CHARTERED PROFESSIONAL ACCOUNTANTS CANADA

Cybersecurity From the Inside Out

A PRACTICAL PRIMER ON MODERN DATA PRIVACY AND GOVERNANCE FOR SMALL AND MEDIUM-SIZED ENTERPRISES (SMES)

By Claudiu Popa, CISSP, CIPP, PMP, CISA, CRISC

Overview
Process
Application
Key Learnings
Resources

What is the issue?

The past few years have accelerated economic changes globally, with the traditional role of the accounting professional evolving at pace with the needs of modern organizations. Canadian businesses and accounting practitioners are rapidly adapting to trends shaped by data and privacy legislation, cybersecurity standards and technology transformations. CPAs can now capitalize on the unprecedented opportunity to help companies and NPOs of all sizes leverage their professional capabilities; in so doing, the CPA becomes the trusted advisor and leader in a modern world impacted by the challenges of evaluating and mitigating risk.

Why is the issue important?

Daily reporting of data breaches and digital hacking events has become a regular occurrence. Whether working from home or in traditional office environments, corporate users are now conditioned to expect fraudulent requests but are not always able to tell which are legitimate and which are not. These events have contributed to rising individual and corporate awareness about the importance of data protection. Reporting and notification regulations have been crucial in exposing pervasive information collection and negligence across diverse industry sectors.

What can be done?

Businesses and NPOs of all sizes have both the challenge and the opportunity to ramp up their cybersecurity game and focus on the layers of prevention, detection and reaction as the key phases of modern risk management strategy. Whether advising on risk minimization techniques or risk transfer mechanisms, CPAs versed in the protective language of information risk management can seize this opportunity to elevate their strategic involvement with standards compliance and provide operational decision support.

Overview

A general lack of investment in cybersecurity has led to a current state of affairs where malicious software is used to steal data, users are intimidated into paying ransoms and victims in all walks of life are defrauded by social engineering scams. According to Beazley Breach Response, 71% of ransomware targets small and medium-sized enterprises (SMEs).

The "new normal" brought to the forefront by COVID-19 has organizations anticipating cyberattacks, with up to 55 per cent of them confessing that they would pay ransoms if it came to that (DarkReading, 2019). In effect, this is an unprecedented development in the world of business, with an estimated 73 per cent of SMEs actually paying extortionists to regain access to their data and systems held hostage by ransomware (Infrascale, 2020).

The role of the CPA as merely filling an accounting function has evolved into that of a collaborative trusted advisor with line of sight into financial aspects of enterprises and input into supplier due diligence and asset protection. Information risk is now top of mind for accounting professionals. This role is now a linchpin with influence across the enterprise and is closely connected with advisory roles that also include IT specialists, human resources and project management.

This guideline is for CPAs and practitioners in SME's that need a cybersecurity strategist with clear line of sight into finance and operations. This guideline will illustrate how SMEs budget for cybersecurity, transfer costly data risk using insurance policies, and prioritize key technological controls for maximum operational effectiveness.

This guideline will introduce concepts that are increasingly relevant to your profession and those of your stakeholders. With data breaches costing companies an average of $4 million per incident (IBM, 2020), organizations must shift their approach to decisions involving cybersecurity and adopt a top-down, management-driven approach that relies on trusted advisory support.

In this context, risk treatment is not complicated, but it is very different from previous approaches and therefore requires the leadership and expertise of a trusted advisor versed in the typical motivations of cybercriminals.

How emerging trends impact your business

Authoritative bodies struggle to understand evolving cybercrime as it arises, and organizations are discovering as much about their own resilience as they are about risk management. With the majority of most organizations' value trapped in intangible assets such as data analytics and personal information, and with many companies shifting to de-centralized, remote working environments, we see an unprecedented confluence of risk factors. The stakes are high for companies large and small, whose existential risk is tied to the supply chain's security, not only their own. The CPA's role has accordingly shifted to that of an advisor, a financial gatekeeper and a technologist as the profession continues to adapt to a landscape that brings a palpable appetite for expert guidance.

It is widely believed that cybersecurity breaches have an economic impact and are a threat to national security. In addition to the aforementioned figures, 90 per cent of Canadian businesses suffered at least one successful breach in 2018 (Cision Canada, 2018). Increasing volumes of information along with low risk maturity place SMEs at risk of financial loss, liability suits and brand damage. What's more, half of small businesses that suffer serious data breaches are out of business six months later (Cybercrime Magazine, 2019).

Accounting professionals must be aware of six fundamental risk factors that impact modern business operations, three external and three internal:

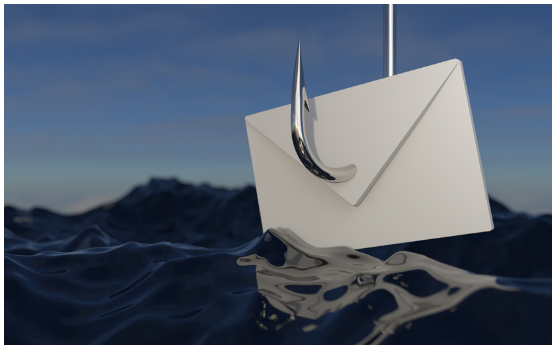
Externally:

- changes in legislation
- technology innovation
- emerging cybersecurity risk

Internally, the need for:

- resilience (to business and cyber risk)
- adaptability (particularly to external factors)
- innovation (the need to remain competitive through continuous transformation and progress)

Business email compromise (BEC) is a form of fraudulent phishing campaign that has seen a 100 per cent increase year over year since 2017. It is now estimated that almost half of all BEC fraud contains malware (Standard Chartered, 2020), which results in wire fraud. Not to be outdone, physical data breaches and theft of devices still accounted for over 70 per cent of data losses (Shred-it and Ponemon Institute, 2020).



In light of significant economic, societal and cultural changes, professional advisors and accounting practitioners must plan to transform the way organizations are supported, from setting appropriate policies and procedures to implementing strategic governance that drives what data is collected and processed by organizations. As privacy and risk governance become mature practice areas within organizations, there is a demand to face the emerging challenge of balancing operational risks with the financial investments required to mitigate or transfer those risks.

Data breaches are not only caused by malicious attackers. According to the Office of the Privacy Commissioner of Canada (2019), almost a quarter of data breaches are accidental, caused by human error rather than malice. Although they are dry statistics, these numbers vividly bring to life the clear and present danger of modern cybersecurity threats. Only a few short years ago, the general public was considered ill-equipped to handle news of data breaches or to conceptualize the impact of identity fraud resulting from concerted efforts to breach security and steal personal information.

Today, increasingly stringent existing legislation forces companies to accept responsibility for information it does not own, and the media relentlessly reports security failures. Authoritative organizations publish readily applicable guidance that drives at the heart of the issues and catalyzes continuous improvement. This guideline places security practices into their proper context and offers a common language for professionals and organizations to adopt in tackling modern security, privacy and compliance challenges.

At a time when few organizations get breach prevention and response right, CPAs can now lead their organizations through a process of risk maturity based on their multifaceted understanding of the financial drivers and objectives of cybercrime. Additionally, the structured approach to designing controls and the ability to concisely present the information that matters most depend on greater trends being observed both nationally and globally. Such impactful information includes:

- According to experts, cyberattacks could prompt the next recession. (Business.com, 2019)
- By 2020, 60 per cent of digital businesses will suffer major service interruptions with potentially global consequences. (CIO, 2018)

The operational stability of an organization depends largely on its financial management, so the expertise of accounting professionals is paramount for the resilience, adaptability and innovation required to ensure not only continuity but also steady, controlled growth.

The status quo for risk management is a theoretical exercise governed by abstract notions and esoteric equations. However, as we will demonstrate, effective risk prevention and response depends on empowering employees with actionable information, examples, checklists, self-assessments and a view into the results of these internal initiatives to ensure everyone is aligned with the organization’s objectives and risk posture. We will introduce new terms such as “operational security” (OPSEC) to illustrate the importance of these concepts to everyday operations. Empowering everyone within the enterprise creates a “human firewall” or a “web of trust” that serves to incrementally raise awareness and increase risk resilience.

Introduction to the topic: How cybersecurity works in all companies

In practice, cybersecurity is supported by three pillars: IT security, administrative security and physical security. An understanding of these fundamental building blocks is an integral part of understanding how to build a resilient and sustainable operation.

Seen through this lens, data breaches and reported cybersecurity incidents are preventable situations that are manageable by organizations of all sizes. In the following three simple examples, we look at real scenarios to understand what drives cyber incidents and why every data breach is preventable.

Controls and safeguards

Security controls fall into three categories, or pillars.

10 EXAMPLES OF CYBERSECURITY CONTROLS FOR EACH FOUNDATIONAL PILLAR

IT security	Administrative security	Physical security
• Encrypted backups	• Employee training	• Monitor privacy screens
• Network firewalls	• Information security policies	• Encrypted USB keys
• Antivirus filtering	• Privacy policies	• Kensington lock and cables
• Intrusion detection systems	• Data and password policies	• Tamper-proof cases
• Password logins	• Patch management programs	• CCTV camera monitoring
• Multi-factor authentication	• Security team meetings	• Access cards
• Data integrity verification	• Data classification	• Physical security zones
• Encrypted email	• Information asset inventories	• Badges and visitor logs
• Anti-ransomware	• Business continuity planning	• Motion sensors
• Security testing and scanning	• Incident and breach processes	• Biometric access

This diverse set of security controls represents key drivers of internal change, from security-related policies to insurance coverage to the focus on GRC (governance, risk and compliance).

Understanding the three types of cybersecurity controls

In tackling cybersecurity, every organization must balance risk-management objectives with the resources available to protect existing assets. Those resources should naturally be prioritized to focus on preventing security incidents. In large numbers of cases, however, statistics show that breaches had been victimizing organizations for over 200 days before they were detected. This is why, in addition to prevention, a sound security strategy also depends on monitoring and auditing. Once detected, an incident requires prompt and adequate response, so corrective controls must be implemented to ensure that steps are taken to deal with breaches as soon as possible. Taken together, preventative, detective and corrective safeguards constitute the substance of every organization's risk-management strategy.

Prevention: a focus on the reducing the risk that a vulnerability can be exploited.

Detection: the discovery and progress monitoring of a security incident, and the associated activities that go along with it.

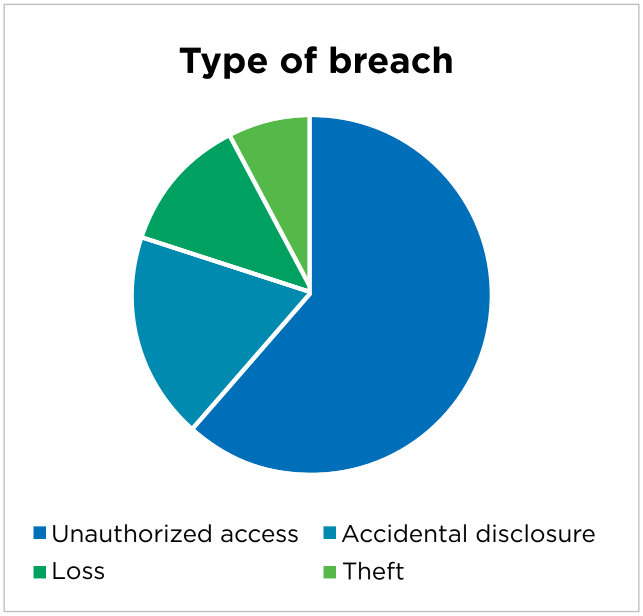
Correction: the series of actions that decrease the severity and impact of an event after an incident has started or occurred.

Establishing the need for more than just prevention

On November 1, 2018, the *Data Security Act* augmented the *Personal Information Privacy and Electronic Documents Act* (PIPEDA) and required companies to monitor and detect breaches, report them if they are material, and notify victims if there is a risk of significant harm to data subjects.

A year after this updated law took effect, the number of reported data breaches increased drastically, indicating that in the absence of detective controls, breaches had simply been overlooked.

- By November 2019, 680 breach reports had been filed, representing a six-fold increase in the volume of the previous year. The privacy commissioner's office called this "revealing" and a "staggering increase."
- Data breaches affected 28 million Canadians in 2019. This not only included the breach at Equifax, but also those experienced by Desjardins and reported by Capital One.
- Fifty-eight per cent of breaches involved unauthorized access, which illustrates the ill intent and share of data breaches that are due to a combination of inadequate safeguards and financial motivation.



The value of CPA practitioners

Accounting practitioners now have an opportunity to contribute to strategic and operational decisions as part of a variety of scenarios including:

- practitioner as risk advisor, providing resilience leadership with a focus on internal controls and key processes
- practitioner as change agent and/or change manager, offering support for education, incident response and adaptation to the six fundamental risk factors

- practitioner as innovator, providing strategic oversight and direction to drive progressive (and profitable) corporate transformation

In practical terms, CPAs can apply a sound mindset to the challenge of deploying cybersecurity solutions in a manner commensurate with available resources. For example**,** let's say that an organization carried out a risk assessment or security review. The outcomes of this activity were summarized simply as recommendations for:

- developing an incident response plan to manage cybersecurity incidents
- implementing a security information and event management system
- enabling automatic updates for software and hardware (where available)
- configuring and enabling up-to-date firewalls, anti-virus and anti-malware software
- implementing two-factor authentication
- developing policies regarding passwords
- providing employee awareness training to minimize human error
- backing up and encrypting data
- establishing appropriate perimeter defenses, such as firewalls
- implementing the principle of "least privilege" by providing users with only the minimal functionality required to perform their duties and responsibilities
- using a simple checklist-based approach to achieving completeness and scalable risk management that applies as much to small business as to nonprofits and larger organizations

This leaves management in a position where a decision must be made to allocate scarce resources to general activities. How can these activities be prioritized? Where's the urgency? Who can be tasked with managing these activities?

Enter the CPA in an advisory role where their perspective on risk and expertise in security controls provide a clear picture of what needs to be done, and when. The approach they would recommend can be summarized in the following table:

Priority	Activity	Category	Type
1	Enable perimeter defence	Physical/IT	Prevent
2	Securely configure devices and systems	IT	All
3	Enable automatic updates	IT	Prevent
4	Develop policies	Admin	All
5	Enforce strong access controls	IT	Prevent
6	Limit user privileges	IT	Prevent

Overview
Process
Application
Key Learnings
Resources

Priority	Activity	Category	Type
7	Provide employee training	Admin	All
8	Adopt a security information system	IT/Admin	Monitor
9	Enact incident response procedures	Admin	Respond
10	Securely back up data and regularly test backups	Physical	Respond

The key here is for CPAs to show that the vast majority of safeguards must not only address security incidents – they must also focus on preventing them in the first place. With at least three of the above controls adopted, greater value can be demonstrated from one activity as each of them serves to prevent, detect and correct (or respond) to cyber incidents.

The ability of CPAs to advise, transfer knowledge and demonstrate thought leadership is enhanced by such simple approaches to planning and delivering risk management.

Facing the challenge

Meeting business objectives has never been so dependent on the qualifications of accounting professionals and CPA practitioners. Their skills and values lend themselves ideally to the task of understanding risk impact and calculating paths to success. Qualified practitioners in tangential disciplines (i.e., chief financial officers or accounting department employees) can be granted sufficient authority and access privileges to unlock business opportunities, strike profitable partnerships and mitigate risky arrangements while supporting the priorities of the organization.

Cybersecurity trends vary from year to year, but it is important for trusted advisors to stay on top of such changes, synthesize the information and transfer it to stakeholders. For instance, current events have shown that criminals rely on three key activities when committing the vast majority of breaches:

1. ransomware and malware infections
2. social engineering and email compromises
3. manual data theft by gaining access to systems

As a result, CPAs must not only be familiar with the appropriate risk mitigation strategies but also be able to clearly articulate the key approaches to deal with each type of issue:

1. ransomware and malware infections
    a. patch management
    b. secure data backups
    c. information security policies (including breach management)
    d. qualified IT security professionals on the team
    e. employee security awareness training

Overview
Process
Application
Key Learnings
Resources

2. social engineering and email compromises
    a. signing up for a cyber-insurance policy
    b. secure configurations and systems "hardening"
    c. role-based employee training
    d. secure data sharing
    e. safe password management practices
3. manual data theft by gaining access to systems
    a. standardized controls across the board
    b. physical security audits
    c. risk transfer
    d. data encryption
    e. business continuity planning and disaster recovery

For the modern accounting professional, it is imperative to be a good communicator and educator, capable of appropriately disseminating and translating risk-based information within the organization. CPAs must also be starters and catalysts. That means initiating activities designed to "get the ball rolling" and empowering other team members to follow shared business objectives. Information security and risk management are, after all, a fundamental part of business operations. The ability to support management decisions with standards-based resources aligned with current norms is critical for the effectiveness of any cybersecurity program. Of similar importance are responsiveness and reachability. The cycle of trust that the modern practitioner must facilitate is defined by the ability to respond promptly to queries from peers and management as well as unplanned incidents and events.

Above all, the practitioner must be a team player. This guideline provides the practical approach to transforming the organization from within while evolving the practitioner from subject matter expert to trusted advisory team member. The risk governance concepts presented herein address the core critical paths of data operations, data valuation and associated policies, with a focus on continuous privacy compliance.

Process

Internal risk-related processes can be classified into five categories we will call the “CPA’s five domains of influence.” This guideline provides checklist-based activities encompassing these five domains. Select from the steps below to learn more.

Step 1: Risk management

Step 2: Cybersecurity controls

Step 3: Governance

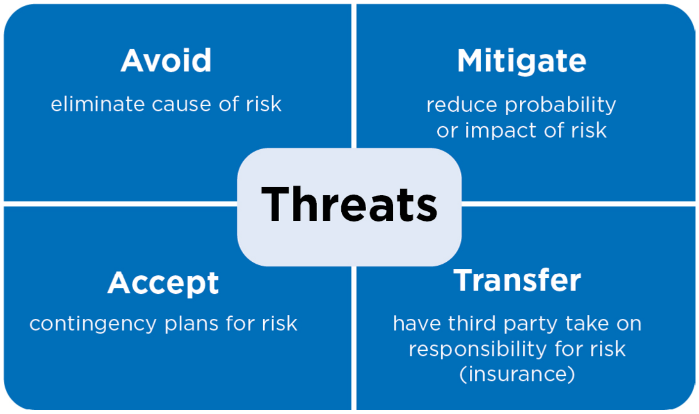
Step 4: Compliance

Step 5: Resilience and sustainability

Applying practical steps to achieve cybersecurity sustainability offers an opportunity to apply standardized steps for the CPA’s five domains of influence.

Applying the Topic to Your Organization

The standardized checklists for cybersecurity sustainability can be adapted to a number of existing risk-assessment methodologies, from Canada's nascent CyberSecure framework to the more established and widely-accessible PCI DSS and National Institute of Standards and Technology (NIST) standards with broad applicability across industry sectors. AICPA's regularly updated guidance within the Trust Services realm covers controls and policies across service organizations, so it is important to have a look at how the five domains of influence map to the needs of organizations of different sizes.


Avoid
eliminate cause of risk
Mitigate
reduce probability or impact of risk
Threats
Accept
contingency plans for risk
Transfer
have third party take on responsibility for risk (insurance)

The Project Management Body of Knowledge (PMBOK) four risk treatment options

Step 1

Risk management

Because financial operations deal directly with intangible assets, cybersecurity has a growing importance in the accounting profession, addressing risks related to previously unpredictable situations and protecting corporate operations. By leveraging risk management, governance and strategic planning, the key cybersecurity practices presented below will help practitioners "set the tone at the top" to reach the modern corporate objectives of resilience, adaptability and innovation to achieve enterprise sustainability.

To properly address risk for small and medium-sized enterprises (SMEs), CPAs must first follow this three-step risk clarification process:

1. Determine the value of information assets.
2. Determine the financial impact of their loss.
3. Establish the need for effective controls to minimize the risk.

As is the case in medical and life sciences scenarios, accounting practitioners must understand the following four risk treatment options (as summarized in the diagram you see here) and strive to be as precise as possible when advising corporate management or SME clients. Once identified, threats present a certain potential for damage. To prevent or reduce this risk, companies have the option to accept it, minimize or mitigate it, transfer it or avoid it outright.

Option 1: Risk avoidance (for unreasonably large exposure)

In their advisory capacity, CPAs should recommend avoiding or terminating activities that carry unreasonable or significant risk to the organization.

Assigning risk ratings to activities helps organizations determine where the activities exist on the risk spectrum. The risk rating calculation is as follows:

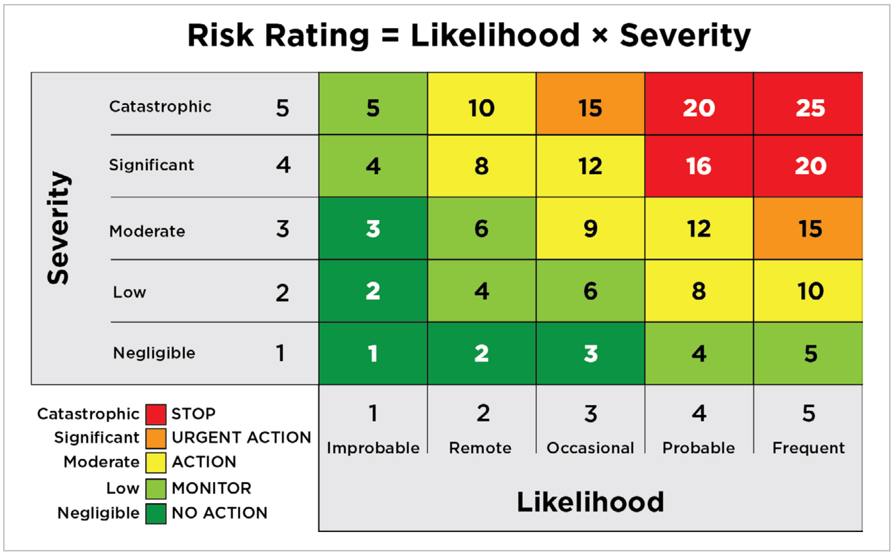
Risk probability (**R**) = Likelihood (**C**) (i.e., the probability of a disruptive event)
multiplied by
Severity (**I**) (i.e., the loss arising from the occurrence).

Thus, the **I**mpact of an adverse event multiplied by the **C**hance that it will occur determines the **R**isk.

This MAG recommends avoiding situations in which a damaging outcome is likely to occur with significant frequency.

Option 2: Risk acceptance (for minor outcomes)

Calculated risks can be assumed or accepted, as long as they are well understood and a clear decision has been made to proceed. As evidenced by many news headlines, most organizations fail to identify and document risks before accepting them. Failure to properly assess and address risk can place the organization and data subjects[1] in peril.



Risk Rating = Likelihood × Severity

Severity		1 Improbable	2 Remote	3 Occasional	4 Probable	5 Frequent
Catastrophic	5	5	10	15	20	25
Significant	4	4	8	12	16	20
Moderate	3	3	6	9	12	15
Low	2	2	4	6	8	10
Negligible	1	1	2	3	4	5
		Likelihood				

Catastrophic	🟥	STOP
Significant	🟧	URGENT ACTION
Moderate	🟨	ACTION
Low	🟩	MONITOR
Negligible	🟩	NO ACTION

Red means avoid, green means accept the risk. light green and yellow risk should be minimized as much as possible, with the residual risk transferred to an insurance underwriter using a cyber liability policy customized to the business and approved by management.

What could go wrong? Improper risk assessment, an incomplete data inventory or simply inadequate security can jeopardize the company's cybersecurity and compliance situation.

In such cases, a false sense of security undermines any protective safeguards the organization has in place and may cause lasting damage. Unfortunately, this is common amongst organizations of all sizes. As an example of preventable data breaches, incidents involving

[1] Data subject refers to any individual person who can be identified, directly or indirectly, via an identifier such as a name, ID number or location data, or via factors specific to the person's physical, physiological, genetic, mental, economic, cultural or social identity.

Overview
Process
Application
Key Learnings
Resources

ransomware grew by 56 per cent in each of the past four quarters (365 Technologies Inc., 2019), indicating that organizations failed to implement preventative safeguards, thus exposing themselves to incidents with potentially crippling consequences.

Option 3: Risk mitigation

This is the best-understood option, as it includes terminology that has entered the popular vernacular, such as firewalls, anti-virus software and passwords. These various methods of enforcing security policy are used to reduce or minimize both specific and general risk. The sufficiency of such measures is often questioned when organizations fail to adequately identify risk using a threat-risk assessment, leading to unexpected exposures or inadequate protective measures. In such situations, companies can suffer from a false sense of security, as they may believe that they have taken sufficient or even excessive steps to protect their assets when in fact significant holes may remain.

To reduce the likelihood of such outcomes, organizations classify distinct threat scenarios and build risk treatment processes for prevention, detection and correction of undesirable outcomes. Such approaches then become safeguards or triggers for actions to be carried out as a matter of operational practice.

Controls are abstract notions of protective safeguards applied in layers to protect them against tampering. We know that such controls as antivirus, firewalls and especially door locks are favourite targets of malicious attackers, so by wrapping valuables in such concentric blankets, SMEs can stop or even slow down attacks long enough for an incident response team to intervene. Such "defence in depth" is a key aspect of modern compliance frameworks and measures traditionally referred to as "best practices."

Option 4: Risk transfer

This is the practice of identifying residual risk after all other treatment options have been exhausted. By adequately painting a picture of residual risk and accountability to decision makers, CPAs and trusted advisors can empower management to make the correct decision to literally transfer the remaining risk to a third party, usually an insurance company, which will take on the risk as part of a cybersecurity liability policy.

By quantitatively helping organizations make risk calculations and conduct standardized risk assessments, practitioners can help build a risk register, which is a list of identified risks associated with the company and their respective exposures.

Overview
Process
Application
Key Learnings
Resources

For example, imagine an organization that has applied layered controls to protect its data from the outside in, that is, from the internal storage mechanisms to the verification of safeguards applied by its service providers and vendors. Such a business is in a good position to present the board with a clear picture of cybersecurity assurance where risk is mitigated in a controlled way. However, after it conducted a threat-risk assessment (TRA) and a subsequent penetration (or red team) testing exercise, the organization determined that the following areas constitute continued exposure and may present as vulnerabilities, should a motivated attacker persist in tackling the challenge:

1. Patches and updates cannot be applied to systems and devices immediately after they are released because best practices dictate that they must be tested to avoid negatively impacting the stability of the organization's operations. This takes time, and that delay represents a risk to the organization's security posture. During that time, an unpatched device or application could be attacked by malware designed to look for missing software or firmware updates and successfully exploit the vulnerability to gain access to the valuable information assets in question.
2. While employees may have been previously trained on cybersecurity and continue to receive annual refreshers, some users may have more access privileges than necessary. If user accounts were to be hijacked or impersonated, attackers would have the opportunity to access the organization with the same access rights as the legitimate users. By enforcing a "need to know" policy, the organization can constrain the impact of breaches to the level of access granted to each individual user. In other words, regardless of the situational awareness of trained and vigilant users, if access controls are limited to using secrecy (i.e., password-only) as opposed to a second layer of authentication such as a code or text message – referred to as "two-factor authentication" – the potential for account takeover is always greater.
3. User error exposes organizations to premeditated and opportunistic cyberattacks. The risk of such events depends on numerous factors that are difficult to constrain and control, including the number of portable devices with access to data, the number of access methods, the access granted to external users with physical access to the premises, and even the number of entrance and exit doors.

Such scenarios are not only easy to illustrate, they can also be presented to management by trusted advisors who can effectively present the need for cyber liability insurance policies. Such coverage is now widely available, and many small and mid-size organizations take out policies every day.

According to Statistics Canada, in 2019 almost one-quarter (24 per cent) of large businesses indicated that they had cyber liability insurance to protect against cybersecurity risks and threats, compared with 14 per cent of medium-sized businesses and seven per cent of small businesses. When the Insurance Bureau of Canada surveyed 300 SME owners, 60 per cent reported that they were not insured, 21 per cent said they were insured and 19 per cent didn't know (Canadian Underwriter, 2019).

Overview
Process
Application
Key Learnings
Resources

In fact, when owners were asked if they have ever considered purchasing cyber insurance for their business, 62 per cent said they had not. Of the total respondents, just over half had no intention of taking out a policy within the next year. When asked about the reason behind unmitigated risks and disruptive losses, respondents indicated that, in part, it was because they did not understand cyber liability insurance. This places the emphasis on the role of accounting practitioners in trusted advisory roles as they are able to explain risk transfer options to management.

Step 2

Cybersecurity controls

Previously in this guidance document, we discussed the need to layer complementary safeguards to address gaps in coverage. The savvy CPA will seek effective visuals and useful metaphors (e.g., the hard-shelled egg with a soft centre representing layered security) to illustrate to management how consistently controls must be deployed.

Additionally, organizations intuitively divide their safeguards between physical measures (e.g., locks on doors), technological measures (e.g., antivirus and firewall software), and administrative measures (e.g., documented policies, procedures and training materials). By striking a balance between these three pillars of cybersecurity, companies are able to compartmentalize their efforts and plan for a scalable, sustainable and resilient protective envelope.

Defence in depth is therefore an effective way to build resilience into a company's protective envelope. But how can organizations achieve security without unnecessary and ineffective overlap? One of the best standardized methods is the NIST Cybersecurity Framework (CSF), whose five main functional areas are subdivided into 23 categories and 108 actual control objectives and outcomes. This visual approach helps organizations understand cybersecurity and map their policies, procedures and compliance priorities to the business of building a scalable risk-management program (depending on the size of the business).

Function identifier	Function	Category identifier	Category
ID	**Identify**	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management

Overview
Process
Application
Key Learnings
Resources

Function identifier	Function	Category identifier	Category
PR	**Protect**	PR.AC	Identify Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Process Protection and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	**Detect**	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	**Respond**	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	**Recover**	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Leveraging NIST's framework as a control scorecard allows organizations to simplify the task of addressing areas where risk may exist:

- Producing an inventory of assets
- Classifying the assets by sensitivity and value
- Creating a list of controls for protecting these assets
- Building procedures for enabling the controls to be effective
- Systematizing processes that manage and monitor controls and procedures
- Enforcing the use of such processes by using policies

Striking the right balance between physical security controls, technological safeguards and administrative security is a good way to layer security without inefficient overlap. This structure is further illustrated in the accompanying MAG case study document, *Cybersecurity From the Trenches*.

Step 3

Governance

Ultimately, the responsibility for *doing the right thing at the right time* rests on the shoulders of management. This means that overseeing all risk at all times is effectively a governance responsibility, albeit one that can be delegated based on functional and operational areas. The balancing act of creating behavioural systems versus enforcing rigid technical constraints is a matter of nesting complementary policies; and again, a cybersecurity framework can help align the need to balance risk with the governance priorities of compliance, resilience, growth and sustainability.

Introducing behavioural and technical controls in a layered manner, therefore, comes together with a functional checklist that maps control categories directly to policies. SMEs should adopt key cybersecurity policies that govern:

- data security and information protection
- risk and asset management
- incident management and associated processes (detection, response and reporting)
- business continuity and recovery (in support of resilience)

Step 4

Compliance

The usefulness of a standardized framework of controls rests in its ability to deliver assurance to internal and external stakeholders about the adequacy of its controls and practices for protecting information assets. Professional risk managers often fine-tune the rich diversity of controls supplied by such a framework to the practical requirements of an organization and the compliance demands of industry standards and legislation.

While some legislation (e.g., Canada's diverse privacy laws) may not be precisely prescriptive, industry standards and audit frameworks such as the AICPA's Trust Services (and associated SOC 2 requirements) are precisely designed to uncover threats to information assets, operations and business continuity. In effect, SOC 2 audits look at Trust Services Principles (TSPs) through the five criteria of security (i.e., security, availability, processing integrity, confidentiality and privacy). For this purpose, the AICPA offers mapping documents, which are included in the references section at the end of this document. The TSPs include direct reference to the three objectives of information security: confidentiality, data integrity and availability.

Step 5

Resilience and sustainability

The importance of business continuity for small and medium-sized businesses is reflected not only in the Trust Services criterion of availability, but also in the focus on resilience that is at the core of every risk management program.

An organization should be impermeable to identified threats, but it must also be resistant to emerging threats and unanticipated risks. To properly assist businesses, CPAs must focus on introducing NIST CSF controls or their simplified counterparts within the federal government's CyberSecure Canada program. As mentioned above, monitoring controls serve to detect breaches and anticipate risks that can be mitigated or corrected with effective safeguards. Resilience, therefore, protects an organization's operations by helping it adapt to new and existing threats, leveraging employee awareness and implementing innovative controls.

In doing so, business and accounting professionals can use resilience, adaptability and innovative approaches to build cybersecurity from within organizations. By adopting standardized best practices, organizations can apply the drivers of the RAISE philosophy, as introduced by CPA Canada, to reach sustainable operations and growth with controlled risk to operations, information assets and human resources.

Key Learnings

As earlier shown by Canada's privacy commissioner's privacy study, it has become clear that breaches remain an ongoing threat for all organizations. Businesses must be aware of the myriad of potential risks and tackle them with a combination of technology, training, policies and processes.

The trends that drive economic progress – innovation, manufacturing, globalization – are increasingly reliant on the use of technology for optimized financial management. With such unique expertise and operational insight, today's CPA is ideally positioned to be a trusted advisor, strategic influencer and visionary. The role of the CPA has shifted to meet the need to support short-term compliance requirements, medium-to long-term strategic vision and overall flexibility to adapt to changing market forces.

As a strategic advisor, the CPA must acquire and maintain expertise in risk management, governance, cybersecurity and compliance. This educational role also plays a key part in demystifying data protection and making risk a concrete, tangible aspect of key roles within the organization (using accessible resources, self-assessments and example-based approaches in place of abstract concepts and theoretical models).

This position empowers savvy practitioners to deliver on the evolving needs of their firms and clients, advising on the strategic cybersecurity planning and thriving in the knowledge economy.

Technology has taken centre stage in the value-based relationship between client and advisor, organization and practitioner. Intangible assets are now collected and retained by systems whose security impacts compliance, governance, and profitability. Cybersecurity determines every organization's resilience, adaptability and ability to remain at the forefront of its industry. Within this context, the CPA is a central figure in the timely strategic and operational decisions that determine the health of the organization.

Resources

References

Business.com, Why small business cyberattacks could prompt next recession (2019)

Canadian Underwriter, Brokers leaving a lot of SME cyber business on the table: Leger poll (2019)

CIO, By 2020, 60 percent of digital businesses will suffer major service interruptions (2018)

Cision Canada, 9 in 10 Canadian companies suffered at least one cyber security breach last year (2018)

Cybercrime Magazine, 60 Percent of small companies close within 6 months of being hacked (2019)

DarkReading, 55% of SMBs would pay up post-ransomware attack (2019)

IBM, How much would a data breach cost your business? (2020)

Infrascale, Infrascale survey reveals close to half of SMBs have been ransomware attack targets (2020)

Office of the Privacy Commissioner of Canada, A full year of mandatory data breach reporting: What we've learned and what businesses need to know (2019)

Shred-it and Ponemon Institute, *Security of Confidential Documents in the Workplace* (2019)

Standard Chartered, The high cost of business email compromise (BEC) fraud (2020)

Statistics Canada, Impact of cybercrime on Canadian businesses (2017)

365 Technologies Inc., Ransomware stats and facts (2019)

Additional resources

Also by Claudiu Popa:

- *The Canadian Privacy and Data Security Toolkit for SME* (1st and 2nd ed. CPA Canada, 2015)
- *Managing Personal Information for Privacy-Savvy Organizations* (Carswell, 2012)
- *The Canadian Cyberfraud Handbook* (Thomson Reuters, 2017)
- *Technology Spotlight: Cybersecurity and Data Protection* (CPA Canada, 2019)
- *Technology Spotlight: Securing Your Brand and Reputation on Social Media* (CPA Canada, 2019)

Overview
Process
Application
Key Learnings
Resources

Further reading

- CPA Canada, *Management Accounting Guideline (MAG)—From Data to Decisions: A Five-Step Approach to Data-Driven Decision-Making* (2021)
- AICPA, Controls Mapping Documents (2017)
- Industry Canada, The CyberSecure Canada Control Framework (2021)
- NIST, Cybersecurity Framework (2020)
- The Canadian Centre for Cyber Security, The Path to Enterprise Security (2020)

About the author

Claudiu Popa, CISSP, CIPP, PMP, CISA, CRISC, is a certified information security and privacy professional and media contributor on enterprise risk management, IT security and data protection. With over 25 years of global experience in security auditing, international standards and board-level risk consulting, Claudiu is a trusted management advisor to Canadian enterprises and their stakeholders, supporting critical security strategy and decision support for privacy and security compliance, data protection and cybercrime prevention.

He is the author of four published books, numerous articles and multiple academic papers on information protection, compliance and risk governance based on primary cybersecurity research. As a certified professional, Claudiu remains an ardent champion of information security and a trusted corporate coach to Canadian organizations that are passionate about improving their security and protecting their customers.

Overview
Process
Application
Key Learnings
Resources

public class PrimitiveParameters
{
public static void main(String[] args)
{go();
}
public static void go()
{int x = 3;
int y = 2;
System.out.println("In method go. x: " + x + " y: " + y);
falseSwap(x,y);
moreParameters(x,y);
public static void falseSwap(int x, int y)
{System.out.println("in method falseSwap. x: " + x + " y: " + y);
int temp = x;
x = y;
y = temp;
System.out.println("in method falseSwap. x: " + x + " y: " + y);
}
public static void moreParameters(int a, int b)
{System.out.println("in method moreParameters. a: " + a + " b: " + b);
a = a * b;
b = 12;
System.out.println("in method moreParameters. a: " + a + " b: " + b);
falseSwap(b,a);
System.out.println("in method moreParameters. a: " + a + " b: " + b);
}

cpacanada.ca/MAGs

DISCLAIMER

This paper was prepared by CPA Canada as non-authoritative guidance.

CPA Canada and the author do not accept any responsibility or liability that might occur directly or indirectly as a consequence of the use or application of or reliance on this material.