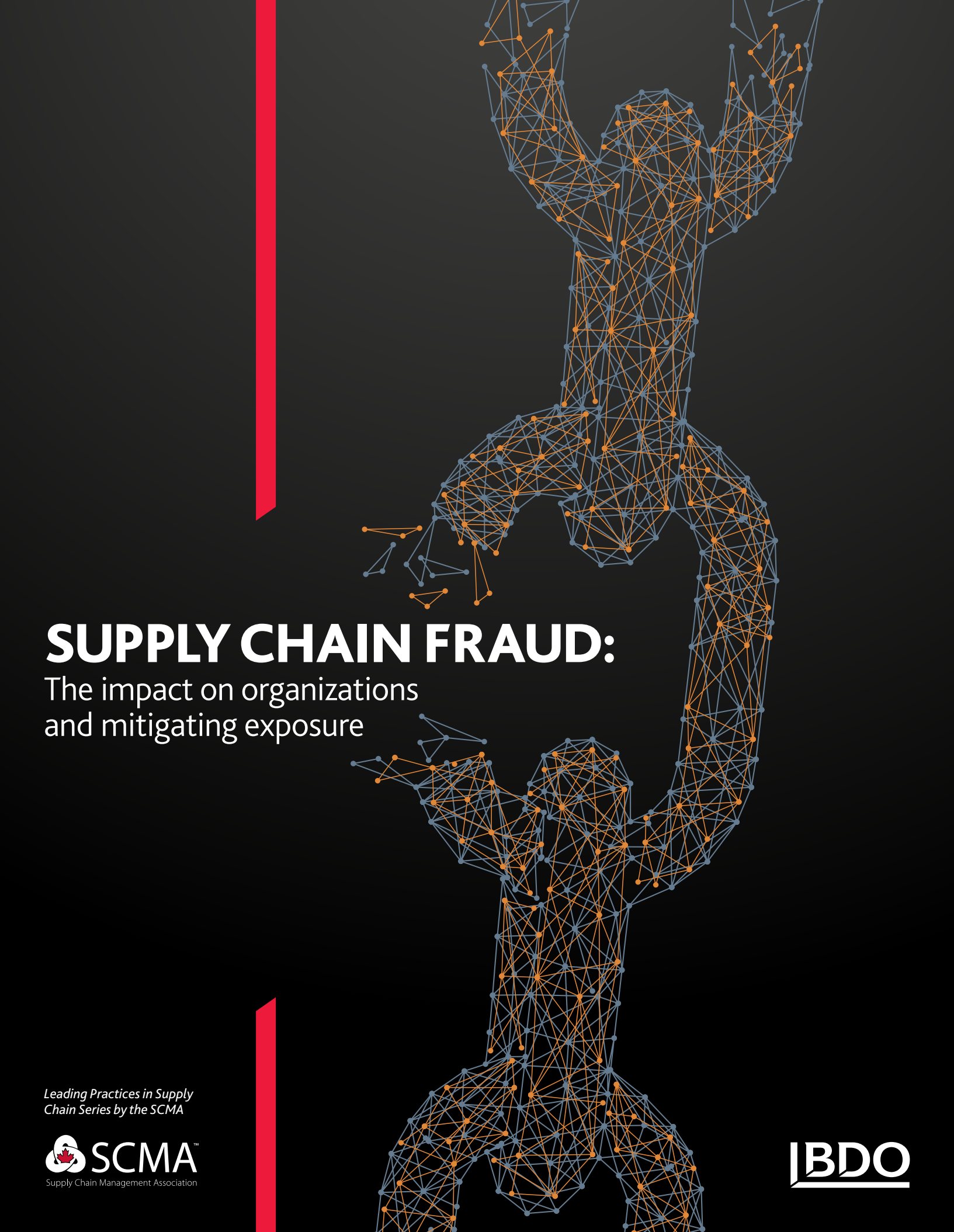


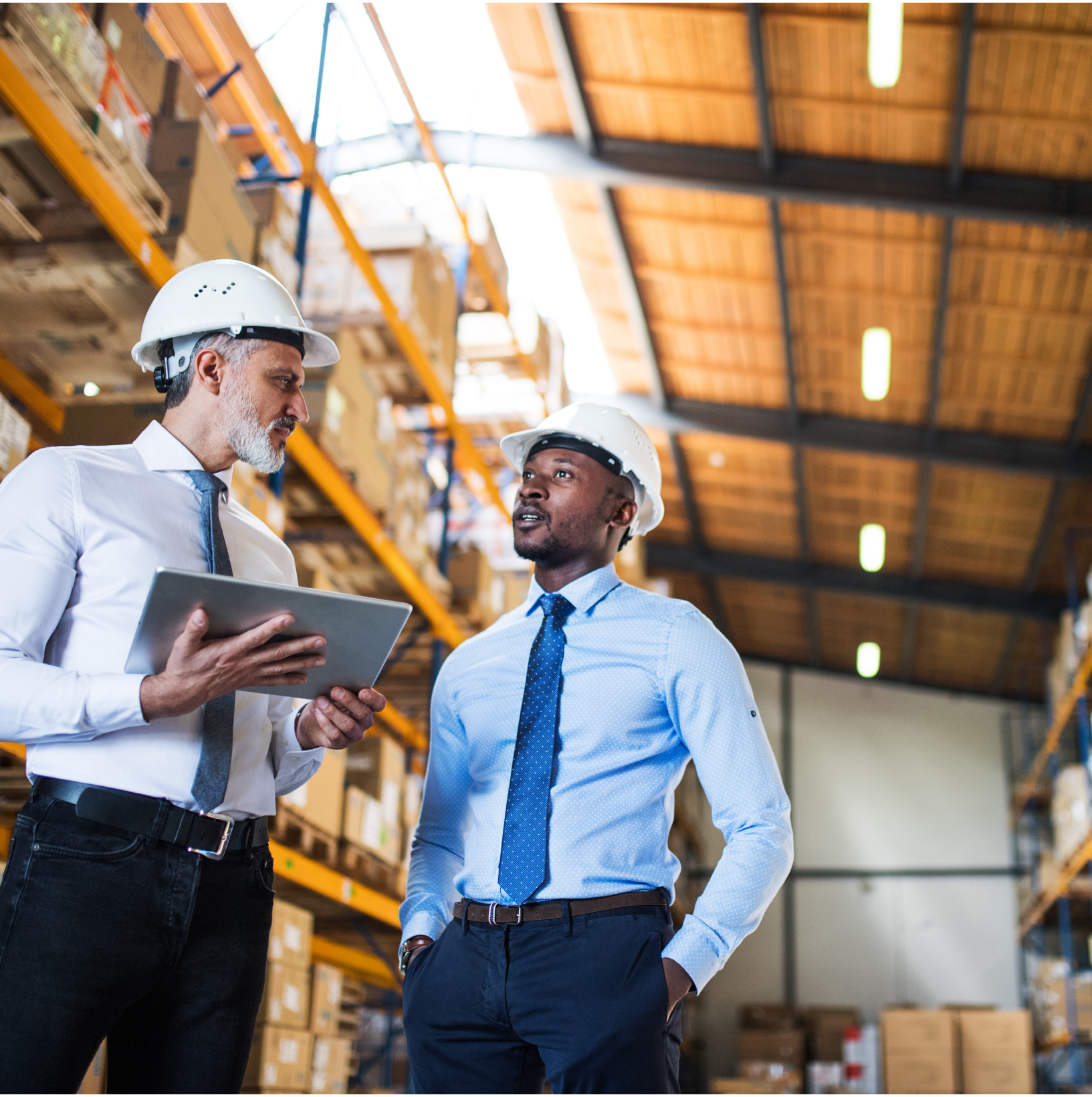
SUPPLY CHAIN FRAUD:

The impact on organizations and mitigating exposure

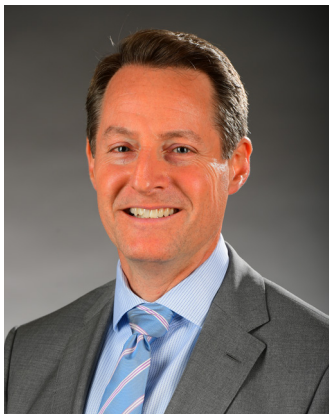
Leading Practices in Supply Chain Series by the SCMA

SCMA™
Supply Chain Management Association

BDO



MESSAGE FROM THE PRESIDENT AND CEO OF SUPPLY CHAIN MANAGEMENT ASSOCIATION



Christian Alan Buhagiar

SCMA™
Supply Chain Management Association

Developed by BDO Canada in collaboration with Supply Chain Management Association (SCMA), this first report in the new SCMA series, *Leading Practices in Supply Chain*, offers Canadian supply chain professionals a comprehensive guide to the most significant issues of fraud and strategies to manage them. With its publication, we have achieved two strategic goals: to disseminate beneficial information to the community and collaborate with industry to unlock opportunities for success.

As the report notes, supply chain fraud is a threat for organizations of all sizes and many businesses do little to protect themselves. We see a clear imperative—as the voice of Canada's supply chain—to share the insights this report contains.

Fraud is a problem that has plagued supply chains for as long as people have been involved in trade, and it remains despite growing transparency throughout supply chains. Understanding the varieties of fraud that affect supply chains and the processes to prevent such frauds is an important first step in defending your company from fraudulent activity.

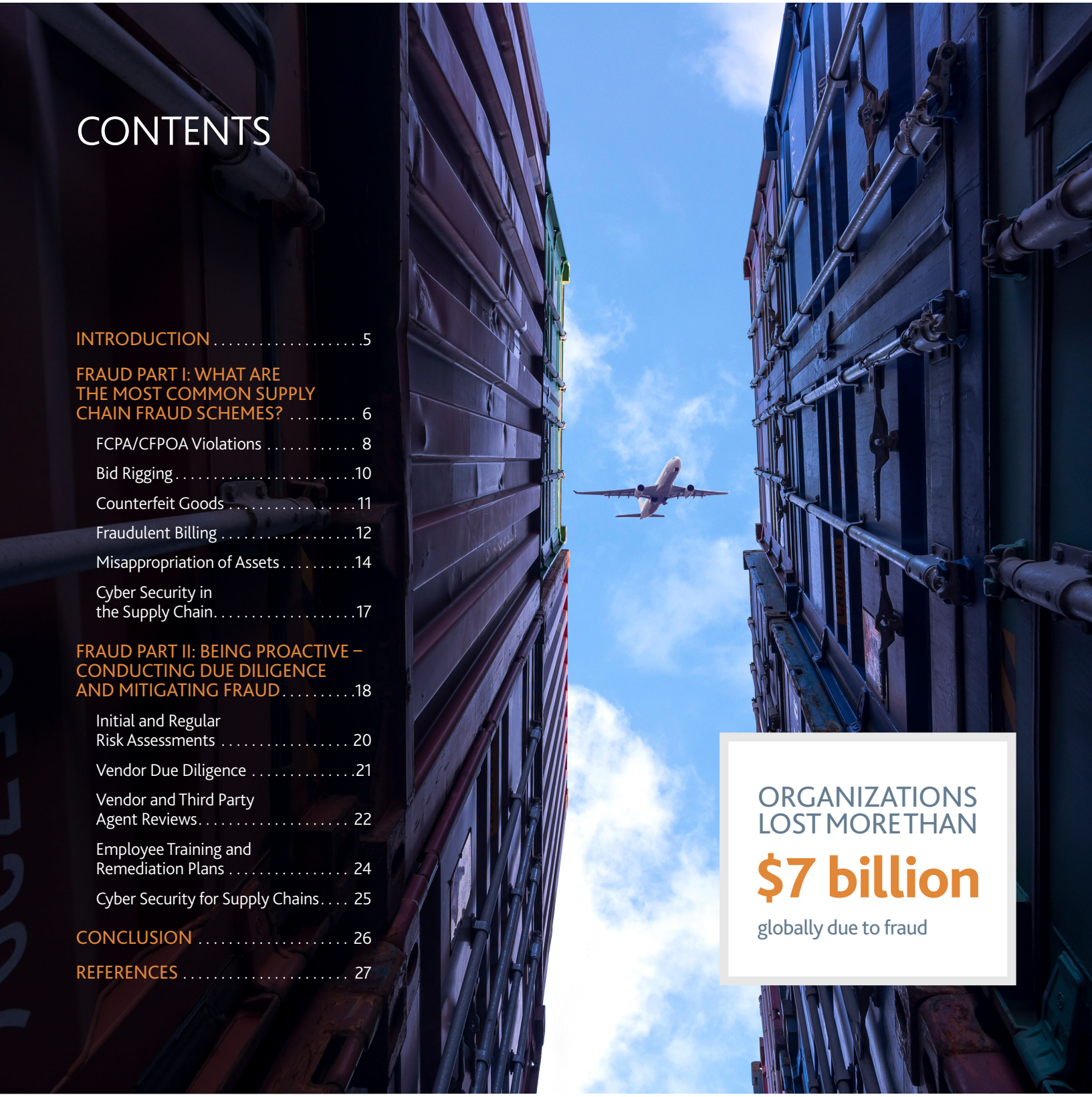
Becoming a victim of fraud exposes your company to challenging losses, potentially of money, time and reputation. Learn how to reduce the risk of fraud in your supply chain by implementing the steps prescribed in Part II of this report to boost your company's security and proactively prevent fraud in your operations. With what you learn from this report, you will be armed to improve your company's internal controls and thereby guard against a host of threats.

We are delighted to collaborate with BDO Canada in the publication of this report and hope it will be a valuable reference for the supply chain community in understanding and managing fraud in the supply chain.

Yours truly,

Christian Alan Buhagiar

CONTENTS



ORGANIZATIONS LOST MORE THAN

$7 billion

globally due to fraud

INTRODUCTION

In the era of Industry 4.0, ultra-high efficiency production, and borderless commerce, supply chain management is a vital strategic function. Protecting supply chain integrity is increasingly a key priority at the corporate governance level. Indeed, it is an organizational risk management imperative.

Supply chain fraud is a threat for organizations of all sizes and in all industries. Unfortunately, many businesses do not take even minimum precautions to protect themselves. Just over 30% of supply chain executives indicated that corruption and bribery are addressed in their company's supply chain management, according to a 2017 Economist Intelligence Unit report.[1] The harsh reality is that fraud is not rare, no organization is immune to it, and it can occur when least expected. There has always been, and continues to be the sense, that "fraud doesn't happen in my company" or "it's someone else's problem." This is not evident in the data or in our experience.

Organizations lost more than $7 billion globally due to fraud, according to the Association of Certified Fraud Examiners (ACFE) biannual 2018 Report to the Nations.[2] Of these losses, organizations only recover a small percentage.

Moreover, losses arising from fraud typically extend far beyond the direct financial losses of misappropriated assets. Consequential costs can include reputational damage, missed commercial opportunities, diminished productivity, investigation and prosecution costs and further investments in internal controls to ensure the problems do not recur.

The focus of this white paper is on the most common supply chain fraud schemes that we have encountered in our practice, including: Foreign Corrupt Practices Act (FCPA) violations, bid rigging, fraudulent billing, counterfeit goods, and misappropriation of assets. We also touch upon increasingly serious cyber threats on supply chains.

Proactive measures can greatly mitigate the risk of supply chain fraud, which include vendor due diligence, compliance verification, and staff training. Effective internal control systems are vital to preventing and detecting improper conduct. Diligence is essential, at every step.

JUST OVER

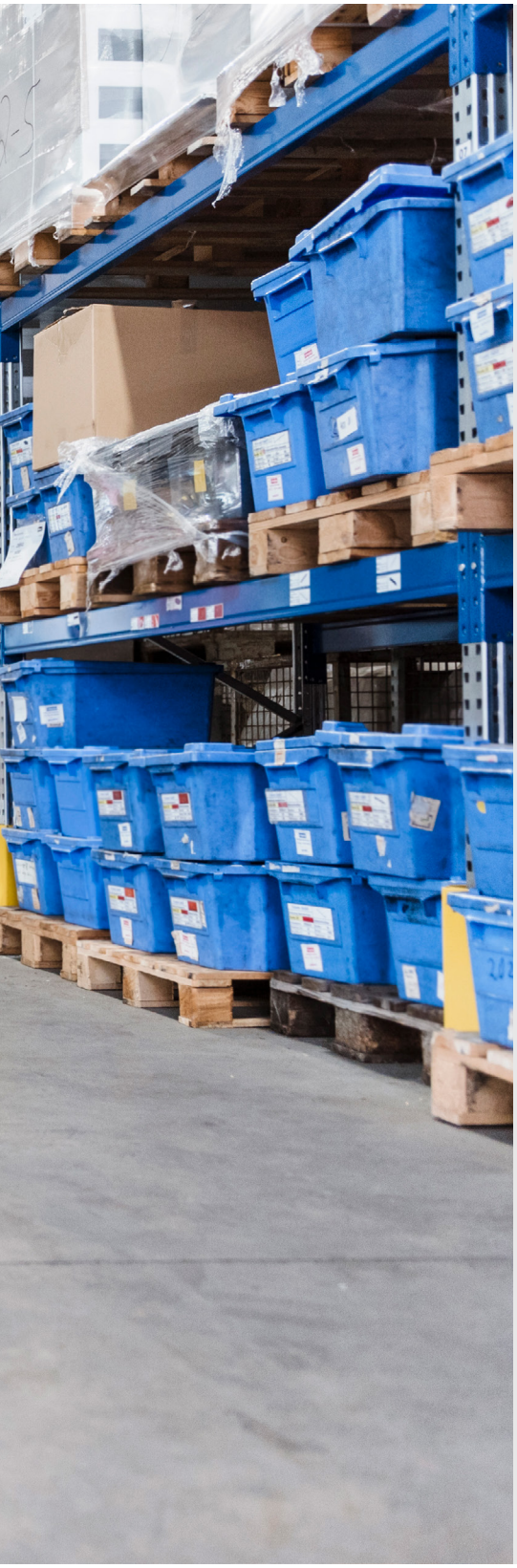
30%

of supply chain executives indicated that corruption and bribery are addressed in their company's supply chain management

Proactive measures can greatly mitigate the risk of supply chain fraud

FRAUD PART I:

What are the most common supply chain fraud schemes?



Supply chain fraud is a pervasive and growing business risk for organizations. This white paper addresses the most common schemes, such as:

FCPA/CFPOA violations:
The FCPA (a U.S. statute) or Canada's Corruption of Foreign Public Officials Act (CFPOA) prohibit companies from influencing foreign officials with monetary payments or other rewards. These laws are intended to prevent companies with a nexus to the U.S. or Canada, respectively, from engaging in practices in foreign countries that are illegal in their domestic jurisdiction (e.g. bribery).

Bid rigging:
Bid rigging occurs when supposedly competing parties collude to arrange the winner for a contract, or when a vendor is coached by the buyer to prepare a superior bid. This could include preferential access to information or withholding information.

Counterfeit goods:
Misrepresenting the quality, service, or origins of a product.

Fraudulent billing:
Overbilling for goods and services, or billing for services that were never rendered or not delivered as contracted.

Misappropriation of assets:
Improper use of resources and inventory fraud, such as redirecting payments or diverting goods.

Cyber security:
Emerging at the forefront of supply chain risk is cyber security. BDO's global cybersecurity experts have identified a significant increase in the frequency of supply chain attacks over the past year. Attackers seek to exploit weaknesses in third-party service providers to gain access to proprietary information or engage in ransom activities.

FCPA/CFPOA VIOLATIONS

Corruption in the supply chain

Any organization with a connection to the U.S. is subject to its anti-corruption statute, the FCPA. Businesses that are active in Canada fall under the CFPOA. Both the FCPA and CFPOA seek to combat corruption in foreign jurisdictions by companies operating with nexus to the U.S. or Canada. Specifically, the FCPA and CFPOA are designed to combat bribery of foreign public officials in relation to obtaining or retaining business. Prohibitions against bribing domestic officials exist in the criminal law statutes of each country. Companies within the scope of these laws may be punished with fines and/or imprisonment (of its officials) for acts of bribery committed by their own employees or agents on their behalf.

Corruption is the second most common scheme in every global region surveyed by the ACFE. Bribes and kickbacks take many forms, which may be exchanged for different benefits. This could include overpaying for goods or services, accepting an unqualified supplier or receiving inferior goods or services. Anyone — an owner, manager or employee — can perpetuate corruption. Corruption is one of the largest fraud risks for organizations in many industries. The following industries have the highest proportion of corruption relative to total fraud cases: the energy industry (53%), manufacturing (51%), and government and public administration (50%).[2]

FCPA/CFPOA violations can and often negatively impact organizations in a number of ways.

- Expulsion from a foreign country or prohibitions from conducting business in that country.
- Financial consequences, from $10,000 per violation, up to $5 million.
- Imprisonment of top ranking individuals for up to 20 years.
- Bribery is, by nature, informal and secretive. Agreements may be unspoken and almost certainly undocumented. This inherent ambiguity creates operational risk.
- Illegal payments (or promises to pay) expose an organization to extortion risk or at least continuing demands for greater benefits.
- Bribery generally occurs when an organization does not want to follow rules and regulations, typically due to either expediency and/or the desire to avoid costs and earn higher profits (e.g. building codes, food safety, transportation or other regulations). Such attitudes speak to the culture of an organization, including its corporate governance and management integrity. Rules and regulations generally exist to protect workers, consumers or the public at large. Thus, circumvention is not only illegal, but also unethical.

CASE STUDY

Company A is a leading integrated oil and gas company. As a global corporate citizen, Company A sought independent assurance to verify that its operators were complying with internal policies, contracts, and laws regarding corporate conduct. BDO was engaged to focus on two primary areas within the company's global supply chain, including:

1. Evaluating supply chain vendors' compliance with Company A's anti-corruption provisions as detailed in each vendor's contracts.
2. Determining whether the vendors were complying with the financial terms of the contracts, and quantifying any recoveries owed to the company due to the supply chain vendor's failure to comply with agreed upon pricing terms.

BDO conducted a comprehensive analysis of Company A's global operations, including in-depth documentary reviews as well as on-site visits. Over nearly two years, BDO attended Company A's active operating sites in South America, North America, Asia-Pacific, the Middle East, Africa, and Europe. They performed detailed analyses of each vendor selected for review, conducted interviews, tested transactions, assessed vendor control environments, validated whether required training was occurring, and prepared detailed reports outlining our findings and recommendations.

BDO determined:

- Supply chain vendors regularly did not comply with the anti-corruption provisions in their contracts with Company A.
  - There was evidence that influence payments were made to local officials. Generally, contractors made these payments while acting under local customs and norms. While there was no indication of other laws being broken or circumvented, the payments were intended to expedite approvals or transactions and conflicted with Company A's corporate code of conduct and domestic laws.
  - Some vendors, or agents of those vendors, had demanded improper payments from Company A (at least some of which were paid by the subsidiary operating company employees).
- Supply chain vendors failed to adhere to the commercial terms of their contracts and owed rebates to the Company A.
  - Rebates for volume targets were not being paid when earned.
  - Vendors were keeping the rebates they received in "cost-plus" arrangements and not passing them on to the contracting company.

The improper payments both by and indirectly on behalf of Company A clearly created significant reputational and legal risk for the company. If discovered and prosecuted, Company A's global operations could have been seriously compromised, including potential expulsion from major projects and exposure to substantial fines.

BID RIGGING

Colluding in the bidding process

Bid rigging "occurs when bidders agree among themselves to eliminate competition in the procurement process, thereby denying the public a fair price."[3] An open competitive bidding process is designed to counteract the risks that are inherent in the procurement of goods and services through non-competitive sourcing.

A common form of bid rigging involves supposedly competing vendors colluding to coordinate or propagate the winner during a bidding process. For example, competing vendors may agree to alternate being the lowest bidder, abstain from a bidding round, or submit deficient bids. Other bid rigging agreements involve subcontracting part of the main contract to the losing bidders, or forming a joint venture to submit a single bid. These actions stifle the market competition that is fundamental in providing the benefits of open bidding.

Bid rigging can also occur when a buyer wants to create an illusion of competitive procurement whilst directing the work to a preferred vendor. The preferred vendor may be provided inside information or be coached to create a bid that is, at least superficially, superior to other vendors.

Bid rigging can result in organizations paying higher prices or receiving inferior goods and services. If an organization falls victim to a bid-rigging scheme, they may pass the extra costs or inferior goods to consumers and others involved in the supply chain. If a government entity pays an inflated amount for services, these additional costs are often passed onto taxpayers.

Bid rigging is a criminal offence in Canada. Organizations or individuals convicted of bid rigging face fines and/or imprisonment for up to 14 years.

CASE STUDY

An international labour union represents a variety of skilled trades employed in the construction industry and has approximately 100,000 members across North America.

The union retained BDO to conduct an investigation into allegations of potential inappropriate activity at their local collective in Toronto, Ontario (the Local). The Director of the Local purportedly had both a related party connection with, and a direct financial interest in, certain vendor companies. The Director allegedly approved these contractors to complete work, and was suspected of approving inflated invoices that were paid by the Local.

BDO's engagement involved the following:

- Reviewing and assessing the internal control environment at the Local. This included reviewing payments made to key vendors, payroll expenses, corporate credit card transactions, expense reimbursements, capital expenditures, procurement process (sole sourced and open bid contracts), employee expense policies, and reports.
- Conducting interviews with management, in-house counsel, finance staff, and general office staff.
- Conducting interviews with multiple suppliers of the Local.
- Quantifying losses suffered by the Local due to the activity of a senior level employee who managed the Local.

BDO identified extensive internal control weaknesses in the Local's procurement process. The historical policies and practices did not address related party contracting. Importantly, no requirements existed for disclosure of non-arm's length transactions nor was there governance oversight of the Director.

BDO provided the Local with recommended actions to improve the internal controls and help avoid this type of fraud in the future.

▲ Back to contents

COUNTERFEIT GOODS

Misleading consumers with inferior products

Counterfeit goods involve misrepresenting the quality or service of the product. This scheme can include falsely labelling products or using substandard materials in products, which can be potentially harmful to consumers. The motivation for using substitute products is usually cost related — inferior materials are less expensive (at least in terms of short-run, direct costs).

Another reason for misrepresenting products is to avoid tariffs. In an era of growing global trade and increasingly complex regulations, product origin is an important factor in assessing tariff costs.

In 2013, the estimated value of international and domestic trade in counterfeit and pirated goods was $1.3 trillion USD. By 2022, the estimated economic value could soar from $1.9 to $2.81 trillion USD, according to International Trademark Association (INTA).[4]

Counterfeit goods represent severe risks to an organization's reputation and brand, as well as their supply chain . Customers pay a premium for products that are purported to be from a specific region or country. Customers lose trust in a company when they discover that a product is of counterfeit quality or origin. In certain industries, like food and healthcare, counterfeit goods not only result in the loss of customer goodwill, but also create potential health risks. The loss of market integrity can take a serious toll on a company's viability.

CASE STUDY

A large privately owned food processing business held exclusive contracts to produce private-label goods for several national retailers. These private-label goods included items represented to be of specific origin and quality.

Based on unusual import activity and irregularities in the reporting of regulated ingredients, federal and provincial regulators appointed BDO forensic accountants to investigate the manufacturing activities of the processor.

Through detailed review of production and purchasing records, BDO identified discrepancies in the sourcing of raw materials used in the production of the private-label goods. Contrary to its contracts with national retailers and the assertions of the processor, goods were not being produced exclusively using domestic, certified organic ingredients. Instead, the imported materials were not only non-organic, but also included highly processed or chemical additives.

Misrepresenting ingredients created serious and immediate risks for the national retailers. Many of the private-label goods were co-branded with various high profile marketing programs (e.g. 100% organic or produced with locally sourced ingredients). This exposed retailers to breach of contract, false advertising, and mislabeling complaints. More importantly, the retailers risked losing the trust of their customers, who had paid premium prices for what they believed were premium goods.

This scheme was detected by exercising contractual audit rights to examine the financial, purchasing, and production records of the processor. The processor initially attempted to restrict the scope of the audit to records that were directly related to the contracts in question. BDO established that broader records were necessary due to the production practices of the processor. Inputs were not segregated or individually tracked. Rather, raw materials from different sources were commingled in storage. This factual basis formed the foundation of the legal argument to secure unfettered access to the processor's complete business records.

Following BDO's report, the retailers terminated their supply contracts with the processor for private-label goods.

FRAUDULENT BILLING

Paying for goods or services not received

Fraudulent billing involves vendors improperly overcharging for goods or services. This ranges from billing for services or goods not rendered to charging prices in excess of agreed rates. Asset misappropriation, which includes fraudulent billing, is the most common fraud scheme, occurring in 89% of the cases in ACFE's 2018 study.[2]

Fraudulent billing is often a surprise to management. Companies do not pay adequate attention to verifying vendor invoices and often assume that vendors are billing according to agreed-upon terms. Unfortunately, this may not hold true in practice as excess billing or duplicate billing can occur by mistake or with intent.

A complicated network of vendors can also increase the risk of improper billing. Layers of sub-vendors can create confusion where earned rebates may not be accurately credited or sales tax (HST) is improperly collected without a requirement to remit.

Using a ghost vendor is another common fraudulent billing scheme. In such cases, an employee or contractor creates a shell company, bills for fabricated services, and then funnels payments received to bank accounts they control. This is outright fraud with a non-existent vendor.

CASE STUDY

The Auditor General's (AG) office of a Canadian metropolis engaged BDO to provide investigative and forensic accounting services. The AG's office had concerns related to contract compliance and a potential conflict of interest involving one particular vendor providing services to the City.

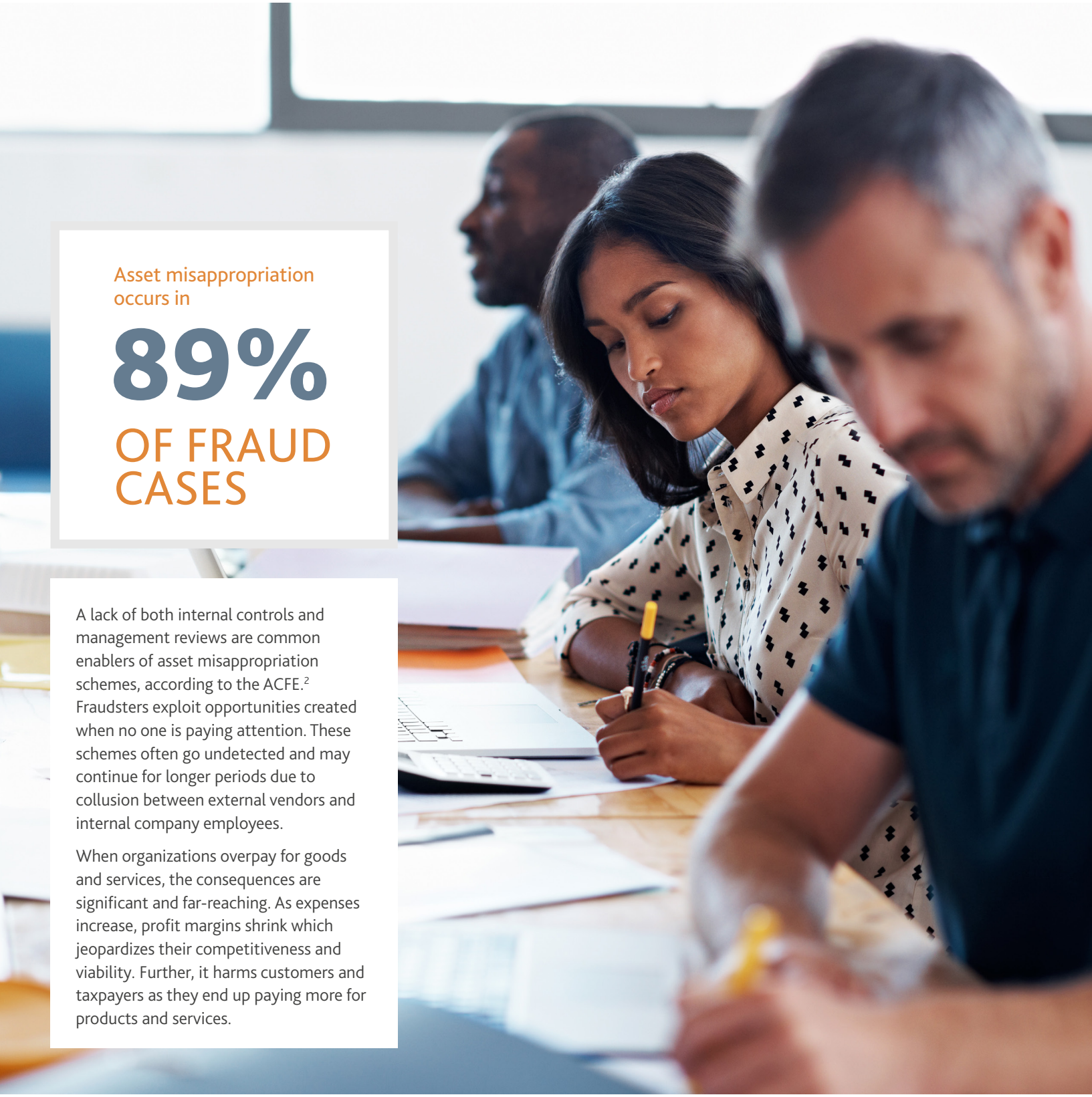
BDO coordinated with the AG's office to gain an understanding of their suspicions and reviewed the AG's preliminary investigation results. Our work focused on the areas with the highest degree of risk and/or likelihood of improper conduct. The engagement team conducted numerous interviews with the AG's office, City staff, and a former vendor employee. BDO reviewed and analyzed source transaction documents, including purchase orders, contracts, invoices, and related supporting documentation.

BDO performed detailed analysis and compared the rates and prices billed to determine if the vendor complied with the pricing schedules in the contracts. The engagement team identified irregularities in the billings and services provided by the vendor, which included:

- Duplicate charges
- Overbilled (incorrectly priced or misstated quantity) parts and labour hours
- Discrepancies between the invoices and supporting documentation

The investigation revealed a significant lack of controls over confirming the vendor has completed work prior to approval of payment, such as ensuring work was completed, if prices charged matched contract prices, and whether the work was required in the first place. There was, in large part, a blind reliance on the vendor to do the work required, bill accurately, and provide competitive pricing. The lack of appropriate controls and oversight allowed the scheme to go on for a number of years without detection. Taxpayer dollars were misappropriated.

The report included various recommendations for improving internal controls to minimize the risk of similar fraud in the future.



Asset misappropriation occurs in

89%

OF FRAUD CASES

A lack of both internal controls and management reviews are common enablers of asset misappropriation schemes, according to the ACFE.[2] Fraudsters exploit opportunities created when no one is paying attention. These schemes often go undetected and may continue for longer periods due to collusion between external vendors and internal company employees.

When organizations overpay for goods and services, the consequences are significant and far-reaching. As expenses increase, profit margins shrink which jeopardizes their competitiveness and viability. Further, it harms customers and taxpayers as they end up paying more for products and services.

MISAPPROPRIATION OF ASSETS

Are you closely monitoring your inventory?

The improper use of resources in supply chain fraud covers a wide spectrum. This white paper focuses on misappropriating assets, including employees taking company assets for personal use, withholding rebates, and stealing. Cheque and payment tampering, billing, and theft of noncash assets rank among the costliest scheme types and usually present the highest risk to organizations, according to the ACFE.[2] To prevent such frauds, companies should install strong physical security, including continuous monitoring of premises (such as retail or warehouse locations) and transportation vehicles. The diversion of assets, along with the ongoing measures to detect and monitor theft, often represent significant costs to the organization (and higher prices for the consumers of their goods or services).

Inventory fraud involves outright stealing physical inventory and misrepresenting inventory records on financial statements. Inventory theft is easier to prevent and detect with ongoing monitoring if perpetrated by individuals acting alone. However, when carried out via collusion with employees of different roles and responsibilities, it becomes harder to detect. For example, a scheme that involves personnel from shipping/receiving (physical custody of assets) and the accounting department (access to books and records) can be more difficult to uncover. Collusion often overrides the internal controls, such as the segregation of duties, within an organization.

"Cheque and payment tampering, billing, and theft of noncash assets rank among the costliest schemes."

CASE STUDY

Having close relationships with customers is good for business. However, having too close of relationships can also be a significant red flag for fraud. A senior sales representative in a large distribution company took great pride in his deep relationships with key customer accounts. One day, the distributor received a request from the accounting department of a large national account. The customer asked for copies of all rebate cheques issued to the distributor for the past five years. As it turns out, the customer did not receive most of the rebate cheques.

The distributor retained BDO Forensics to conduct a discrete investigation. Upon reviewing the available banking and accounting records, including cancelled cheques and cheque requisition forms, BDO discovered a simple but effective diversion scheme.

- The distributor's sales representative had indeed developed a very close relationship with a senior manager in the customer's finance group.
- From time to time, the sales representative would requisition cheques, ostensibly to issue payments to the customer earned on volume or promotional rebates.
- Instead of mailing the rebate cheques, the sales representative insisted on hand delivering the cheques to the customer.
- The cheques were never delivered to the customer. The sales representative took the cheques to an intermediary, who exchanged cash in the same amount as the rebate cheque.
- The sales rep then took the cash and delivered it (presumably minus his share) to the finance manager.
- This scheme was perpetrated over many years, with the confirmed diversions totaling well into the hundreds of thousands of dollars.

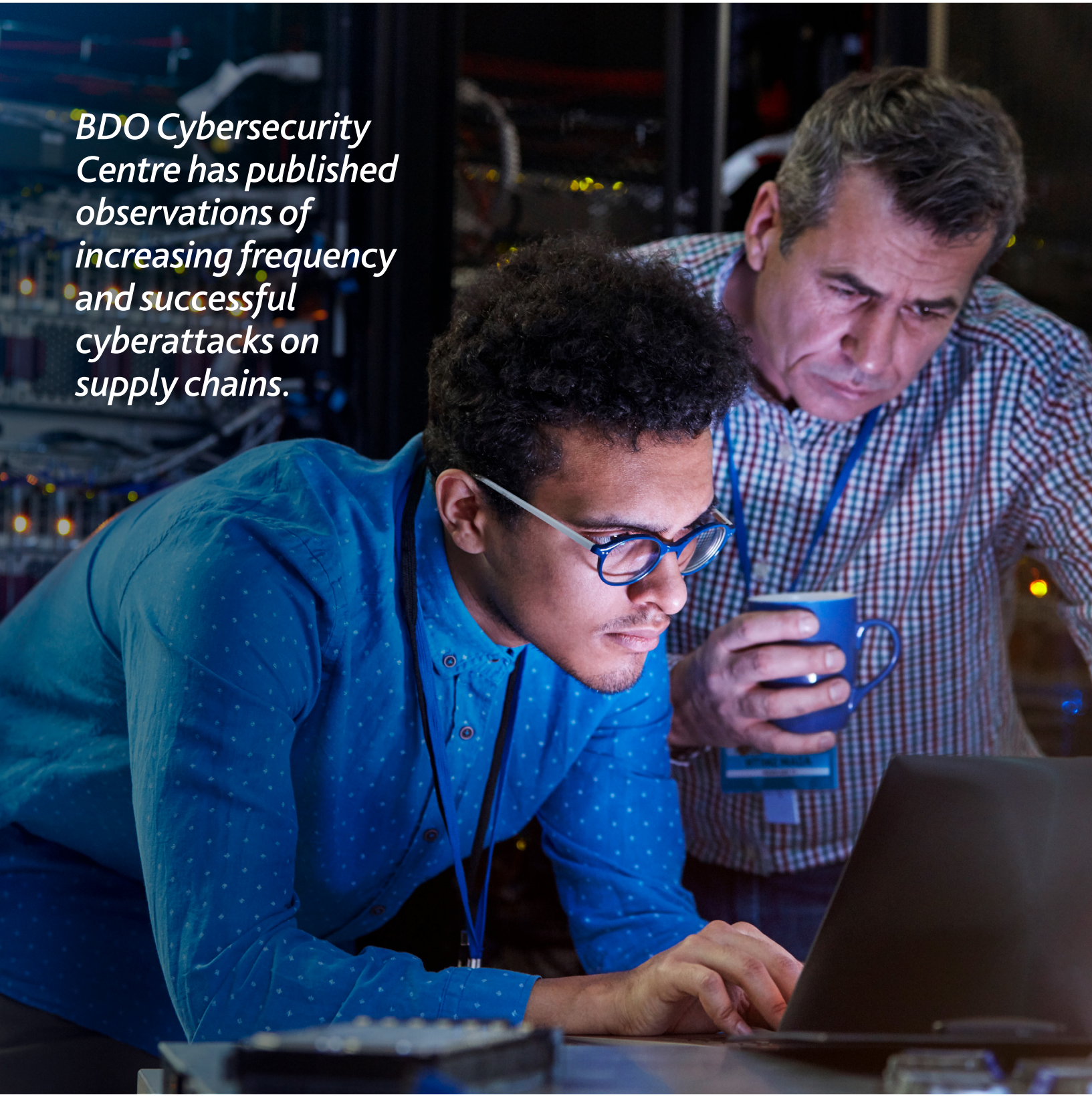
This scheme was simple and should have been detected by routine internal controls.

Distributor's perspective:

- Segregation of Controls: The sales representative should not have been permitted to requisition cheques and have custody of the negotiable instruments. The cheques should have been mailed directly to the customer.
- Payment Verification: The depositing account (payee) should have been verified in the course of routine bank reconciliation procedures.
- Policies and Procedures: Someone other than the sales representative should have been required to authorize credits and deductions from customer rebate accrual accounts, including verification of rebate entitlement.

Customer's perspective:

- Policies and Procedures: Rebates earned from suppliers should have been tracked and reconciled with periodic account statements from the supplier.


BDO Cybersecurity Centre has published observations of increasing frequency and successful cyberattacks on supply chains.

CYBER SECURITY IN THE SUPPLY CHAIN

Protecting supply chains from technology vulnerabilities

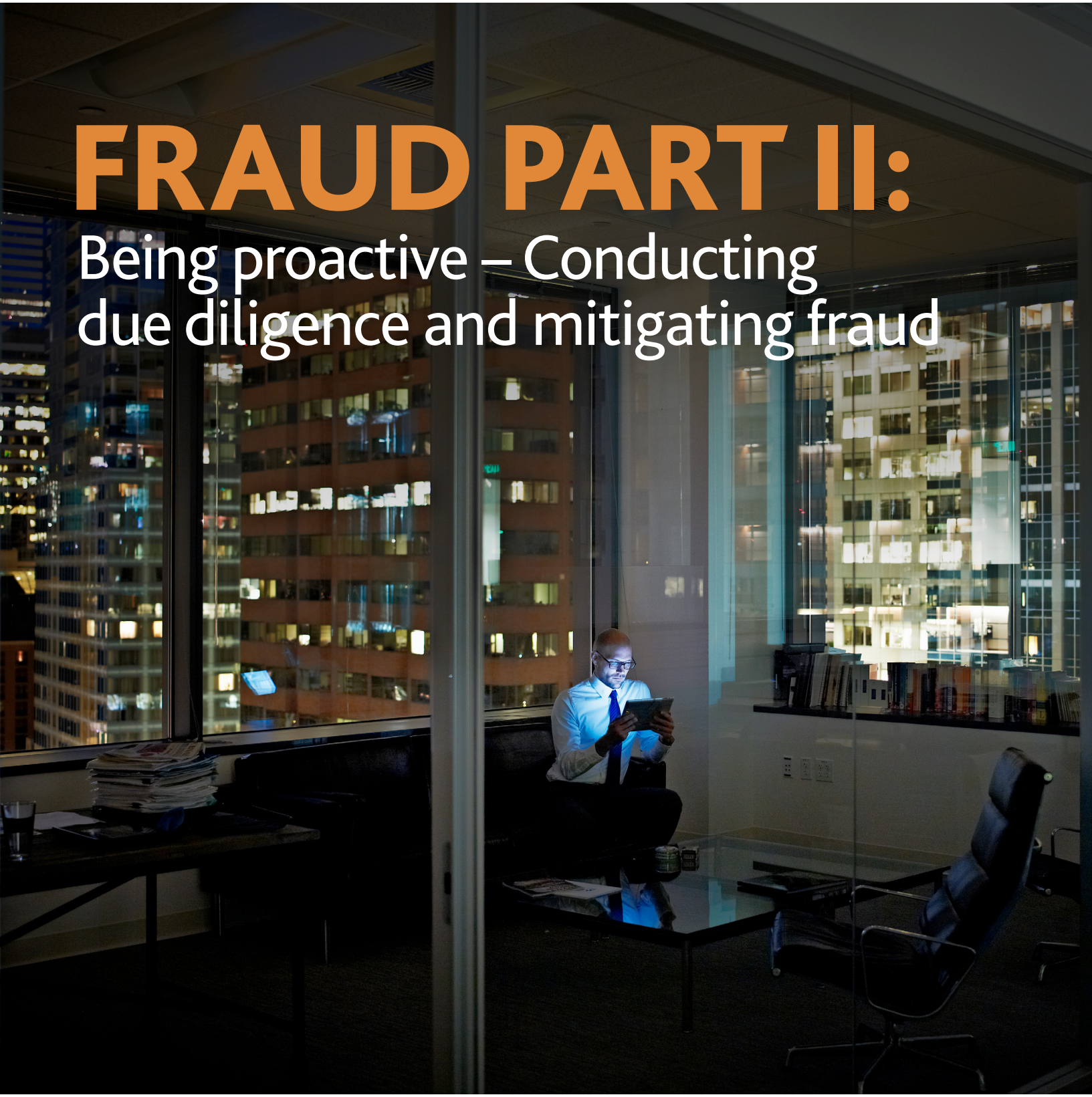
As supply chain partners become more integrated from a technology perspective, protecting the integrity of data and communications is a top priority. Blockchain technology, using encrypted interlinked transaction records, offers substantial safeguards from fraud involving altered records.

Nevertheless, the recent reporting involving an alleged widespread and long-running hardware hack by China underscores the core vulnerability in global supply chains. In a Bloomberg Businessweek article, alarming details were set out about how China infiltrated the supply chain of a supercomputer manufacturer.[5] A tiny microchip was placed into the processing boards of computers that ended up at Apple, Amazon, the U.S. military and even the CIA. The chips purportedly enabled the perpetrators to not only intercept data, but also inject malicious code into the host machines.

The significance of this attack is not only its scale, but the fact that it even occurred. Previously hardware corruption was viewed to be very difficult and unlikely to occur. This new reality, resulting in the "most significant supply chain attack known to have been carried out against American companies," highlights the importance of rethinking basic security assumptions.[5] Vigilance is required not only for the data that is processed, but for the hardware upon which it is processed.

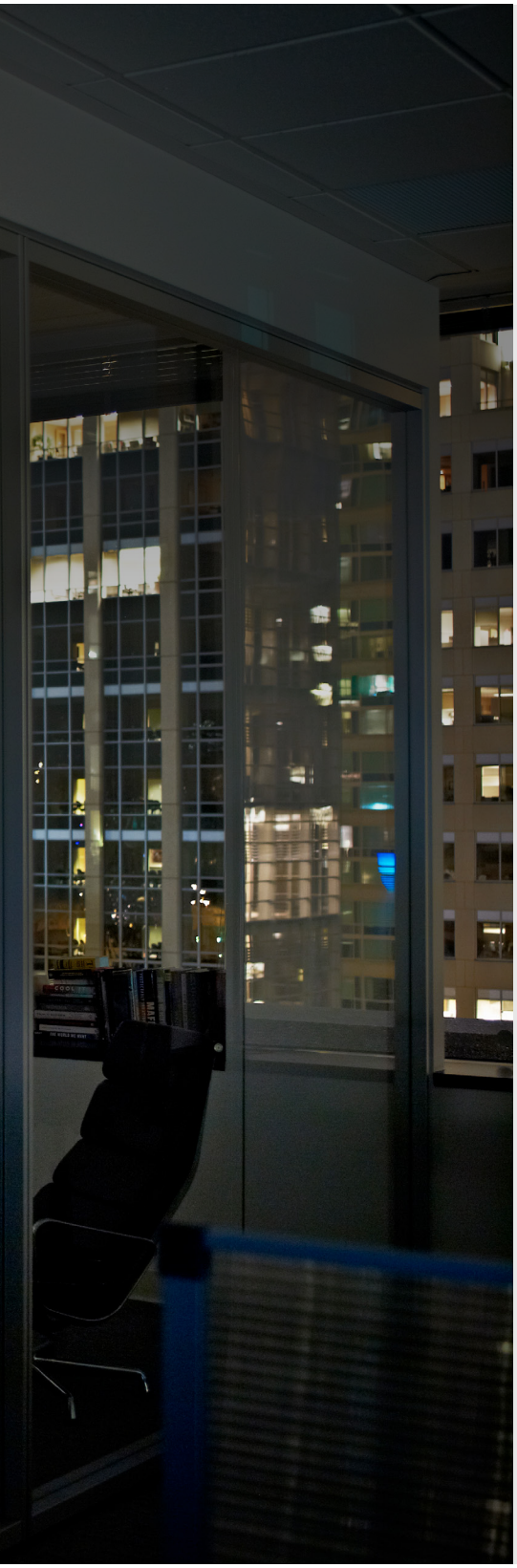
On a less dramatic, but still alarming scale, the BDO Cybersecurity Centre has published observations of increasing frequency and successful cyberattacks on supply chains. Exploiting technology weaknesses in third-party vendors allowed attackers to compromise operating systems and communication protocols for supply chains around the world. The attacks have ranged from seizing control of supply chain systems to facilitating ransom payments to installing backdoor pathways to allow future, undetected access (presumably for malicious intent).

Perhaps most concerning is that recent conventional coding "hacks" have included infiltration of legitimate and widely utilized software programs (e.g., NetSarang connectivity software or the Office 365 productivity suite). Like the hardware corruption example, cyber security cannot be assumed as a given, even if working with a reputable vendor.



FRAUD PART II:

Being proactive – Conducting due diligence and mitigating fraud



While supply chain fraud is an ever-present risk, organizations do not just have to accept it as the cost of doing business. You can take steps to reduce the risk of fraud in your supply chain. Common precautions include:

Regular risk assessments:
Evaluating the potential risks in business operations. Before and while supply chain relationships are operative, consider the probable areas of fraud. Internal controls can only be designed and implemented to address anticipated risks.

Vendor due diligence:
Proactive measures ensure that procurement authorities have the information needed to make an informed and educated decision at the vendor acceptance stage. Before you sign a contract, do you know enough about your potential business partner?

Vendor and third party agent reviews:
Ongoing monitoring via vendor and third party agent (e.g. authorized subcontractor) reviews is a reactive approach to verifying that your partners (including subcontractors, intermediaries, and agents) are following key contract provisions and obligations. Many agreements provide for audit rights — are you exercising your rights diligently?

Employee training and remediation plans:
Conduct regular training and create remediation plans to mitigate the impact of fraud. Are your employees properly trained?

Cyber security — monitoring – detection – response:
Cyberattacks should be viewed as inevitable. Preparing your supply chain for an attack involves ongoing vigilance and having a planned response.

INITIAL AND REGULAR RISK ASSESSMENTS

Do you know your risks

Organizations can protect themselves from supply chain fraud by simply conducting regular risk assessments. Understanding fraud origins and consequences requires intimate familiarity with how your organization conducts business. How are contracting decisions made? Who has approval authority? How are potential suppliers identified and vetted? Once identified, organizations should prioritize the identified risks in terms of probability of occurrence and possible consequences.

This prioritization will likely be influenced by a combination of quantitative (e.g. dollar value of potential losses) and qualitative (e.g. purity of ingredients for a health food producer) measures. It is then the responsibility of management, with corporate governance oversight, to establish tolerable and intolerable risks. Internal controls should be developed to address the latter.

Common risk factors include, but are not limited to:

- Countries in which your company operates: Fraud and corruption are more prevalent in some jurisdictions.[6]
- The industry in which your company operates: Some industries are more susceptible to fraud, such as those predominantly transacting in cash.
- Company culture: Is it one of adherence to rules and procedures or one of "do what it takes to get the job done?" What example does governance and management leadership set?
- Segregation of duties: Is there a concentration of control or authority in employees?
- Quality of information systems: Are management information and accounting systems, including internal controls in those systems, robust or weak?

Thoughtful consideration of risks is crucial in order to develop strong safeguards.

Evaluating your supply chain risk landscape should occur regularly and yearly. Risks in your supply chain will continuously evolve along with the environment in which your business operates. Hence, priorities will also change over time. The allocation of resources, including management attention and corporate resources, should likewise respond accordingly.

Evaluating your supply chain risk landscape should occur regularly, or at least yearly.

VENDOR DUE DILIGENCE

What do you know about your vendors?

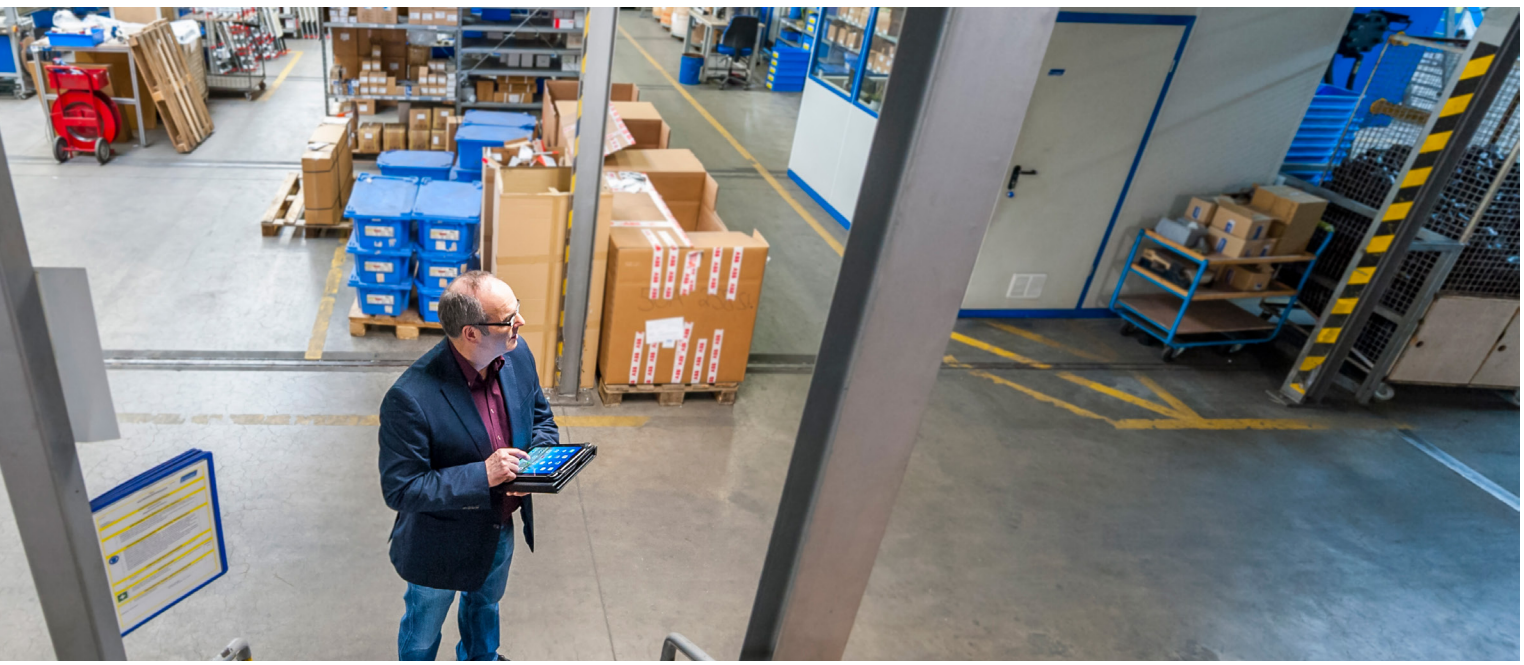
It is important that organizations research potential vendors before agreeing to terms. Due diligence can identify fraud risks while uncovering previous violations, convictions, and other possible issues. Prudential analysis (assessment of fiscal viability) is also a common vendor diligence measure. Financial stability is an important factor in the probability of an individual or organization engaging in fraud.

Conducting vendor due diligence can help your organization:

- Gain valuable insight into vendors' operational practices and culture regarding ethical behavior.
- Mitigate reputational damage and regulatory risk created by business partners.
- Identify risk areas, and where to invest prevention detection resources efficiently and effectively.
- Reduce exposure to fraud.

Thoughtful consideration of risks is crucial in order to develop strong safeguards.

Vendor due diligence may include, among other things, reviewing a vendor's existing and past customer relationships, code of conduct, business practices, online and social media presence, litigation history of vendors, management and other key stakeholders, regulatory filings, key management interviews, onsite visits and so on. As we investigate supply chain fraud, we often discover previous incidents of similar schemes perpetrated by the same individuals. Thus, probing past behaviour, attitudes, and culture (of individuals and of an organization) can be very informative.



VENDOR AND THIRD PARTY AGENT REVIEWS

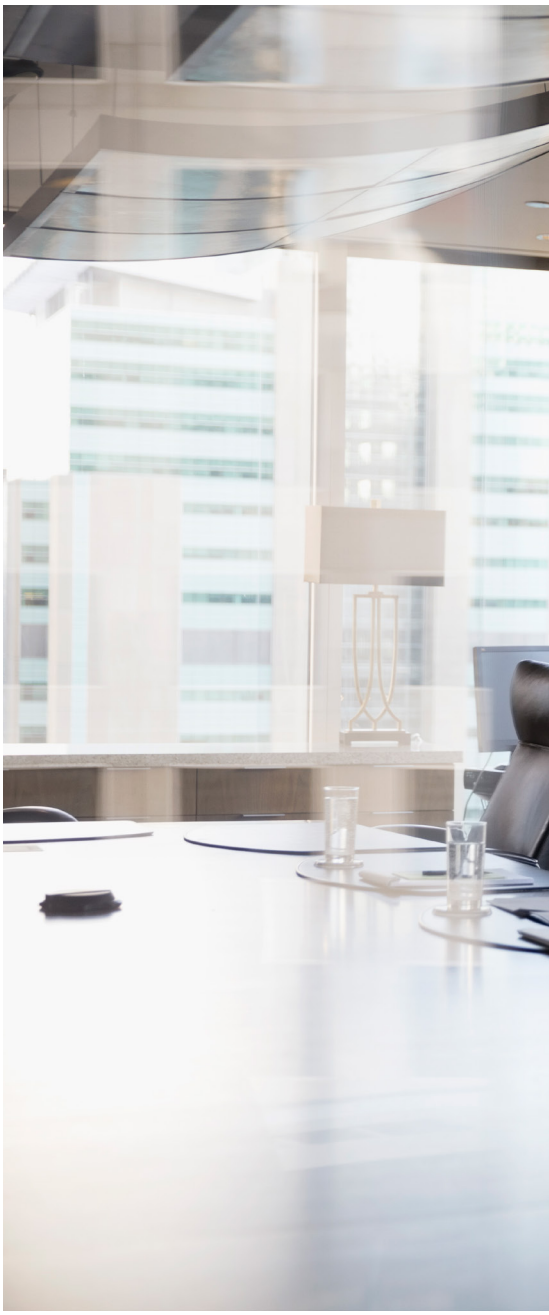
Analyzing contracts and agreements

As supply chains grow more complicated and global in reach, ongoing monitoring of contract compliance is essential. Using external professionals to provide independent, expert, and local oversight can also enhance supply chain integrity. Independent reviews ensure that vendors and any other agents are fulfilling obligations under contract, and not subcontracting work to an unauthorized contractor or dealing inappropriately with regulatory officials to expedite the contracted work.

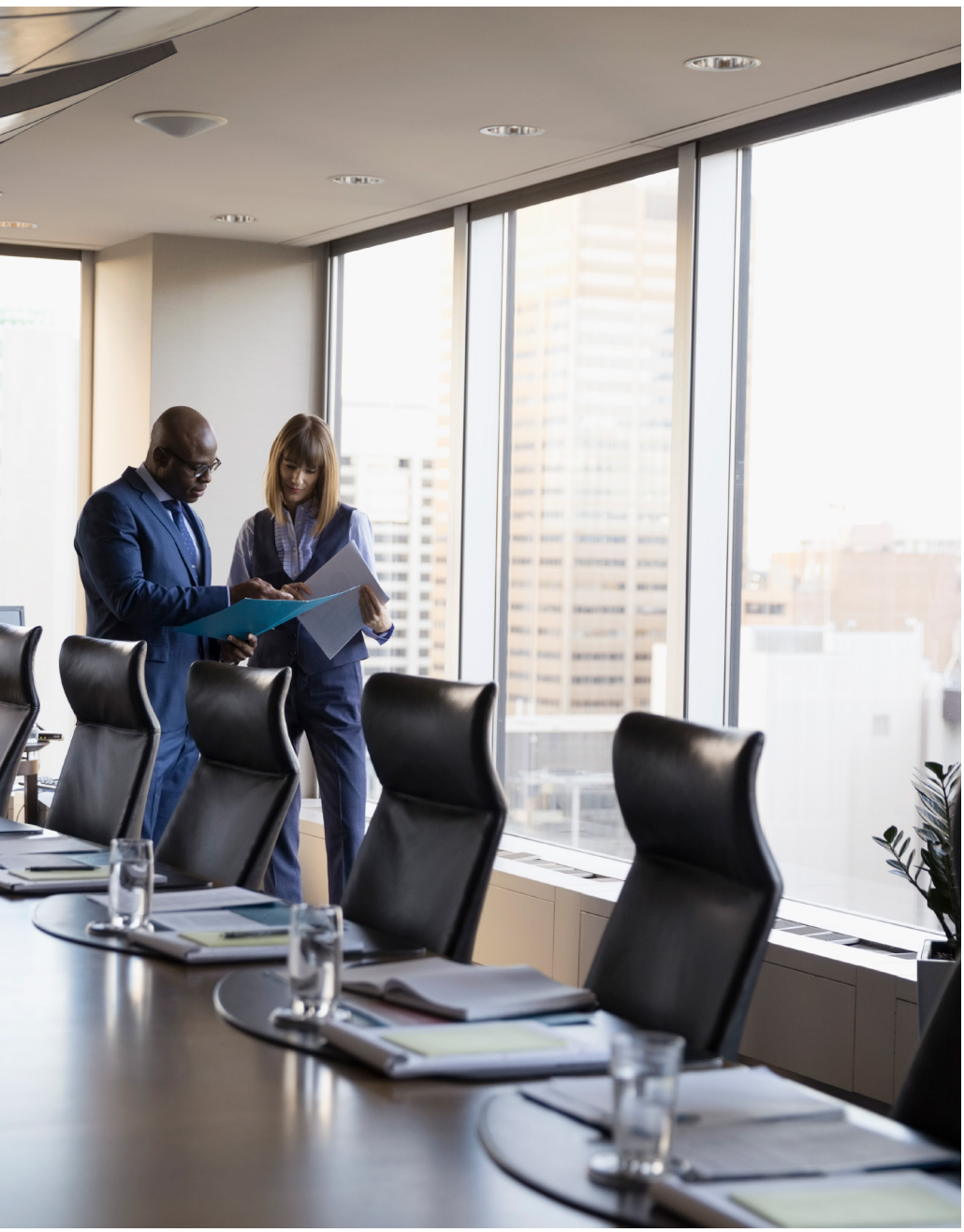
Compliance verification is commonly performed shortly after an agreement is signed with a vendor, but it should be ongoing. Organizations should conduct regular reviews of their vendors and contracts to ensure continuing compliance.

Externally or internally, compliance reviews may include, among other things:

- Verifying key terms such as pricing, costs (including rebates), materials, and timing.
- Testing compliance with FCPA guidelines, contractual ethical guidelines, code of conduct, labour restrictions, and use of subcontractors.
- The reviews may include documentary examination, conducting interviews with management, suppliers (subs), and employees, online/ database review, and site visits. Site visits can be important if vendors operate in jurisdictions with which an organization is unfamiliar. The investigators must be cognizant of different customs, culture and local business practices and see how they compare to the agreed upon behaviour of the vendor.



Compliance verification is commonly performed shortly after an agreement is signed with a vendor, but it should be ongoing.



"Data monitoring/ analysis and surprise audits were correlated with the largest reductions in fraud loss and duration."

Insisting upon an audit clause sends a strong message to vendors that they are serious about respecting agreed upon business conduct, policies, and procedures. The clause should be exercised regularly to reinforce the importance of compliance. The 2018 ACFE Report states, "Data monitoring/ analysis and surprise audits were correlated with the largest reductions in fraud loss and duration." It is a common finding that when controls are enforced, risks of wrongdoing diminish significantly.

EMPLOYEE TRAINING AND REMEDIATION PLANS

Don't forget the human factor

Preventing fraud from happening in the first place is ideal and employee training can help. Organizations should develop guidelines and concepts that help ensure that employees are in compliance and going through the proper channels. You should also have a code of conduct for all employees to follow. A good code of conduct will assist employees in understanding expected policies and expectations such as accepting gifts, under what circumstances an employee can facilitate payment (if at all), and processes for sole-sourcing contracts.[7]

It is critical that you not only state what the employees cannot do, but also provide guidance on the expected behaviour when faced with tough decisions. Specific guidelines and fraud awareness trainings can also go a long way in preventing fraud. "In addition to establishing employee training, we also recommend examining internal controls, policies, and procedures for mitigating fraud risks. According to the ACFE, internal control weaknesses are the culprit for nearly 50% of fraud cases. Furthermore, anti-fraud controls are linked with lower fraud losses and faster detection.[2]

Whistleblowing, a concept that enables an organization to receive hints and tips about fraud from whistleblowers, is also effective. Whistleblowers might fear retaliation, so it is imperative they are able to make reports anonymously where legally permissible. It is also beneficial for certain organizations to establish a tip/ethical hotline, as tips are the most common means of fraud detection. Employees of the victim organizations were responsible for a little more than half of all tips (53%), according to the ACFE.[2] "Fraud losses were 50% smaller at organizations with hotlines than those without."

Top 10 Anti-Fraud Controls

1. Code of Conduct
2. External Audit of Financial Statements
3. Internal Audit Department
4. Management Certificate of Financial Statements
5. External Audit of Internal Controls Over Financial Reporting
6. Management Review
7. Hotline
8. Independent Audit Committee
9. Employee Support Programs
10. Anti-Fraud Policy

Elements of an Effective Whistleblower Program

- Culture of Integrity and Ethics
- Anonymity, Confidentiality, and Financial Support
- No Retaliation
- Educate and Publicize
- Independent (Third-Party) Processing

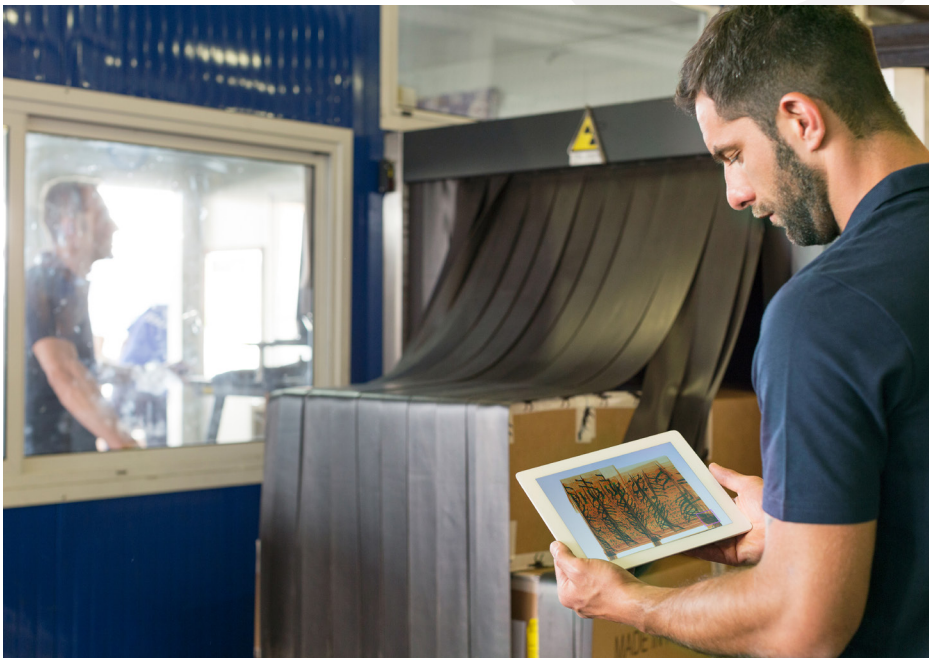
Reporting is more than simply making a hotline available. In order for individuals to feel comfortable coming forward, key elements include a culture of openness, management (and board governance) tone towards unethical or illegal behaviour, and assurances that whistleblowers will not be retaliated against — or perhaps even rewarded. It is also advisable to use confidential hotlines (via phone or internet) tied to an external, independent whistleblower service provider who reports directly to the board or ethics committees. Organizations should also utilize remediation plans, which involves analyzing the root causes of fraud and implementing countermeasures to avoid similar cases in the future. Data monitoring and analysis were associated with the biggest drops in both fraud loss and duration.[2]

▲ Back to contents

CYBER SECURITY FOR SUPPLY CHAINS

Monitoring – Detection – Response

Monitoring and detecting cyber activity is likely already a high priority for your IT team. Triggers such as unusual data traffic and brute force access attempts are flagged immediately to your IT professionals. However, what additional concerns should be addressed by a supply chain professional?



1. **Prioritizing Supply Chain Digital Assets:** Security resources are typically limited. Supply chain professionals can improve the efficiency and effectiveness of cyber security programs by identifying the most valuable digital assets in your supply chain. By prioritizing mission critical data and systems, resources can be allocated accordingly to mitigate risk.

   The cyber risk assessment should include vendors. Over 60% of data breaches occur because of access through third party vendors.[8] Ensuring your cyber security means understanding the cyber security of your business partners.

2. **Quantifying Risks:** Identify the consequences of a cyber-breach on your supply chain and estimate the resultant costs. Aside from understanding the consequences of a cyber-breach, quantifying costs will allow you to make an informed decision about insurance coverage. Does your organization have cyber liability insurance and is the coverage adequate?

3. **Response Plan:** Does your organization have formal incident response, disaster recovery and business continuity plans? Do you have a policy on whether and how to respond to ransomware events? Having developed plans will allow your organization to react swiftly and effectively in the event of a breach.

OVER **60%** of data breaches occur because of access through third party vendors.

CONCLUSION

Where do we go from here?

Organizations will continue to be susceptible to supply chain fraud due to the vast complexity involved in today's supply chains. Technology, cross border aspects, weak internal controls and especially collusion contribute to fraud risks. The best-case scenario is to avoid supply chain fraud in the first place, but it is not always possible. However, staying aware and providing training on the most common schemes can help keep organizations from becoming victims. Taking action and being proactive can protect your organization, making you less likely to face the harsh consequences of fraud.

Your organization can and should address these issues to better position themselves in the marketplace. Vendor due diligence, compliance reviews, regular risk assessments, and employee training and remediation plans are the chief measures to combating fraud. Creating and executing a well-planned internal control strategy and framework can help position your organization for supply chain success, while maintaining your reputation, investment, and productivity.

Creating and executing a well-planned internal control strategy and framework can help position your organization for supply chain success

REFERENCES

1 No more excuses — Responsible supply chains in a globalised world (2017)

2 Report to the Nations — 2018 Global Study on Occupational Fraud and Abuse (2018)

3 Detecting Bid Rigging in Public Procurement (2009)

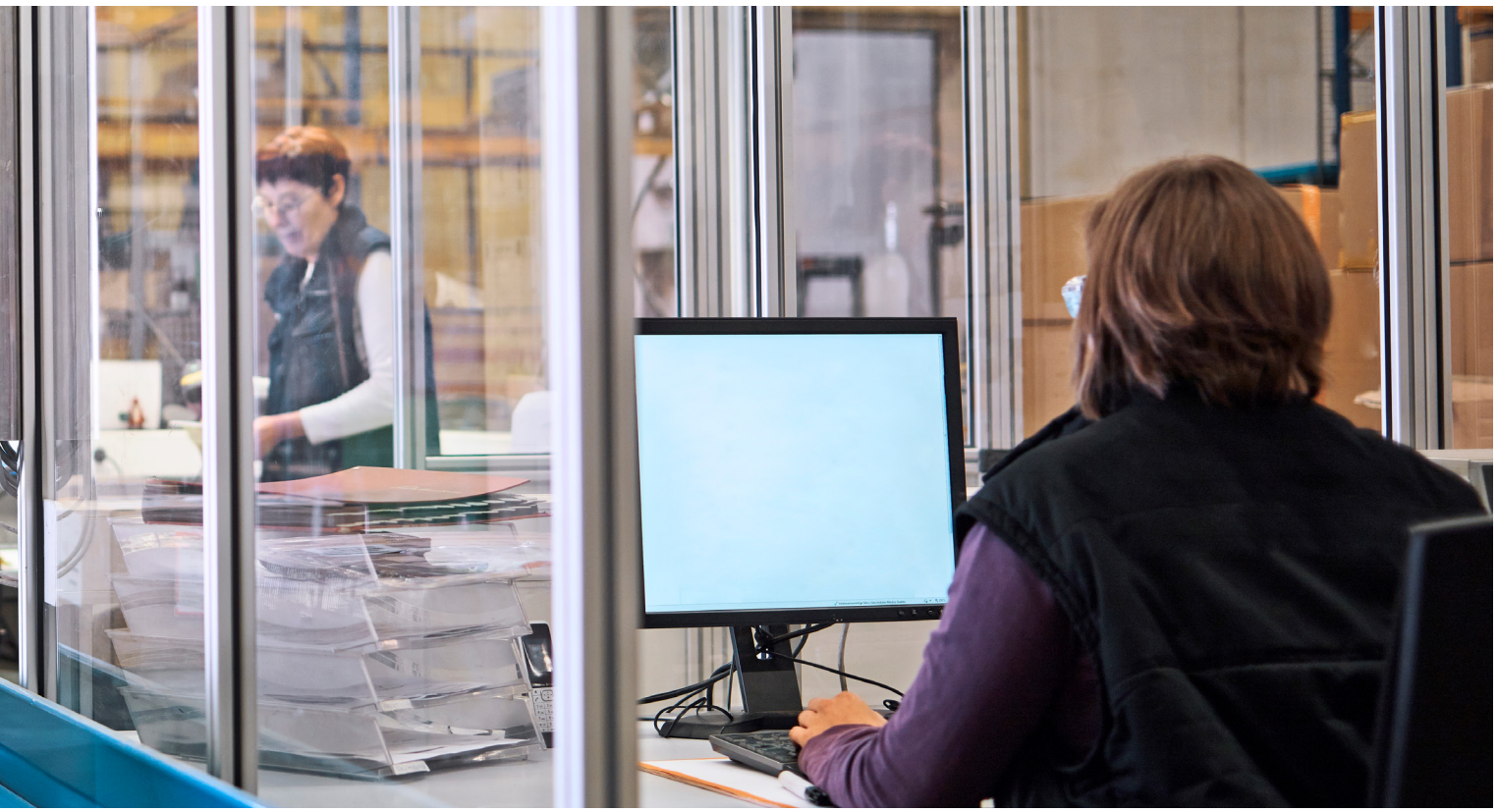
4 Addressing the Sale of Counterfeits on the Internet (2017)

5 The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies (October 4, 2018)

6 Corruption Perceptions Index (February 2018)

7 SCMA Code of Ethics for Professionals in the field of Supply Chain Management (2016)

8 BDO Global, 10 things CFOs should do immediately about cyber security (September 2018)



FOR MORE INFORMATION:

ALAN MAK
Partner, National Forensics Practice Leader
416-914-6387
amak@bdo.ca

CHETAN SEHGAL
Partner, Forensics & Litigation Support
416-775-7812
csehgal@bdo.ca

ANNE-MARIE BÉLANGER
Partner, Forensic & Litigation Support
514-931-2483
abelanger@bdo.ca

BOB FERGUSON
Partner, Forensic & Litigation Support
416-369-4764
bferguson@bdo.ca

ROSANNE WALTERS
Partner, Forensics & Litigation Support
604-363-5307
rwalters@bdo.ca

ABOUT BDO

BDO is a leading provider of professional services to clients of all sizes in virtually all business sectors. Our team delivers a comprehensive range of assurance, accounting, tax, and advisory services, complemented by a deep industry knowledge gained from nearly 100 years working within local communities. As part of the international BDO network, we're able to provide seamless and consistent cross-border services to clients with global needs.

Assurance | Accounting | Tax | Advisory
www.bdo.ca

FOR MORE INFORMATION:

Toronto: 416-977-7111
Toll Free: 1-888-799-0877

SCMA.com
SCMA.com/linkedin
twitter.com/scmanational
facebook.com/scmanational

ABOUT SCMA

The Supply Chain Management Association™ (SCMA™) is the voice of Canada's supply chain, representing and serving more than 6,000 professionals across the country, as well as the wider supply chain community. SCMA is a federation, with a national secretariat and 10 provincial/territorial Institutes. Its mission is to "provide leadership to the Canadian supply chain community, provide value to all members, and advance the profession." Through its education, advocacy and resource-development initiatives, the association endeavours to advance its vision, to see that "Canadian supply chain professionals and organizations are recognized for leading innovation, global competitiveness and driving economic growth." Its Supply Chain Management Professional (SCMP) designation is Canada's most-sought-after professional designation for those entering the field and advancing as leaders in supply chain.