While cybersecurity insurance is an important aspect of an organisation's strategy, it should not replace best practices, policies and controls. In fact, having an effective cybersecurity programme in place can reduce premiums.

- Evaluating first and third party risks associated with the IT systems and networks in your business
- Assessing the potential events that could cause first or third party risks to materialise
- Analysing the controls that are currently in place and whether they need further improvement

Appendix II:
Cybersecurity risk management reporting framework

In response to the growing demand for information about the effectiveness of organisational efforts to manage cybersecurity threats, the AICPA has developed a cybersecurity risk management reporting framework. While there are many methods and frameworks for developing cybersecurity risk management programmes, this framework is a common language for organisations to communicate about, and report on, these efforts.

This framework is designed to help organisations demonstrate to key stakeholders the extent and effectiveness of their cyber risk readiness efforts. Companies can use it internally to explain, in a consistent manner, all of the policies, procedures and controls it has implemented to address the cybersecurity risks that are critical to their business. It can also be used for reporting to senior management, boards of directors and other stakeholders to facilitate their understanding of the entity's cyber risk management programme.

Being a key component of a new System and Organisation Controls (SOC) for Cybersecurity attest engagement, it can also assist organisations in demonstrating to analysts, investors and other external parties that they have effective processes and controls in place to detect, respond to, mitigate and recover from breaches and other security events.

Benchmarks, which management can use in describing their cybersecurity risk management programme, are captured in the framework's *Description Criteria for Managements Description of the Entity's Cybersecurity Risk Management Program*.

An *Illustrative cybersecurity risk management report* has also been developed to provide an example for how an entity might prepare and present a description of its cybersecurity risk management programme.

The description criteria are categorised into the following sections:

Nature of business and operations — Disclosures about the nature of the entity's business and operations.

Nature of information at risk — Disclosures about the principal types of sensitive information the entity creates, collects, transmits, uses and stores that are susceptible to cybersecurity risk.

Cybersecurity risk management programme objectives (cybersecurity objectives) — Disclosures about the entity's principal cybersecurity objectives related to availability, confidentiality, integrity of data, and integrity of processing and the process for establishing, maintaining, and approving them.

Factors that have a significant effect on inherent cybersecurity risks — Disclosures about factors that have a significant effect on the entity's inherent cybersecurity risks, including the

- Characteristics of technologies, connection types, use of service providers and delivery channels the entity uses;
- Organisational and user characteristics;
- Environmental, technological, organisational and other changes during the period covered by the description, the entity and in its environment.

Cybersecurity risk governance structure — Disclosures about the entity's cybersecurity risk governance structure, including the processes for establishing, maintaining and communicating integrity and ethical values, providing board oversight, establishing accountability, and hiring and developing qualified personnel.

Cybersecurity risk assessment process — Disclosures related the entity's process for:

- Identifying cybersecurity risks and environmental, technological, organisational and other changes that could have a significant effect on the entity's cybersecurity risk management programme;
- Assessing the related risks to the achievement of the entity's cybersecurity objectives; and
- Identifying, assessing, and managing the risks associated with vendors and business partners.

Cybersecurity communications and the quality of cybersecurity information — Disclosures about the entity's process for communicating cybersecurity objectives, expectations, responsibilities, and related matters to both internal and external users, including the thresholds for communicating identified security events that are monitored, investigated and determined to be security incidents, requiring a response, remediation or both.

Monitoring of the Cybersecurity Risk Management Programme — Disclosures related to the process the entity uses to assess the effectiveness of controls included in its cybersecurity risk management programme, including information about the corrective actions taken when security events, threats, vulnerabilities, and control deficiencies are identified.

Cybersecurity Control Processes — Disclosures about

- The entity's process for developing a response to assessed risks, including the design and implementation of control processes;
- The entity's IT infrastructure and its network architectural characteristics; and
- The key security policies and processes implemented and operated to address the entity's cybersecurity risks.

Appendix III:
Center for Internet Security — CIS Controls v8

The Center for Internet Security Inc. (CIS®) is a nonprofit organisation responsible for developing globally recognised best practices for securing IT systems and data. The CIS has become an international community of experts having a mission 'to create confidence in the connected world'.

This appendix is a summary of CIS Controls which have been updated and enhanced to keep pace with cloud-based and hybrid environments, virtualisation and mobility, along with changing attacker tactics, and the recent shift to Work-from-Home.

CIS Controls are a prioritised set of safeguards to mitigate the most prevalent cyber-attacks against systems and networks.

The CIS Controls have been mapped to a very wide variety of formal Risk Management Frameworks (like NIST®, Federal Information Security Modernization Act (FISMA), International Organization for Standardization (ISO), etc.).

The have also been structured to provide guidance according to Implementation Groups or IGs:

- An IG1 enterprise is small- to medium-sized with limited IT and cybersecurity expertise to dedicate towards protecting IT assets and personnel.
- An IG2 enterprise employs individuals responsible for managing and protecting IT infrastructure.
- An IG3 enterprise employs security experts that specialise in the different facets of cybersecurity (e.g., risk management, penetration testing, application security).

The controls applicable to IG1 are considered to be 'basic cyber hygiene' and are also applicable to IG2 and IG3. Similarly, additional controls applicable to IG2 are also applicable to the IG3 group.

The presentation of controls in the guidance contain the following elements:

- Overview — A brief description of the intent of the control and its utility as a defensive action
- Why is this control critical? — A description of the importance of this control in blocking, mitigating or identifying attacks, and an explanation of how attackers actively exploit the absence of this control
- Procedures and tools — A more technical description of the processes and technologies that enable implementation and automation of this control
- Safeguard descriptions — A table of the specific actions that enterprises should take to implement the control.

Overview descriptions of the 18 controls encompassed in this framework, including the proportion of safeguards for each control that apply to Implementation Group 1 are as follows:

Control 01. Inventory and Control of Enterprise Assets — IG1= 2/5

Actively manage (inventory, track and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorised and unmanaged assets to remove or remediate.

Enterprises cannot defend what they do not know they have.

Control 02. Inventory and Control of Software Assets — IG1= 3/7

Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorised software is installed and can execute, and that unauthorised and unmanaged software is found and prevented from installation or execution.

Control 03. Data Protection — IG1= 6/14

Develop processes and technical controls to identify, classify, securely handle, retain and dispose of data.

Control 04. Secure Configuration of Enterprise Assets and Software — IG1= 7/12

Establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications).

Default configurations for enterprise assets and software are normally geared towards ease-of-deployment and ease-of-use rather than security.

Control 05. Account Management — IG1= 4/6

Use processes and tools to assign and manage authorisation to credentials for user accounts, including administrator accounts, as well as service accounts, to enterprise assets and software.

Control 06. Access Control Management — IG1= 5/8

Use processes and tools to create, assign, manage, and revoke access credentials and privileges for users, administrator and service accounts for enterprise assets and software.

Control 07. Continuous Vulnerability Management — IG1= 4/7

Develop a plan to continuously assess and track vulnerabilities on all enterprise assets within the enterprise's infrastructure, to remediate, and minimise, the window of opportunity for attackers. Monitor public and private industry sources for new threat and vulnerability information.

Control 08. Audit Log Management — IG1= 3/12

Collect, alert, review and retain audit logs of events that could help detect, understand or recover from an attack.

Control 09. Email and Web Browser Protections — IG1= 2/7

Improve protections and detections of threats from email and web vectors, as these are opportunities for attackers to manipulate human behavior through direct engagement.

Control 10. Malware Defenses — IG1= 3/7

Prevent or control the installation, spread, and execution of malicious applications, code, or scripts on enterprise assets.

Control 11. Data Recovery — IG1= 4/5

Establish and maintain data recovery practices sufficient to restore in-scope enterprise assets to a pre-incident and trusted state.

Control 12. Network Infrastructure Management — IG1= 1/8

Establish, implement and actively manage (track, report and correct) network devices, to prevent attackers from exploiting vulnerable network services and access points.

Control 13. Network Monitoring and Defense — IG1= 0/11

Operate processes and tooling to establish and maintain comprehensive network monitoring and defense against security threats across the enterprise's network infrastructure and user base.

An effective security awareness training program should not just be a canned, once-a-year training video coupled with regular phishing testing.

Control 14. Security Awareness and Skills Training — IG1= 8/9

Establish and maintain a security awareness program to influence behavior among the workforce to be security conscious and properly skilled to reduce cybersecurity risks to the enterprise.

Control 15. Service Provider Management — IG1= 1/7

Develop a process to evaluate service providers who hold sensitive data, or are responsible for an enterprise's critical IT platforms or processes, to ensure these providers are protecting those platforms and data appropriately.

Control 16. Application Software Security — IG1= 0/14

Manage the security life cycle of in-house developed, hosted, or acquired software to prevent, detect, and remediate security weaknesses before they can impact the enterprise.

Control 17. Incident Response Management — IG1= 3/9

Establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training and communications) to prepare, detect and quickly respond to an attack.

Even if enterprise does not have resources to conduct incident response within an enterprise, it is still critical to have a plan.

Control 18. Penetration Testing — IG1= 0/5

Test the effectiveness and resiliency of enterprise assets through identifying and exploiting weaknesses in controls (people, processes and technology), and simulating the objectives and actions of an attacker.

Appendix IV:

CISA MS-ISAC *Ransomware Guide* – Part 2: Ransomware Response Checklist

CISA, the Computer Information Sharing Agency is a federal agency with Department of Homeland Security oversight. The Multi-State Information Sharing & Analysis Center (MS-ISAC) is a voluntary, collaborative effort designated by the DHS to provide cyber threat services for state, local, tribal and territorial governments (SLTTs). The CIS (Appendix III) is home to MS-ISAC.

The CISA MS-ISAC *Ransomware Guide* Part 2 provides an extensive Ransomware Response Checklist that is relevant for any organisation. The following is an excerpt of the first five steps in that guide that address detection and analysis of impacted systems in the event of a ransomware attack. The Checklist encourages working through the first three steps in order.

Detection and analysis

1. Determine which systems were affected and immediately isolate them.
   - If several systems or subnets appear to be affected, take the network offline at the switch level. It may not be feasible to disconnect individual systems during an incident.
   - If taking the network temporarily offline is not immediately possible, locate the network (e.g., Ethernet) cable and unplug affected devices from the network or remove them from Wi-Fi to contain the infection.
   - After an initial compromise, malicious actors may monitor your organisation's activity or communications to understand if their actions have been detected. Be sure to isolate systems in a coordinated manner and use out-of-band communication methods such as phone calls or other means to avoid tipping off actors that they have been discovered and that mitigation actions are being undertaken. Not doing so could cause actors to move laterally to preserve their access — already a common tactic — or deploy ransomware widely before networks being taken offline.

Note: Step 2 will prevent you from maintaining ransomware infection artifacts and potential evidence stored in volatile memory. It should be carried out only if it is not possible to temporarily shut down the network or disconnect affected hosts from the network using other means.

2. Only in the event you are unable to disconnect devices from the network, power them down to avoid further spread of the ransomware infection.

3. Triage affected systems for restoration and recovery.
   - Identify and prioritise critical systems for restoration and confirm the nature of data housed on impacted systems. Prioritise restoration and recovery based on a predefined critical asset list that includes information systems critical for health and safety, revenue generation, or other critical services, as well as systems they depend on.

- Keep track of systems and devices that are not perceived to be affected so they can be deprioritised for restoration and recovery. This enables your organisation to get back to business in a more efficient manner.

Remember: Paying ransom will not ensure your data is decrypted or that your systems or data will no longer be compromised. CISA, MS-ISAC and federal law enforcement do not recommend paying ransom.

4. Confer with your team to develop and document an initial understanding of what has occurred based on initial analysis.

5. Using the contact information provided in the Checklist, engage your internal and external teams and stakeholders with an understanding of what they can provide to help you mitigate, respond to, and recover from the incident.

   - Share the information you have at your disposal to receive the most timely and relevant assistance. Keep management and senior leaders informed via regular updates as the situation develops. Relevant stakeholders may include your IT department, managed security service providers, cyber insurance company, and departmental or elected leaders.

The remaining sections in the 19-step checklist address issues related to containment and eradication and recovery and post-incident response activity. The checklist also provides information about assistance that can be provided by CISA and MS-ISAC.

The Checklist also provides contacts for Federal Asset Response services, and for Federal Threat Response services. Asset response services include guidance for evaluating and remediating ransomware incidents, recommendations for containment and mitigation strategies and phishing email, storage, media, log and malware analysis. Federal threat response services include law enforcement and national security investigative activity.

Additional reading and resources

Cybersecurity Resource Center

Center for Audit Quality (CAQ)

Centre for Cybersecurity

Journal of Accountancy articles:

Audit Committee Cybersecurity Disclosures Rising in Proxy Statements

Cybersecurity Requirements Provide New Opportunity for CPAs

Data Thieves Strike at Any Weak Point

3 Ways to Defeat Ransomware: Plan, Prevent, Not Pay

FM magazine articles:

Cyberattacks Stemming from Software on the Rise

5 Signs There Could Be IP Theft in Your Supply Chain

Stay Vigilant Against These 5 Data Security Risks

Notes

aicpa.org | aicpa-cima.com | cgma.org | cimaglobal.com

August 2021

ISBN 978-1-85971-845-2

Founded by AICPA and CIMA, the Association of International Certified Professional Accountants powers leaders in accounting and finance around the globe.