Pulling fraud out of the shadows

Luxembourg in context of the Global Economic Crime and Fraud Survey 2018

pwc

www.pwc.com/fraudsurvey

Executive Summary

Michael Weis
Partner, Forensic Services and Financial Crime Leader, PwC Luxembourg

In PwC's 2018 Global Economic Crime and Fraud Survey, "only" 49% of global organisations said they'd been a victim of fraud and economic crime. However, we know this number should be much higher. So, what about the other 51%?

The reality is, too few companies are fully aware of the fraud risks they face. That's why this year's Global Economic Crime and Fraud Survey, gathering valuable data from more than 7,200 respondents across 123 different territories, aims to pull fraud out from the shadows – and shed much-needed light on some of the most important strategic challenges confronting every organisation. In Luxembourg we had 72 participants, mostly coming from the Financial Sector for obvious reasons.

Dominant on the business agenda

Economic crime continues to be a dominant item on the business agenda, and no industry sector, region or size of business is immune.

Fighting fraud has progressed from being an operational or legal matter to a central business issue. Fraud, today, is tech-enabled, innovative, opportunistic and pervasive.

Technology has advanced in leaps and bounds, fraudsters are more strategic and sophisticated in their approach. Meanwhile, regulatory regimes are far more robust — with enforcement intensifying around much of the world, often with cross-border cooperation.

Companies, at risk of their reputations, are under unparalleled public and regulatory scrutiny to account for any suggestion of internal or externally motivated fraud.

Luxembourg's focus on AML and Tax

In this publication, we provide data and analysis of Luxembourgish respondents to help you assess the risks to which your business is exposed relative to the global context.

In Luxembourg, as a major financial centre, the majority of our respondents are subject to Anti-Money Laundering/Combating the Financing of Terrorism (AML/CTF) regulations at both the local and international levels. This explains why AML and the related tax topics score very high as a main topic of concern in Luxembourg.

Next

Should you require further details or explanations, our Luxembourg financial crime team is ready to support you. We have forensic investigators, accounting professionals, computer forensic specialists and regulatory experts who can help you to understand your business risks. Whether you are working to prevent fraud, assess the impact or understand exactly what has happened, our team of local experts can draw upon global experience to provide direct insight.

We would be pleased to review the results of the survey with you personally, and discuss how they relate to your organisation or industry.

Four steps to fight fraud

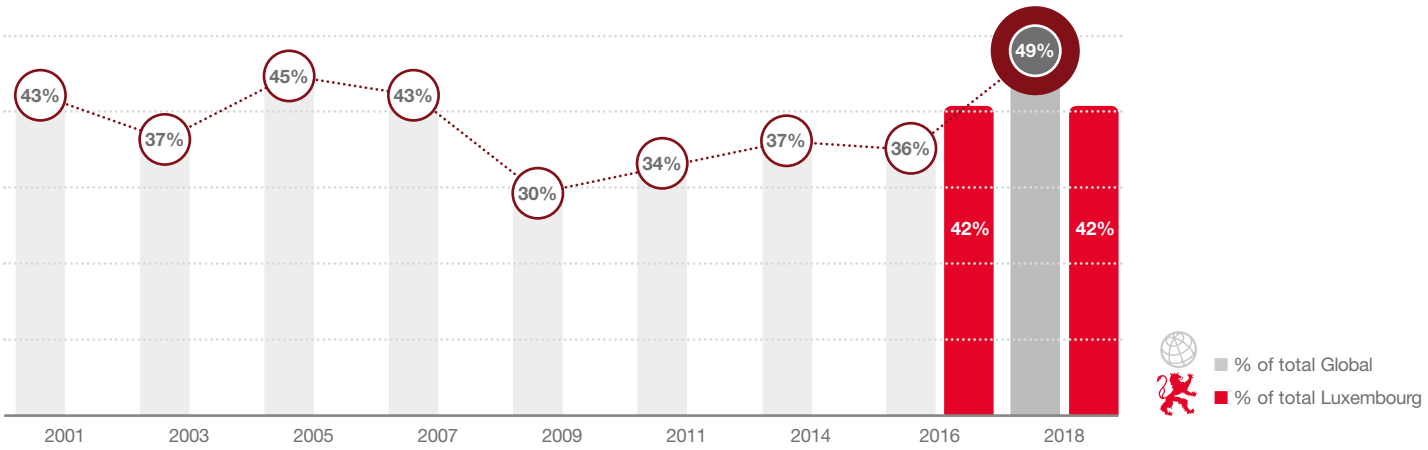
Recognise fraud when you see it

Is fraud really on the rise – or just our awareness of it?

This year, 49% of respondents to our Global Economic Crime and Fraud Survey said their companies had been victims of fraud or economic crime, up from 36% in 2016. Whereas 42 % of Luxembourg organisations have experienced economic crime in the past 24 months, the same level as 2016. Luxembourg remains stable, but high. The rise globally can be explained by a combination of growing global awareness of fraud, a larger number of survey responses, and greater clarity about what "fraud" actually means. But every organisation – no matter how vigilant – is vulnerable to blind spots. And because those blind spots usually only become apparent with hindsight, throwing light onto them as early as possible can vastly enhance fraud-fighting efforts.

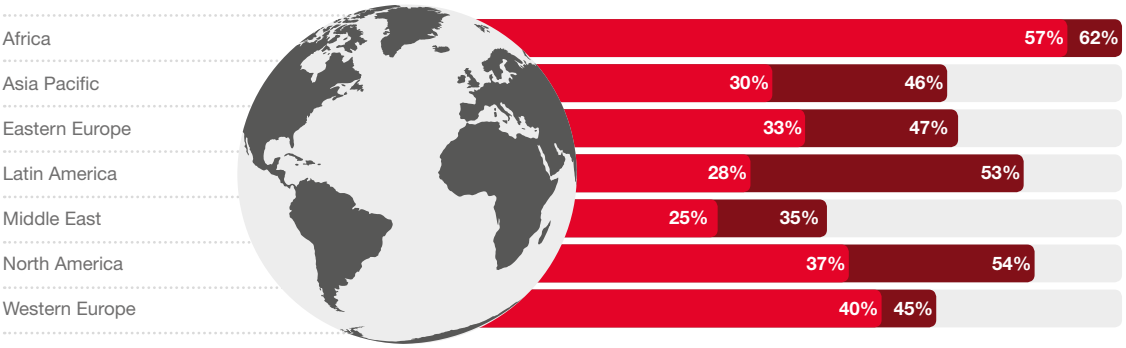
Companies today face a perfect storm of fraud risk – internal, external, regulatory and reputational

Exhibit 1: The reported rate of economic crime is on the rise



Q. Has your organisation experienced any fraud and/or economic crime within the last 24 months?
Source: PwC's 2018 Global Economic Crime and Fraud Survey

Exhibit 2: The reported rate of economic crime has increased across all territories



Q. Has your organisation experienced any fraud and/or economic crime within the last 24 months?
Source: PwC's 2018 Global Economic Crime and Fraud Survey

Just as the reported rate of economic crime has increased since 2016, so has the amount that companies are spending to fight it:

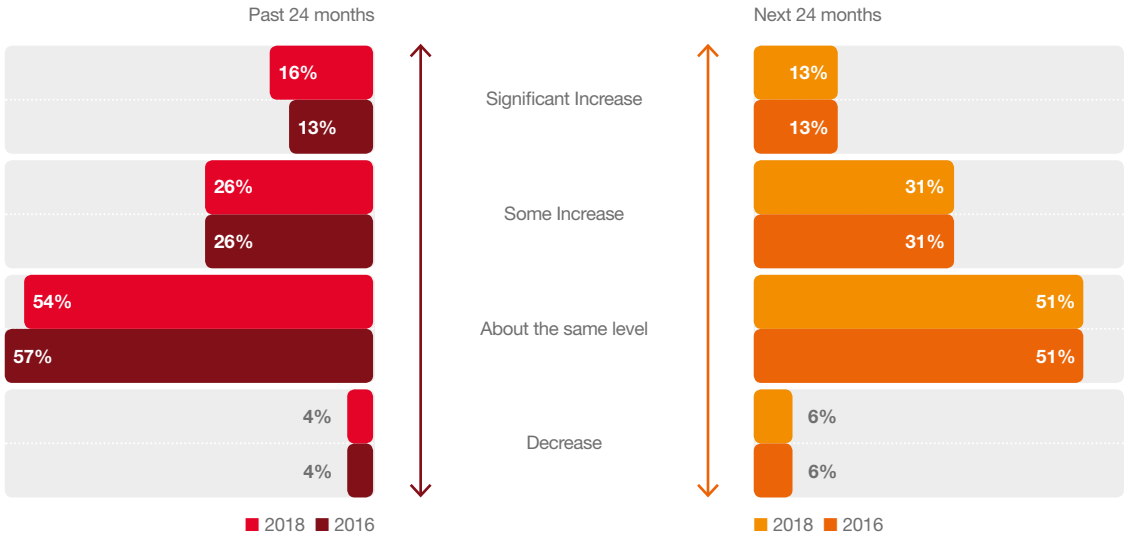
- 42% of respondents said their companies had increased spending on combatting fraud and economic crime over the past two years (up from 39% in 2016).
- 44% of respondents said they plan to boost spending over the next two years.

Where is this money being spent? Organisations are using ever-more powerful technology and data analytics tools to fight fraud. And, in addition to these technology-based controls, many are also expanding whistle-blower programmes and taking steps to keep leadership in the loop.

But do these measures represent a genuine shift to more proactive approaches to fraud and corruption? Or are they just a rear-guard action, driven principally by enhanced anti-bribery/anti-corruption legislation and increasingly globalised forms of enforcement? In other words, are we still missing something vital in the fight against fraud?

Our survey results strongly suggest we are. Our Luxembourg experience would even rather confirm underspending on combatting fraud compared to global trends.

Exhibit 3: Organisations continue to increase spending on combatting fraud



Q. How has/is your organisation adjusting the amount of funds used to combat fraud and/or economic crime?"

Source: PwC's 2018 Global Economic Crime and Fraud Survey

59%

of CEOs agree or strongly agree that organisations are currently experiencing increased pressure to hold individual leaders accountable for any organisational misconduct

Source: PwC's 21st CEO Survey

71%

of CEOs measure trust between their workforce and their organisation's senior leadership

Source: PwC's 21st CEO Survey

Fraud risk assessments are the first step in preventing fraud before it takes root

Despite the increase in spending, many organisations are still addressing fraud prevention by using a reactive, defensive approach:

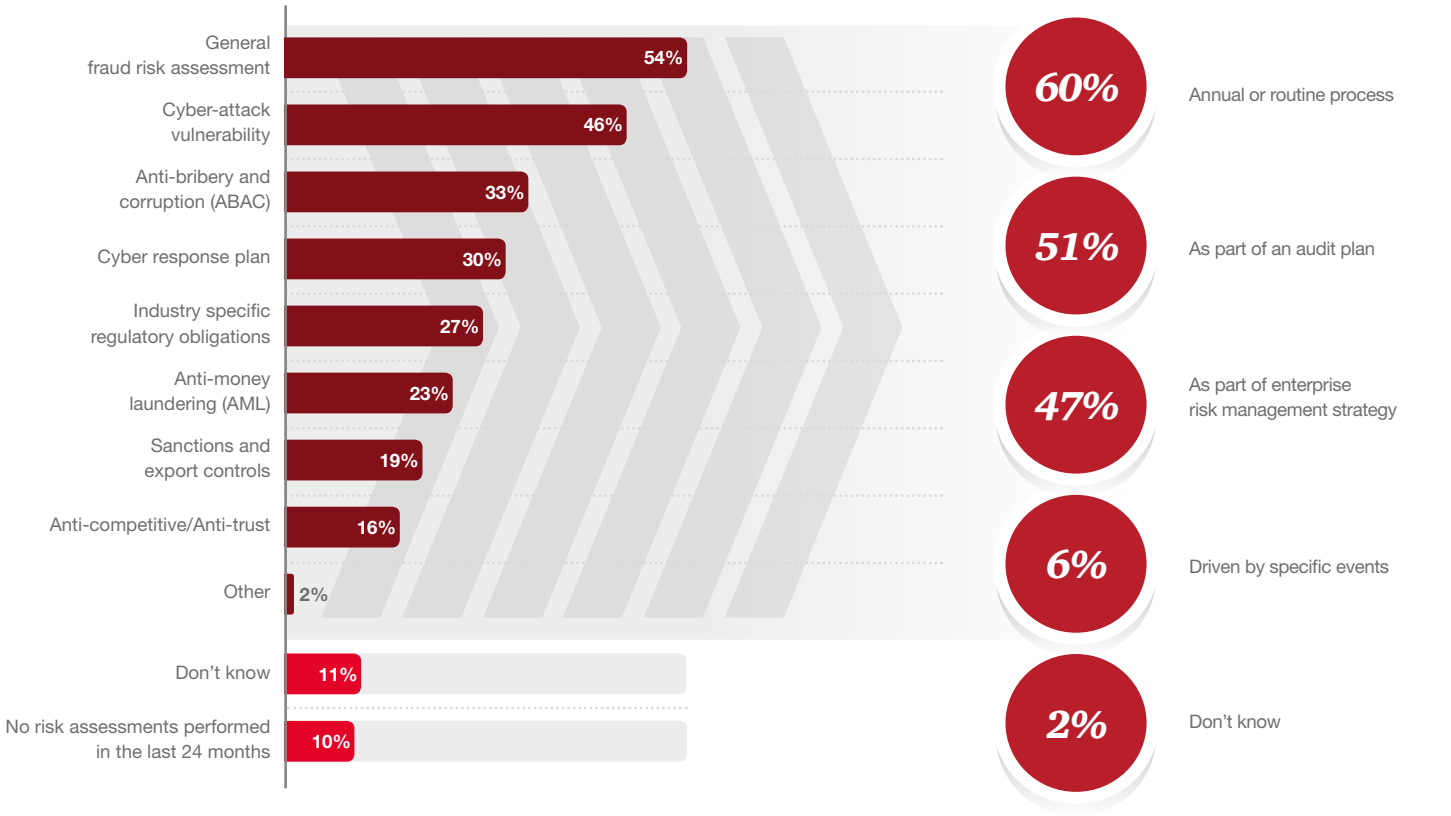
- **Only 54% of global organisations said they have conducted a general fraud or economic crime risk assessment in the past 2 years.**
- Less than half said they had conducted a cybercrime risk assessment.
- Fewer than a third said their company performed risk assessments in the critical areas of anti-bribery and corruption, Anti-money laundering, or sanctions and export controls.
- **One in ten respondents had not performed any risk assessments at all in the past 2 years.**

However, the rules of the game are changing profoundly and irreversibly. Public tolerance for corporate and/or personal misbehaviour is vanishing. Not only is sensitivity to corporate misconduct at an all-time high, some corporations and leaders are also now being held to account for past behaviour, conducted when the "unspoken rules" of doing business might have been thought to be different. PwC's 21st CEO Survey underscores this theme: in it, chief executives cite trust and leadership accountability as two of the most significant threats to business growth.

This points to a heightened risk when fraud or economic crime spills into public view – and a greater need for organisations to take a lead in preventing fraud before it can take root. Fraud risk assessments can help organisations do so by identifying the specific frauds they need to look for. Moreover, these assessments are increasingly looked on favourably by regulators in enforcement actions.

In Luxembourg this is even less explicit than what we see globally, since traditionally, the focus in Luxembourg is around AML rules. Broader types of risk assessment are less common still.

Exhibit 4: Less than half of all organisations have performed targeted risk assessments in the last 2 years



Q. In the last 24 months, has your organisation performed a risk assessment on any of the following areas?

Source: PwC's 2018 Global Economic Crime and Fraud Survey

Q. What prompted your organisation to perform a risk assessment?

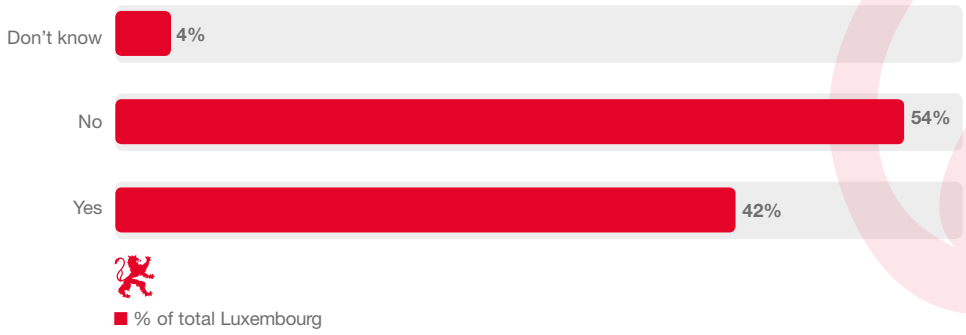
Source: PwC's 2018 Global Economic Crime and Fraud Survey

The experience of economic crime

Today, as in our 2016 report, 42% of Luxembourg organisations report having experienced economic crime in the past 24 months; the percentage remains stable, but high. The stable rate is probably due to a continued focus on money laundering and cybercrime prevention policies implemented by most companies. However, Luxembourg, with its large Financial Sector, remains a prime target for criminals. The continued efforts of regulators, law enforcement and businesses increased measures are at best managing to keep things stable. Based on our experience and knowledge of financial crime incidents in the past 24 month, there is a trend of increasing cases of misconduct, coupled with a lack of awareness, resulting in under-reporting of incidents.

Luxembourg has dedicated and (not always though) sophisticated detection measures and tools for the core money laundering field, but needs to extend these into other potential areas of fraud and misconduct.

Exhibit 5: Occurrence of economic crime in past 24 month



Q. Has your organisation experienced any economic crime in your country within the last 24 months?
Source: PwC's 2018 Global Economic Crime and Fraud Survey

The Global results have shown some **"new frauds"** – the ones whose prominence has grown up so much that we have measured them as separated threats for the first time. These include fraud committed by the consumer (29%) and business misconduct (28%) at 3rd and 4th place, respectively, among all reported frauds.

We believe that the inclusion of these two categories is partially responsible for the decrease (from 64% in 2016 to 45% in 2018) in the larger category of asset misappropriation.

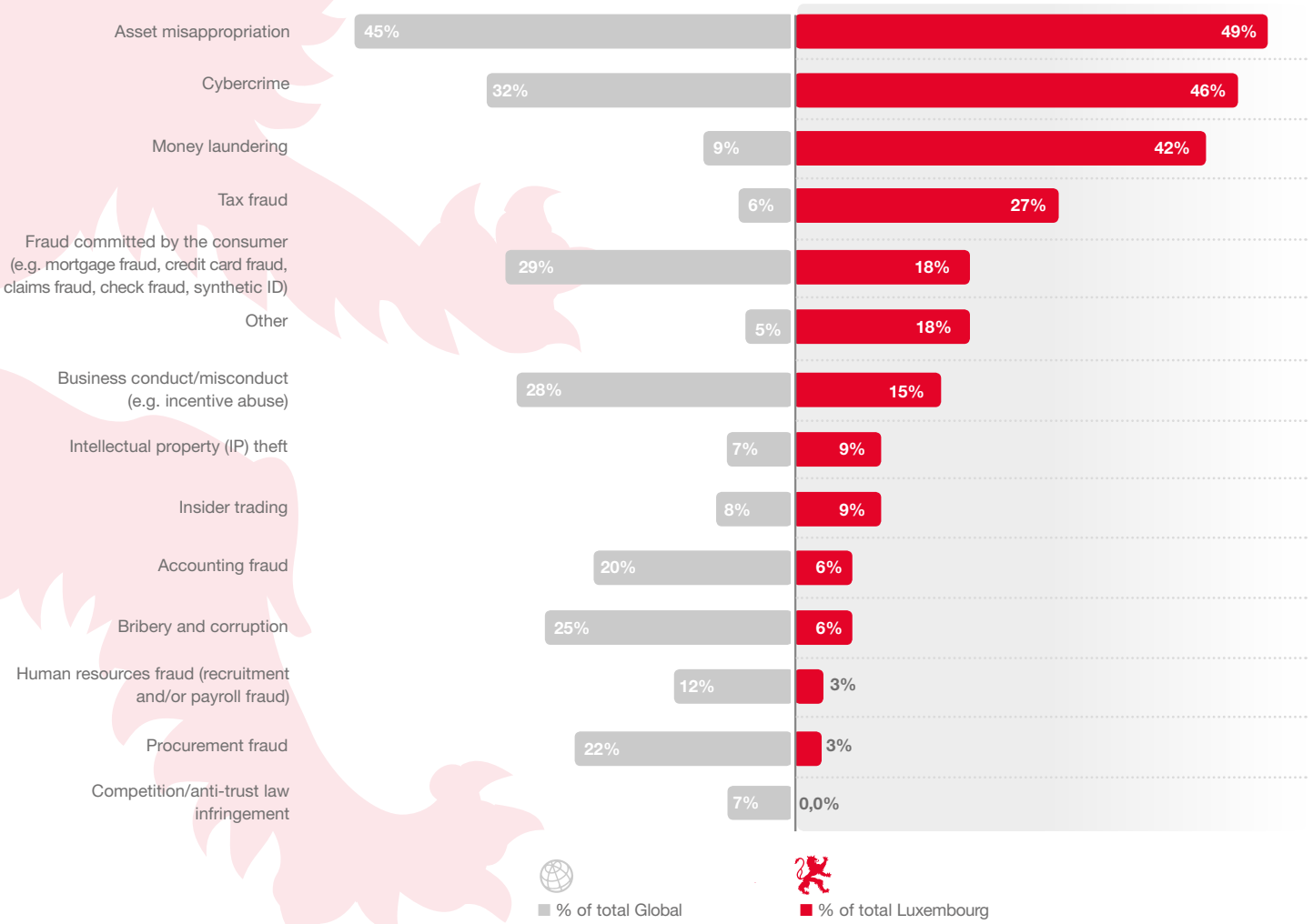
Being a major financial centre, tax issues are an important topic in Luxembourg since end of 2016 and not the least with the adoption of the 4th EU AML Directive making tax fraud a predicate offence for money laundering.

Most commonly reported types of economic crime

The most pervasive economic crimes reported by global respondents for 2018 are highlighted in the figure below, with Asset misappropriation being top followed by Cybercrime and the "new kids on the block" Consumer Fraud and Business Misconduct.

When looking at the Luxembourg double-digit scorers Asset Misappropriation remains top with Cybercrime as a close second. Third is money laundering; understandable given Luxembourg's Financial Centre status. However, the "new kid on the block" for Luxembourg is Tax Fraud coming in 4th, at 5 times above the global average!

Exhibit 6: Most commonly reported types of economic crime



Q. What type of fraud and/or economic crime has your organisation experienced in your country within the last 24 months?

Source: PwC's 2018 Global Economic Crime and Fraud Survey

Following the Tax Reform Law of 23 December 2016, in line with 4th AML Directive (AML4D), Luxembourg (CSSF Circular 17/650) has strengthened measures to fight tax fraud, institutionalising and formalising the regulatory focus.

Tax fraud is viewed as a predicate offence that underlies money laundering activity. Hence, internal policies, procedures and measures in Luxembourg organisations had to be updated to include primary tax offences (risk assessment, documentation of client files, monitoring of transactions, etc.). Additionally, based on an EU directive, Luxembourg now applies the Common Reporting Standard. For the 2016 tax year, Luxembourg financial institutions had to provide information to the tax authorities beginning on 30 June 2017.

These major improvements, reinforcing the fight against tax fraud, explains why tax fraud has emerged in fourth position in the type of economic crime that Luxembourg organisations have, and expect to experience.

Statistics, related to money laundering and suspicious activity reporting (SAR), from the public prosecutor's Financial Intelligence Unit (FIU) show an increase and corroborate the findings of this survey.

Cybercrime remains the second largest type of economic crime reported by Luxembourg companies in 2018 and is reportedly the most impactful and disruptive for their organisations. Cybercrime, in addition to being disruptive is also seen as a vehicle for fraud that often results in asset misappropriation dirctly or indirectly.

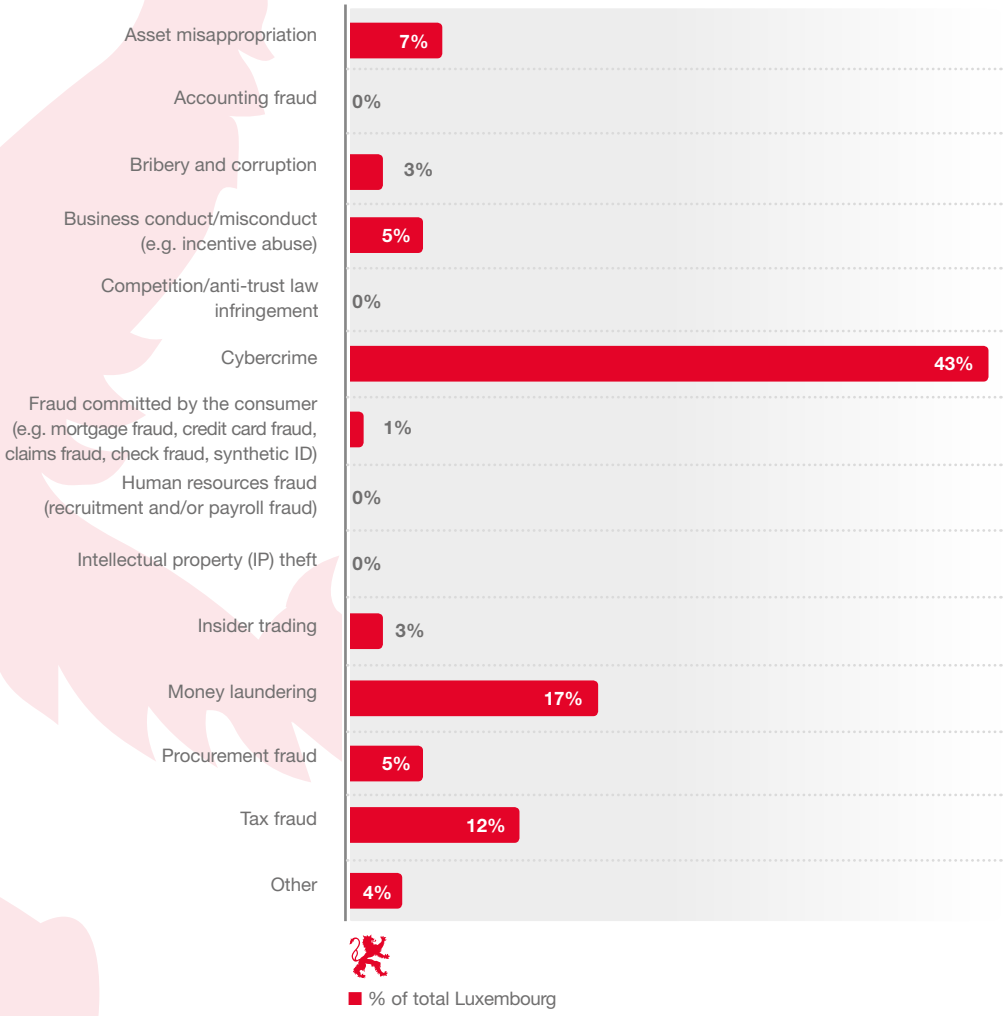
It is interesting to note that classical crimes like **bribery and corruption**, compared globally, score very low in Luxembourg. Luxembourg is less subject to bribery and/or corruption because of the nature of its industry. However, bribery and corruption remain an important global topic, as confirmed by the latest Transparency International CPI report, due to the continued pressure from ever increasing international anti-corruption laws like the UK Bribery Act, that has started getting traction with deferred prosecution agreements, and other related laws in the US, and Sapin II in France.

The unprecedented leak of 11.5m files (the "Panama Papers") from the database of the world's fourth biggest offshore law firm in 2016/17 affected Luxembourg and many other large financial centres. Companies had to respond to CSSF requests, special audits were instituted by regulators locally and globally, and some banks needed to account for tax related situations in addition to paying regulatory fines for AML breaches. The topic remains a continued challenge as related stories like the recent "Paradise Papers" have highlighted.

Asset misappropriation

is the **most common form of economic crime** experienced by organisations in 2018 followed by cybercrime and money laundering. This is not surprising for a sector processing money and given the low cost of conversion for fraudsters.

Exhibit 7: Economic crime most likely to be disruptive in the next 24 months



Q. Thinking about the next 24 months, which of the following fraud and/or economic crimes is likely to be the most disruptive/serious in terms of the impact on your organisation (monetary or otherwise)?

Source: PwC's 2018 Global Economic Crime and Fraud Survey

Reported likelihood of economic crimes in the next 24 months

From a Luxembourg perspective, cybercrime and money laundering are a major concern. 43% of Luxembourgish companies expect cybercrime to be the most disruptive to their organisation in the next 24 months, followed by money laundering and tax fraud. Anti-money laundering, augmented by a very strong regulatory framework, receives significant attention locally, and is considered to be "under control".

In the preceding 24 months, 1 out of 2 Luxembourgish companies were targeted by a phishing attack or a malware infection. Clearly, organisations need to increase their efforts for employee security awareness and training.

Humans are the first vector of cyber-attack and ideal prey for malicious individuals who want to compromise an organisation. Luxembourg, with its high concentration of financial institutions and data centres, was a more frequent subject of attacks of these types of than the rest of the world

Classical crimes like bribery and corruption get very low scores in Luxembourg relative to the global results (3% in Luxembourg whereas 12% in global). However, bribery and corruption qualify as primary offences for money laundering and could, indirectly, be very relevant with higher statisitics than reported. What most financial institutions underestimate is their risk exposure to corruption payments being channeled through their accounts. Those are not easy to spot, but highly toxic for financial institutions as they immediately create the money laundering offence. Reputable clients could quickly turn out to be bribe payers, or recipients, as recent international scandals confirmed.

As a large financial centre Luxembourg certainly bears the risk of being abused for such transactions and this risk seems to be underestimated still. Given the prevalence of asset misappropriation, it is perhaps surprising that only 7% of Luxembourg respondents expect this to be an issue in the next 24 months. Conversely, significantly higher proportions of Luxembourg companies expect to be the victim of cybercrime (43%) and money laundering (17%).

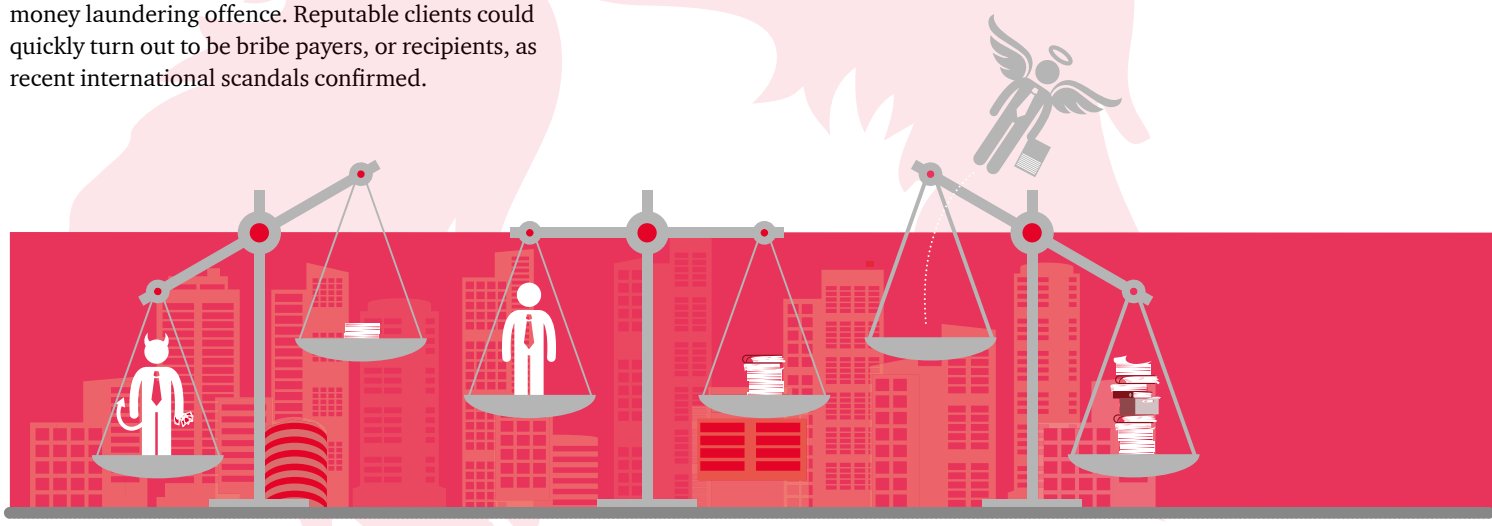
Asset misappropriation is usually the easiest type of fraud to detect. However, in Luxembourg, it ranks below cybercrime, money laundering and tax fraud as a future concern. Luxembourg-based organisations would be well advised not to underestimate asset misappropriation and to review their controls in this area and remind their staff that, although the risks linked to cybercrime and money laundering are high, they are just as likely to fall victim to more conventional frauds.

1 out of 2

Luxembourgish companies were targeted by a phishing attack or a malware infection.

43%

of Luxembourgish companies expect cybercrime to be the most disruptive to their organisation in the next 24 months, followed by money laundering and tax fraud.



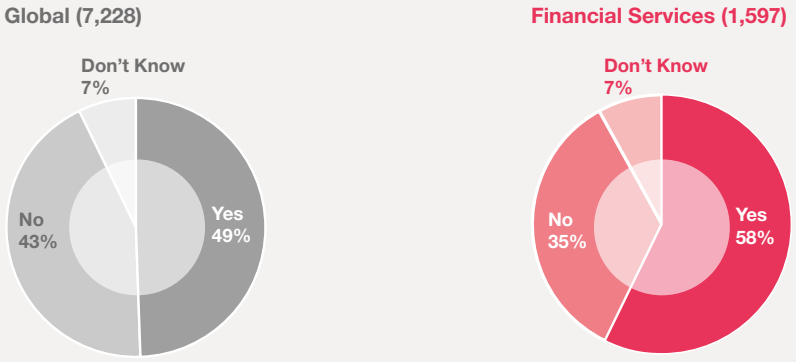
An FS perspective

Fraud and Economic Crime trends

With 58% of organisations having experienced fraud and/or economic crime within the last 24 months, FS is among the top 3 of exposed industries, while the Insurance sector in particular is #1 with 62%.

Fraud and economic crime experienced

Has your organisation experienced any fraud and/or economic crime in your country within the last 24 months?



Monitoring and preventing fraud

FS is far more focused on performing risk assessments than other sectors, not the least due to the high exposure to financial crime.

Risk assessments performed

In the last 24 months, has your organisation performed a risk assessment on any of the following areas?

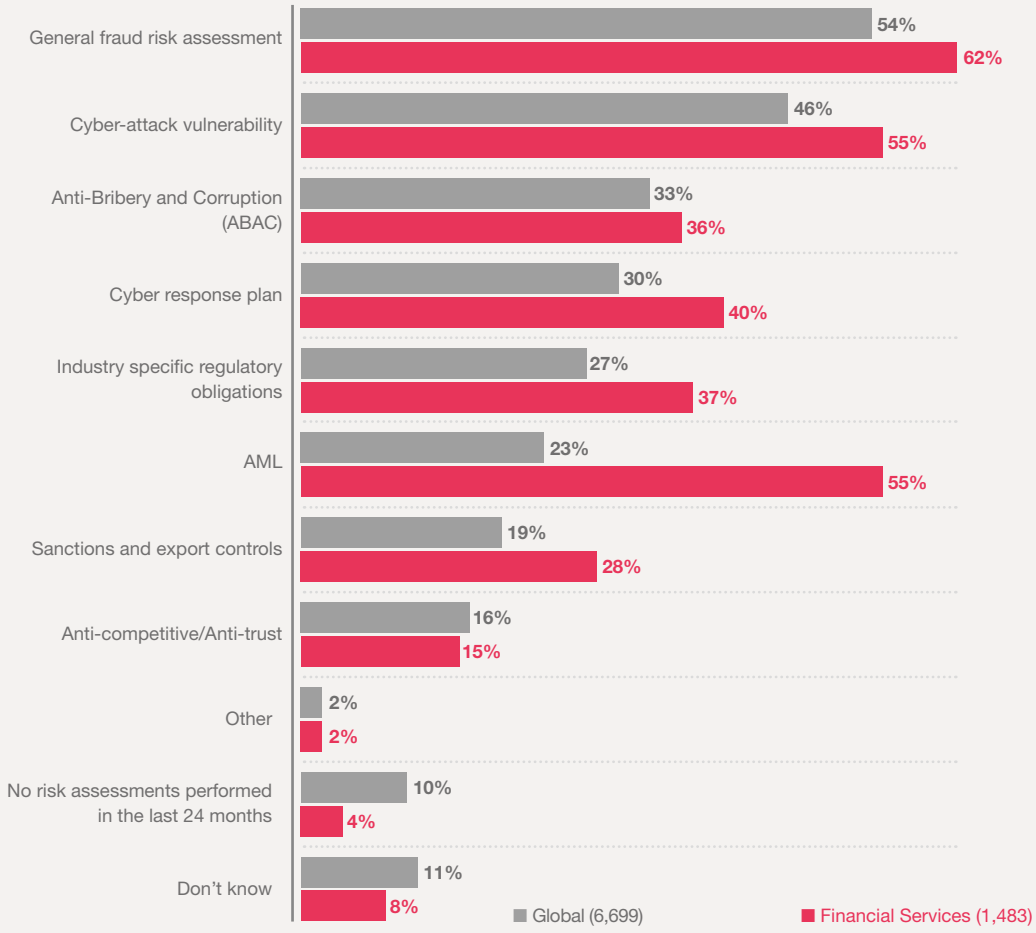
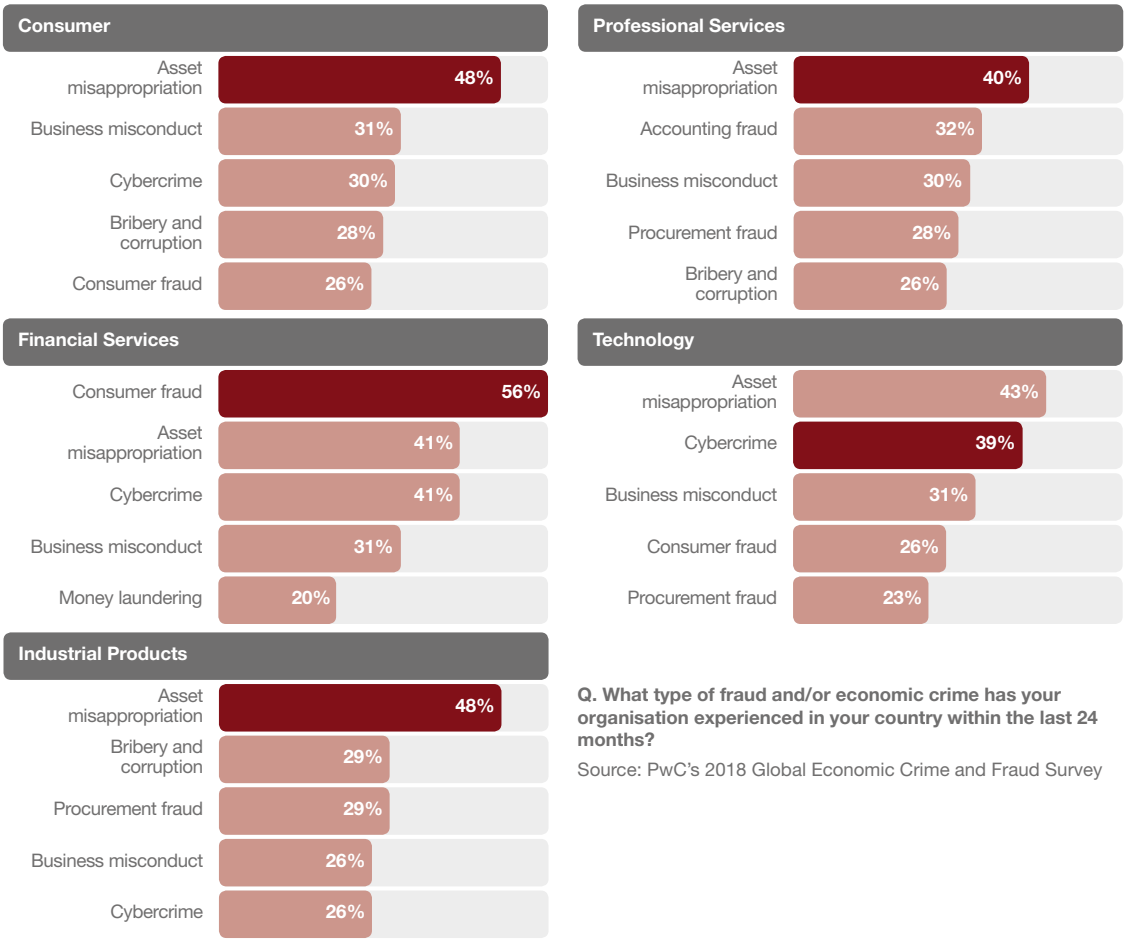


Exhibit 8: Asset misappropriation, consumer fraud and cybercrime were the most frequently reported frauds across industries



Q. What type of fraud and/or economic crime has your organisation experienced in your country within the last 24 months?

Source: PwC's 2018 Global Economic Crime and Fraud Survey

Conduct risk: the "hidden risk" behind many internal frauds

Two types of fraud – consumer fraud and business misconduct – have grown in prominence to such an extent that this year's survey is measuring them as separate threats for the first time. Of the respondents who indicated their companies had experienced fraud in the last two years, 29% said they had suffered from consumer fraud and 28% said they had suffered from business misconduct (making these, respectively, the 3rd and 4th most frequently reported frauds this year, behind asset misappropriation at 45% and cybercrime at 31%). It should be noted that the significant decrease in reported incidents of asset misappropriation (down from 64% in 2016) is at least partly explained by the inclusion of these new frauds in the survey.

These methodological changes reflect the growing recognition of a broad category of internal fraud risk: "conduct risk". This is the risk that employee actions will imperil the delivery of fair customer outcomes or market integrity. And, unlike operational breakdowns or external threats (which can often be checked by internal controls), conduct risk requires a more holistic response – and a shift in attitude. Several large investigation cases we worked on recently in Luxembourg fell exactly in this category, which is a real issue for the relevant organisation, as detection and prevention are more complex, but the impact can be really severe.

At present, many companies treat compliance, ethics and enterprise risk management as separate functions – sometimes they even exist in separate siloes within an organisation. But, like all organisational silos, this means these functions rarely add up to a strategic whole. The parts of an organisation that investigate fraud, the parts that manage the risk of fraud, and the parts that report fraud to the board or regulators become disjointed.

From the Luxembourg perspective those distinctions make sense, especially since the conduct aspect is more apparent with significant negative impact, even though it may not result in any direct personal profit to the actor.

When that happens, operational gaps can emerge and fraud can too easily be brushed under the carpet or seen as someone else's problem – to the detriment of the overall effectiveness of fraud prevention, financial performance and regulatory outcomes.

A more innovative approach is to reframe these functions as components of conduct risk. It enables a company to better measure and manage compliance, ethics and risk management horizontally and embed them in its strategic decision-making process. It also means fraud and ethical breaches can be approached more dispassionately, with less emotion, as a fact of life that every organisation has to deal with. Moreover, adopting this more systemic – and realistic – stance towards conduct risk can enable cost efficiencies between ethics, fraud and anti-corruption compliance programmes. It is an important step in breaking down the silos between key anti-fraud functions – and pulling fraud out of the shadows.

Looking for fraud in the right places

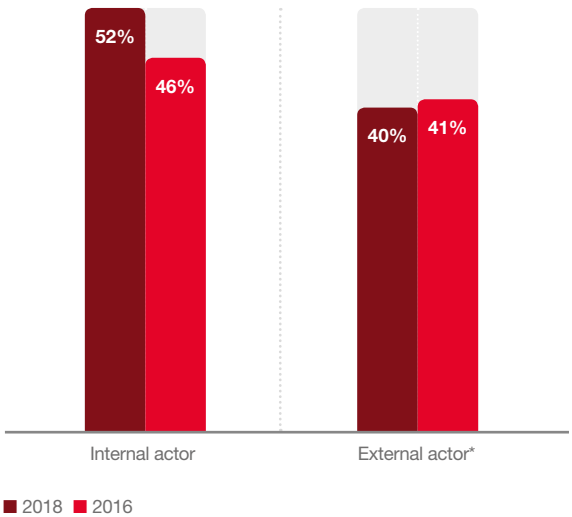
Our survey revealed a significant increase in the share of economic crime committed by internal actors (from 46% in 2016 to 52% in 2018) and a dramatic increase in the proportion of those crimes attributed to senior management (from 16% in 2016 to 24% in 2018). Indeed, internal actors were a third more likely than external actors to be the perpetrators of the most disruptive frauds. In Luxembourg 82% of the fraud was perpetrated by external actors which is based on the growing importance of cybercrime which almost by definition is committed by external actors.

However, one of a company's biggest fraud blind spots – and biggest threats – is often not to do with its employees, but rather the people it does business with. These are the third parties with whom companies have regular and profitable relationships: agents, vendors, shared service providers and customers. In other words, the people and organisations with whom a certain degree of mutual trust is expected, but who may actually be stealing from the company.

24%

of reported internal frauds were committed by senior management

Exhibit 9: Internal actors are the main perpetrators of fraud



***68%**

of external actors committing the fraud are "frenemies" of the organisation – agents, vendors, shared service providers and customers

Q. Who was the main perpetrator of the most disruptive fraud?

Source: PwC's 2018 Global Economic Crime and Fraud Survey

Take a dynamic approach

Chief executives are accountable

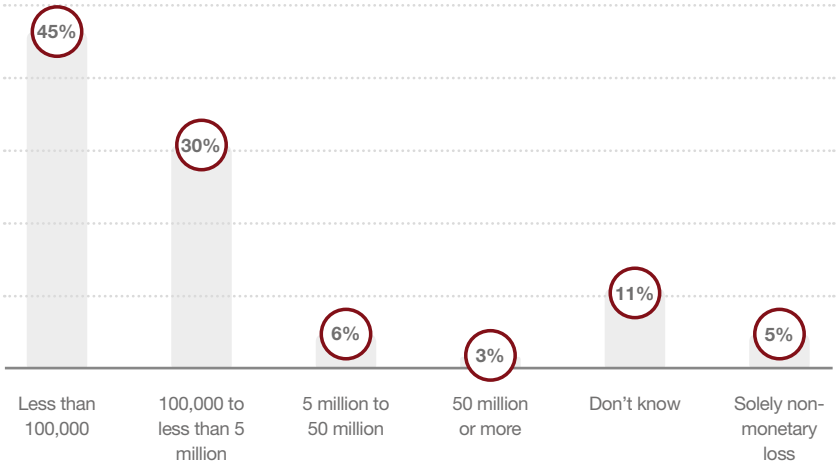
Our survey underscores that the direct monetary cost of fraud and its aftermath can be substantial. But when secondary costs (such as investigations and other interventions) are included, the true picture of overall cost can be much higher.

46%

of respondents said their organisation spent the same or more on investigations and other interventions than was directly lost to fraud itself

When the financial costs of fraud hit the bottom line of a business, it is only natural for the board and shareholders to require explanations from senior management. In today's world, however, a leader's responsibility doesn't stop there. In fact, that's just the beginning.

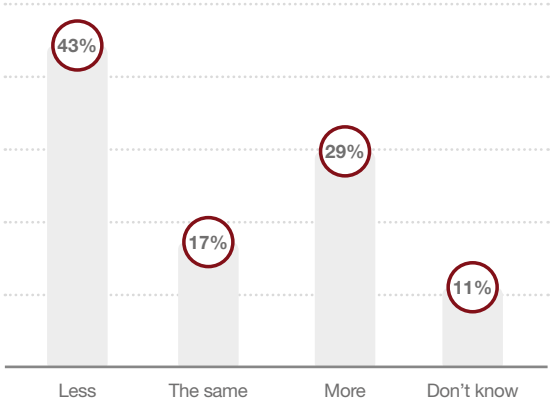
Exhibit 10: Direct monetary losses due to fraud can be substantial (in USD)



Q. In financial terms, approximately, how much do you think your organisation may have directly lost through the most disruptive crime over the last 24 months?

Source: PwC's 2018 Global Economic Crime and Fraud Survey

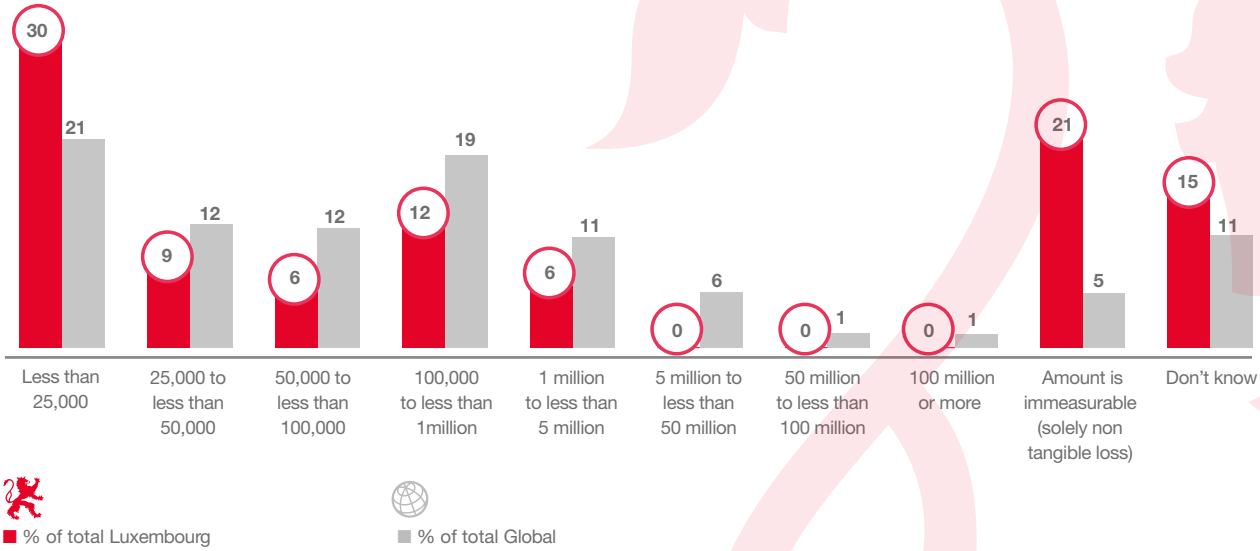
Exhibit 11: The amount spent on investigations and other interventions as a result of fraud is significant



Q. As a result of the most disruptive crime experienced in the last 24 months, was the amount spent by your organisation on investigations and/or other interventions, more, less or the same as that which was lost through this crime?

Source: PwC's 2018 Global Economic Crime and Fraud Survey

Exhibit 12: Financial losses due to economic crime (in USD)



Q. In financial terms, approximately, how much do you think your organisation may have directly lost through the most disruptive crime over the last 24 months?

Source: PwC's 2018 Global Economic Crime and Fraud Survey

The final impact of economic crime includes not only direct losses, but also, for example, the costs of remediation and mitigation.

19% of the participants in the global survey suffered costs between USD 100,000 and USD 1 million, with 12% of the Luxembourg companies experiencing similar level of loss. Such financial impact is already significant. An additional 6% even suffered losses between USD 1-5 million which results in almost a fifth of cases above USD 100,000 in Luxembourg. Still 15% of cases are between USD 25,000 and 100,000. However, with trust-based businesses like Financial Services, the reputational "non-financial" impact is inestimable. In addition, investigation and remediation costs can also quickly add up. Furthermore, financial consequences imposed by regulators have also significantly increased in the recent months. A pretty concerning figure is always the "don't know" (15%) since from our experience there is often some significant damage hidden because organisations do not have proper intelligence due to a lack of risk assessments and professional incident management and remediation. Such "don't know" cases then sometimes transpose themselves in bad surprises at a later stage.

Financial fines for regulatory non-compliance and legal breaches imposed by Luxembourg and continental Europe do not (yet) come close to those imposed by their US counterparts. However, CSSF penalties for non-compliance with AML rules and regulations can be in 10 Million EUR range and above quite quickly now and currently, we are not even far from this threshold.

With the implementation the 4th AML EU Directive the trend towards more significant fines is expected to continue.

Your reputation is not subject to any jurisdiction, law or due process.

This paradox describes the perils of blind spots, and how inaction actually becomes negative action. Despite the dutiful increase in spending on antifraud measures, there is still an overhang of an outworn attitude: That fraud is something to react to – a cost of doing business, essentially – rather than something worth going on the offensive to eradicate for strategic reasons.

A company's security maturity level could have an impact on the its valorisation given the large resources (especially human and financial) that are needed to establish or improve it.
An acquired organisation also carries its cyber-security, potential financial, legal and reputational risks to the buying entity.
Only 36% of Luxembourgish companies perform cyber-security due diligence during the acquisition process.

Globally, and in Luxembourg, majority of the economic crimes have triggered losses below the USD 25,000 threshold, which is considered low. However, given the significant possible impact there is no room for complacency and again the indirect costs are often underestimated. The lower level damage amount frauds are also typically linked to consumer fraud and cyber-related attacks that are committed from external fraudsters. The inside jobs, e.g. misconduct, happen less often, but the financial impact quickly skyrockets.

The Luxembourgish experience is that financial sector clients suffer significant losses from a small number of crimes or incidences of misconduct, while the non-financial sector has a greater number of incidences, but with smaller impact.

Global impact of economic crime

When analysing the broader impact of economic crime on organisations, 36% of Luxembourg companies consider that it doesn't affect employee morale, compared to only 19% globally. Employee morale is difficult to measure, and the low impact might be underestimated. Additionally, some companies prefer to say nothing on the subject.

42% of Luxemburgish companies report that crime incidents have no impact on their business relations. This may be due to the fact that Luxembourg has traditionally maintained a low profile on reporting local incidents, and its financial sector relies on its international reputation and clientele who are not aware of local incidents. This conclusion from the respondents is, however, a risky one since such situations are increasingly sensitive for business partners, and bad news travels fast.

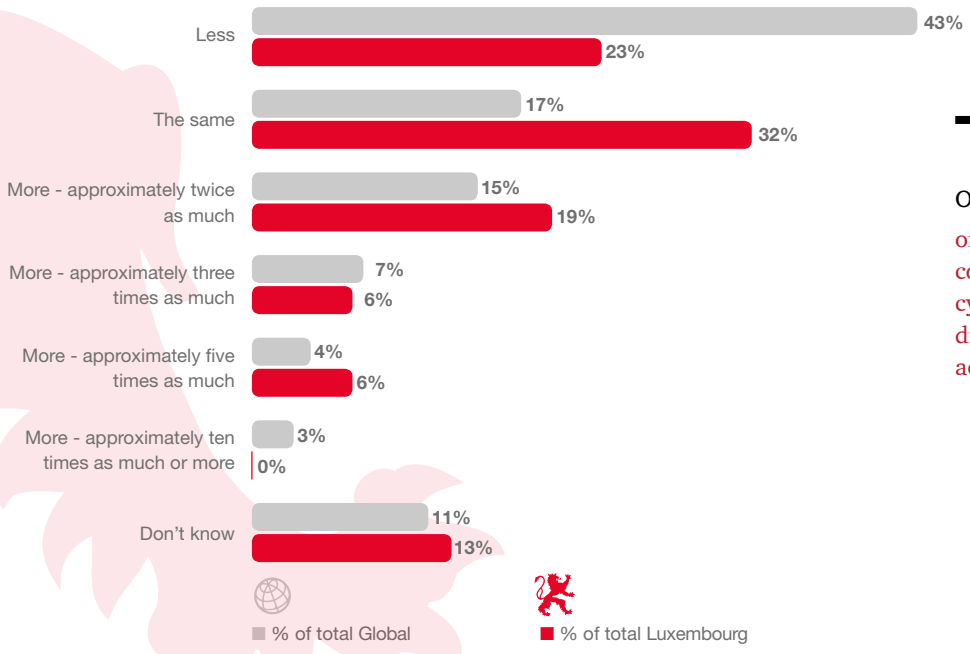
In Luxembourg 27% of the organisations considered that most disruptive crimes experienced seriously compromise their **relations with the regulators**. This observation confirms the implementation of enhanced regulations, regulator controls and increasingly hefty consequences of non-compliance.

Implementation of the 4th AML EU Directive, in addition to more concerted actions from regulators in Europe and beyond get more and more traction, has given Luxembourg regulators more "fire-power" to sanction breaches.

Almost **3 out of 4**

Luxembourgish organisations have understood the challenges of sharing information related to cyber-attacks with the government and/or law enforcement agencies. This may be due to regulatory obligations, especially in the financial sector, or perhaps on a realisation that this fight cannot be won alone.

Exhibit 13: Amount spent for fraud investigations



Q. As a result of the most disruptive crime experienced in the last 24 months, was the amount spent by your organisation on investigations and/or other interventions, more, less or the same as that which was lost through this crime?

Source: PwC's 2018 Global Economic Crime and Fraud Survey

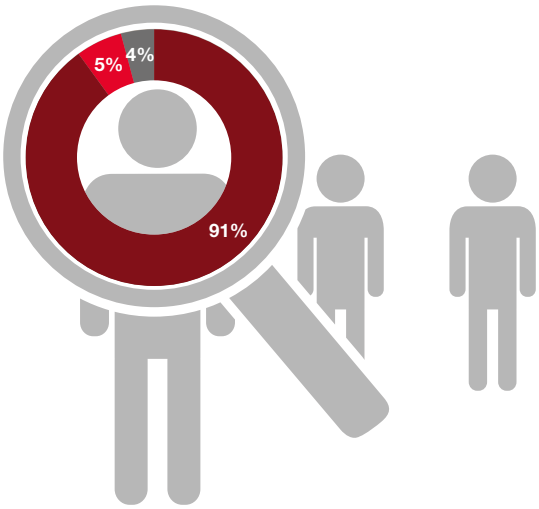
Only **36%**

of Luxembourgish companies perform cyber-security due diligence during the acquisition process.

A chief executive is increasingly seen as the personal embodiment of an organisation – with their finger on the pulse of every facet of its culture and operations at all times. So, when ethical or compliance breakdowns happen, these individuals are often held personally responsible – both by the public and, increasingly, by regulators. Whether merited or not, one thing is clear: the C-suite can no longer claim ignorance as an excuse.

Our survey shows that in nine in every ten cases, the most serious incidents of fraud have been brought to the attention of senior management. In addition, 17% of respondents indicated that the CEO has primary responsibility for their organisation's ethics and compliance programme. This puts a sharp spotlight on how the front office is managing the crisis – and the extent to which they are (or are not) adjusting their risk profiles accordingly.

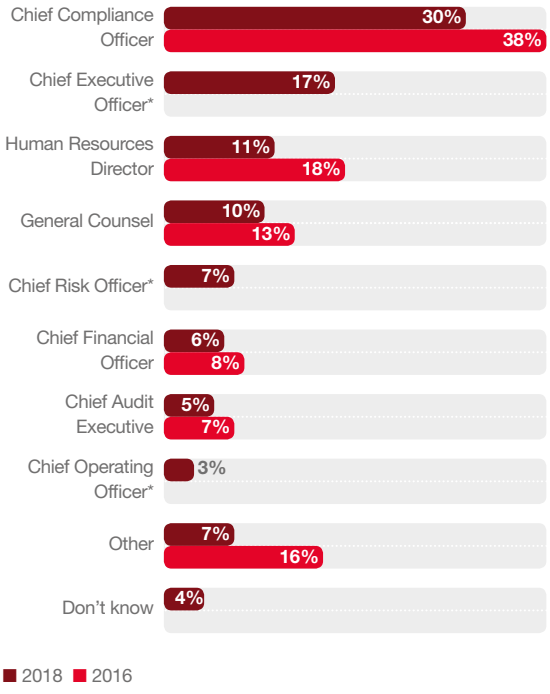
Exhibit 14: Organisations are reporting serious frauds to senior management



Q. Was the most disruptive incident you indicated brought to the attention of your board level executives or to senior leaders charged with governance?

Source: PwC's 2018 Global Economic Crime and Fraud Survey

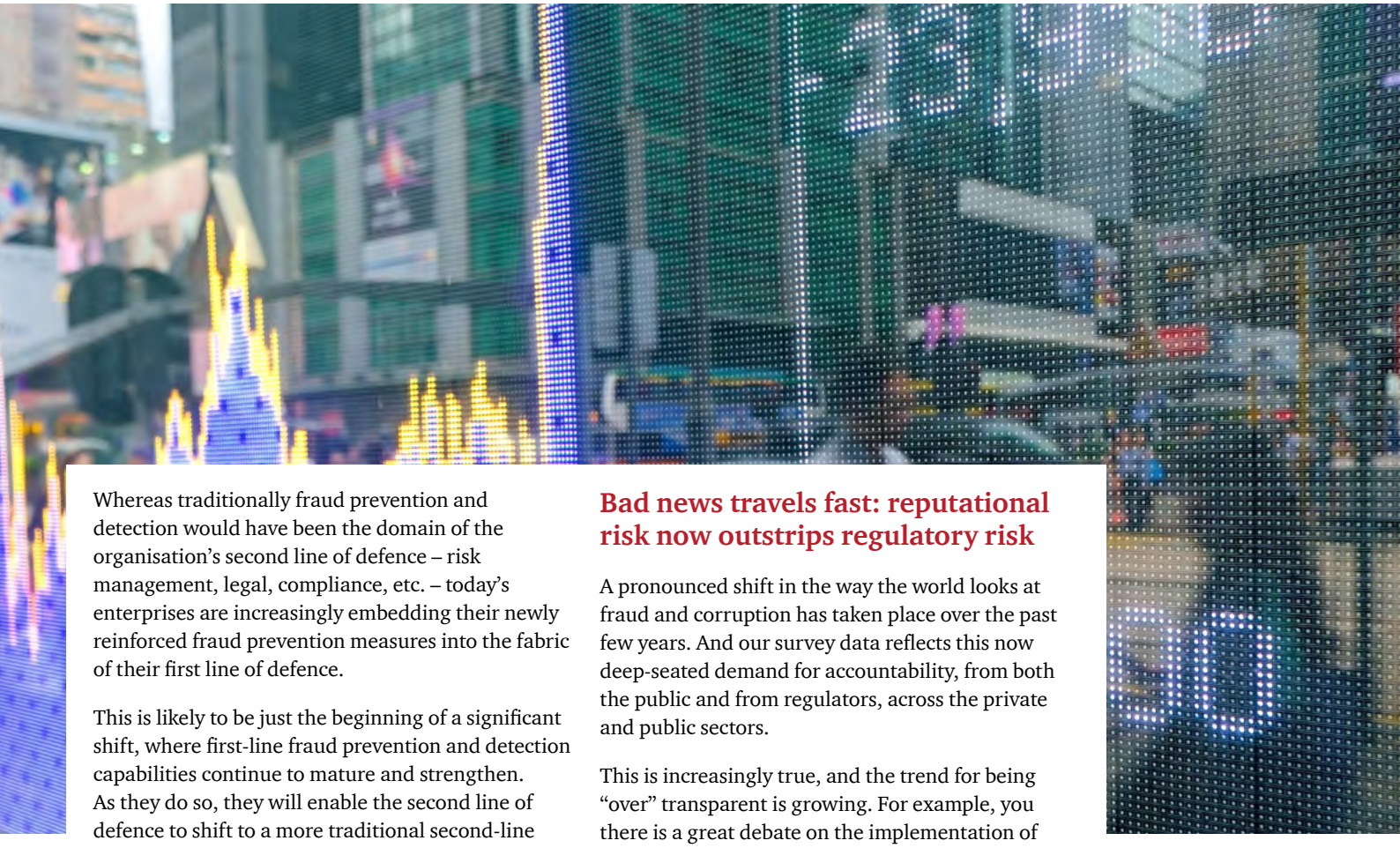
Exhibit 15: Primary accountability for ethics and compliance programmes resides with the C-suite



* New option in 2018.

Q. Who has primary responsibility for the business ethics and compliance program in your organisation?

Source: PwC's 2018 Global Economic Crime and Fraud Survey



Whereas traditionally fraud prevention and detection would have been the domain of the organisation's second line of defence – risk management, legal, compliance, etc. – today's enterprises are increasingly embedding their newly reinforced fraud prevention measures into the fabric of their first line of defence.

This is likely to be just the beginning of a significant shift, where first-line fraud prevention and detection capabilities continue to mature and strengthen. As they do so, they will enable the second line of defence to shift to a more traditional second-line approach: governance and oversight and setting risk tolerance, frameworks and policies.

In a world where the boundaries between industries, technologies and regulatory bodies continue to blur – and where fraudsters are looking for soft spots to attack beyond their traditional, highly protected financial services targets – this is an important development.

Bad news travels fast: reputational risk now outstrips regulatory risk

A pronounced shift in the way the world looks at fraud and corruption has taken place over the past few years. And our survey data reflects this now deep-seated demand for accountability, from both the public and from regulators, across the private and public sectors.

This is increasingly true, and the trend for being "over" transparent is growing. For example, you there is a great debate on the implementation of public beneficial ownership register in the context of AML4D. It calls into question to what extent everyone needs to know everything about everyone!

Exhibit 16: Fraud detection moves up to the first line of defence

1

Executive management

The CEO and executives are responsible for management of risk and are held accountable by the Board.

2

Risk functions

Compliance or the risk function are supposed to govern the risk and related controls, and to have an oversight role, but the first line has to manage it.

3

Internal audit

The Internal Auditor is responsible for independent assurance and is accountable to the Audit and Risk Committee.

Your reputation is subject to no jurisdiction, law or due process

That's because, in this era of radical transparency, companies often don't get to decide when an issue becomes a crisis. Rather, that's down to the jury of public opinion. Moreover, society's rules can change much faster than regulators' – and there is little public tolerance for those who break them. Regulators, by definition, operate within a limited jurisdiction and in accordance with well-defined rules. A company's brand reputation, on the other hand, is subject to no fixed jurisdiction, law or due process.

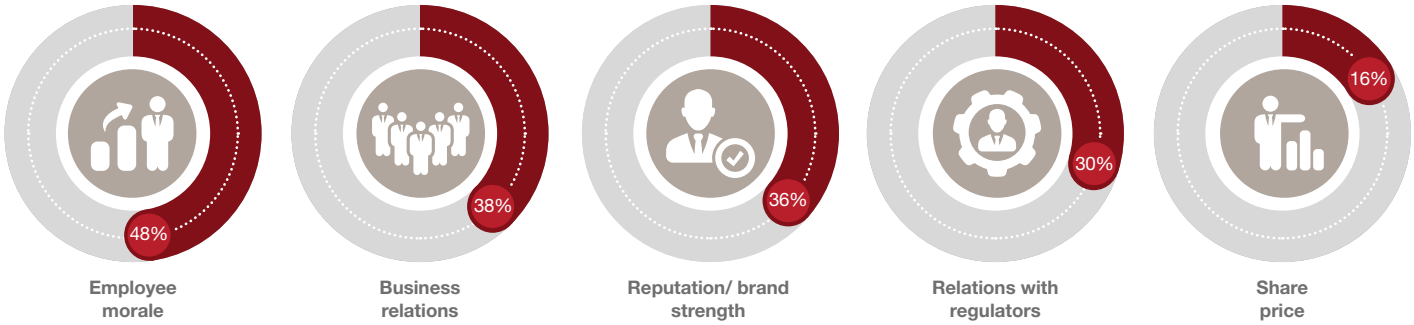
The executives we surveyed consistently ranked reputational harm at or near the top of negative impacts from various forms of economic crime, with public perception (reputation/brand strength, business relations and share price) taking the hardest hit – a level of impact that has increased since 2016 and the global trends are confirmed by local feedback.

Regulatory compliance remains as critical as ever – if not more so. Across the board, regulations and reporting requirements, touching both legal and ethical behaviour, continue to expand. Scrutiny and enforcement are also on the rise globally, and cross-border regulatory cooperation is becoming increasingly routine.

In our survey, 54% of respondents involved in money movement (and/or any of the following lines of business: financial institutions, mutual funds, money service businesses, broker dealers, insurance companies, or dealers in precious metals, stones or jewels) indicated they had experienced an Anti-money laundering (AML) regulatory enforcement or inspection in the last two years (up by 4 percentage points from 2016). And an identical proportion (54%) expect recent changes in the geopolitical regulatory environment to have a greater impact on their organisations over the next two years.

In Luxembourg 33% of the respondents declared having had a regulatory inspection in the 24 past months with no major feedback nor consequences like significant fines. This confirms the high maturity of Luxembourg AML regimes, but the continued efforts of the CSSF on-site visits will certainly remain a topic to be prepared for, with a focus on tax compliance.

Exhibit 17: Fraud and economic crime impact all elements of the business

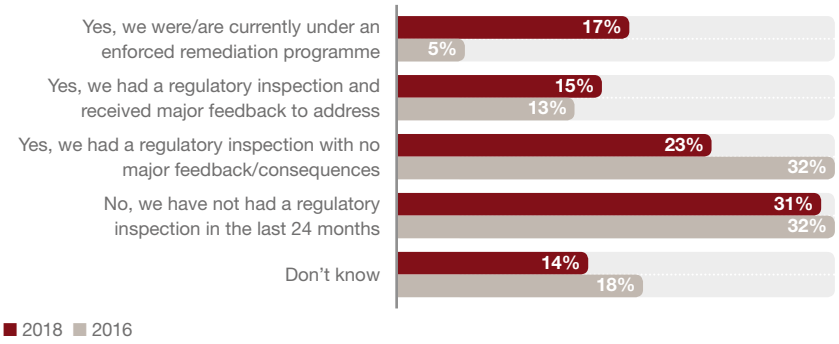


Q. What was the level of impact of the most disruptive fraud/economic crime experienced on the following aspects of your business operations?
Source: PwC's 2018 Global Economic Crime and Fraud Survey

33%

of the respondents, in Luxembourg declared having had a regulatory inspection in the 24 past months with no major feedback nor consequences like significant fines.

Exhibit 18: The number of regulatory enforcements and inspections continues to rise



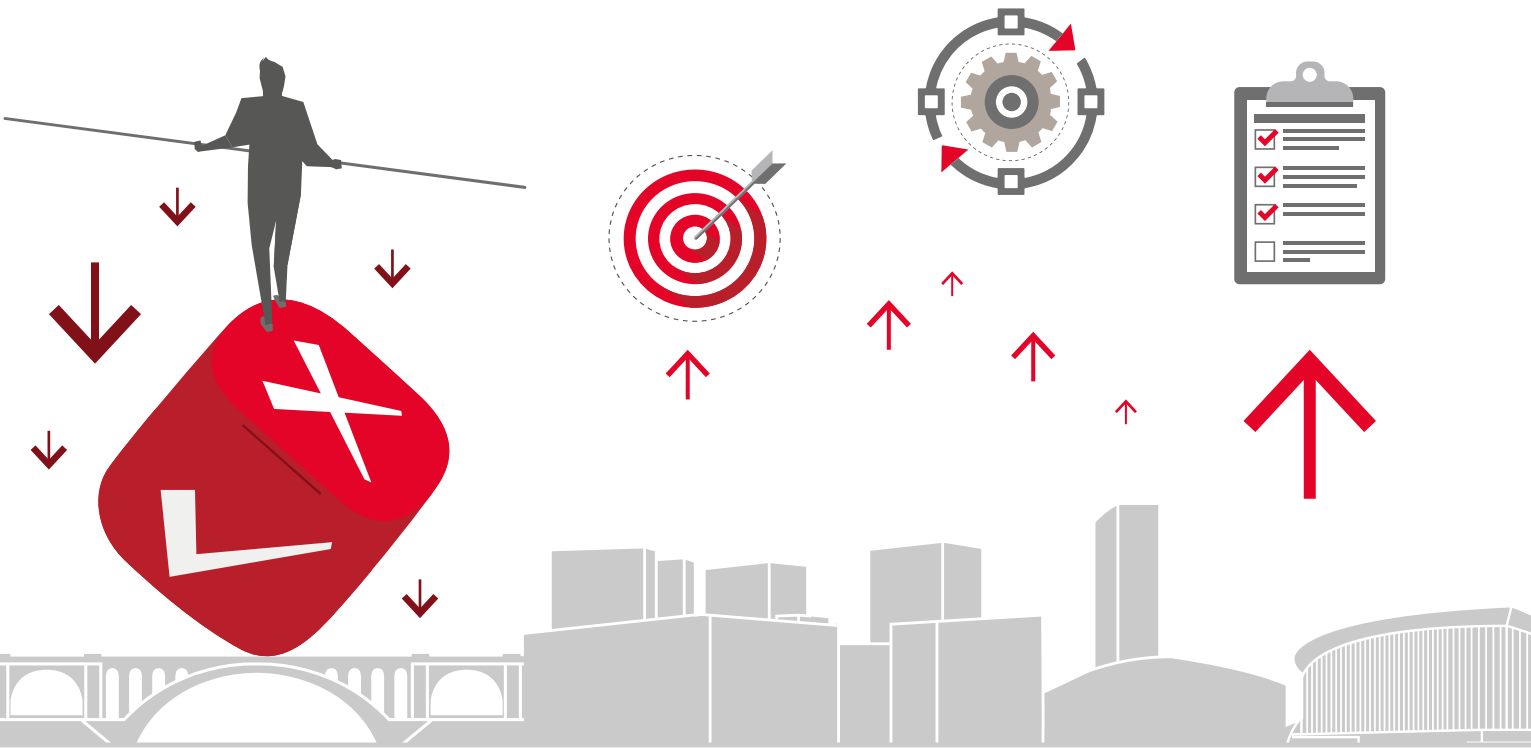
*Organisations involved in money movement and/or any of these lines of business are: Financial Institution, Mutual Funds, Money Service Business, Broker Dealer, Insurance Company, Dealers in Precious Metals, Stones or Jewels.

Q. Has your organisation experienced any regulatory enforcement/inspection in relation to AML in the last 24 months?

Source: PwC's 2018 Global Economic Crime and Fraud Survey

54%

said they expect changes in the regulatory environment to have an increased impact on their organisation in the next 2 years



Harness the protective power of technology

Fraud risk assessments and detection have become more instituted in financial organisations especially since global regulatory obligations have made them more sophisticated and often mandatory. However, this is not yet the case in Luxembourg as its risk assessment focus is on AML related issues. Hence, 70 % of Luxembourgish companies have performed an AML/CFT risk assessment compared to 23% globally. However, since AML and fraud are closely linked, best practices in AML risk assessments increasingly include fraud related risks.

Our survey shows that only 55% of Luxembourg organisations said they have conducted any kind of fraud or economic crime risk assessment. Only 40% of respondents had conducted an anti-bribery/ anti-corruption risk assessment. This is an especially worrisome statistic, considering how impactful and expensive this crime has become, on both the regulatory and financial side, around the world. However, with 70% of the respondents having performed an AML risk assessment and 58% having performed cyber-attack vulnerability assessments, the survey shows a clear focus of the risk assessment practice on Anti-Money Laundering and cybercrime. This is consistent with what Luxembourg perceives as its most likely threats. It is worth nothing that the regular ICA Fund Governance Surveys highlight a strong concern and focus of directors/boards on AML/KYC related matters, but the wider rules of Financial Crime are typically not in the focus of their considerations. Our results suggest that this would require some second thoughts. A particular focus should then be given to the fact what to do based on such risk assessments, since our local discussions show that there is often little tangible action to tackle identified risks in an efficient way.

With cyber-criminals becoming increasingly more sophisticated, organisations have no choice but to prepare for the worst. The definition and implementation of a **Cyber security program** to tackle cyber-security risks has become a standard practice for 2 out of 3 organisations. However, these programs fail to properly tackle crucial aspects of cyber-security: Detection & Response.

Only a third of respondents include a dedicated Security Operations Centre in their programs, and only 23% are testing their incident response practices to ensure their efficiency. Worst, despite the Luxembourgish Market understanding of the importance of including cyber-security in their operational risk assessments, only about 1/4th of these risks assessments are covering their cyber-response plan, making it difficult for organisations to guarantee their efficiency and completeness.

Despite best practices and regulations, in only half of Luxembourgish organisations the Chief Information Security Officer (CISO) reports directly to a board level executive. Board members still need to be convinced to invest in "Detect & Respond" capabilities and to improve the overall quality of their Cyber security program.

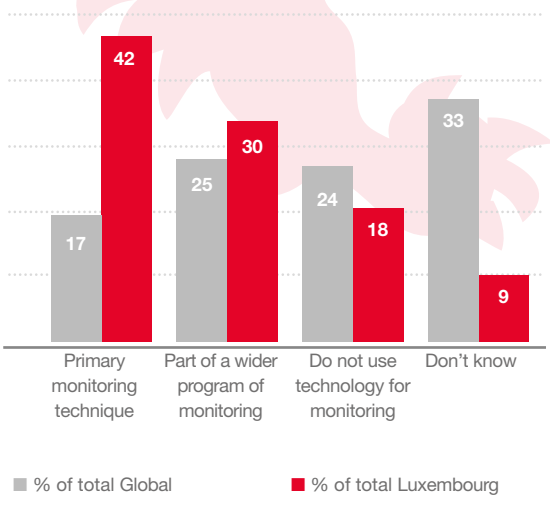
Screening tools are used to monitor third party due diligence. For 47% of the organisations in Luxembourg, it is at least part of a wider program of monitoring if not the primary monitoring technique. At it is specific to financial sector, it is less developed at a global level.

In a strong financial environment, where **Transactions Monitoring** are mandatory, it is encouraging to see a positive feedback regarding its

70%

of Luxembourgish companies have performed an AML/ CFT risk assessment compared to 23% globally.

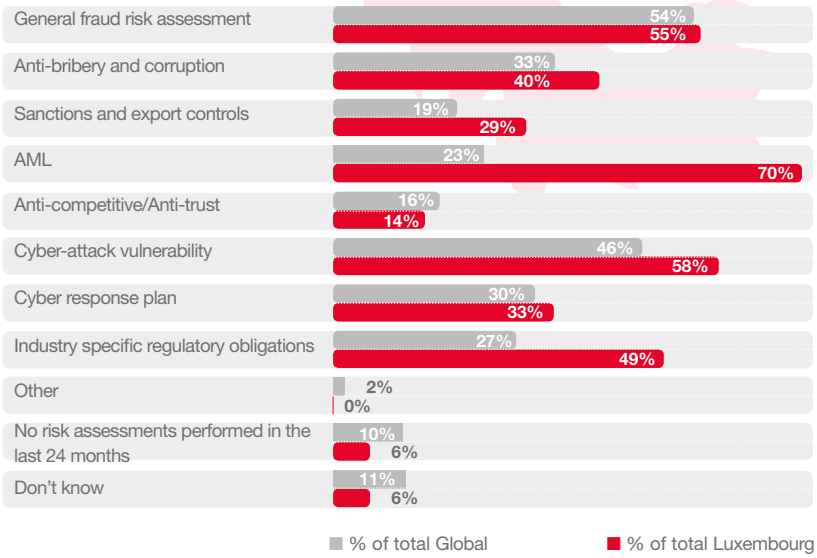
Exhibit 19: Use of technology as an instrument to detect AML activities



Q. To what extent do you use technology as an instrument to monitor fraud and/or economic crime in each of the following areas?

Source: PwC's 2018 Global Economic Crime and Fraud Survey

Exhibit 20: Risk assessments performed



Q. In the last 24 months, has your organisation performed a risk assessment on any of the following areas?

Source: PwC's 2018 Global Economic Crime and Fraud Survey

use. Transaction monitoring, from a Luxembourg perspective, strongly depends of the scale and nature of the transactions. Furthermore, the majority of the transactions occur cross-border making transaction monitoring scenarios more complex. The default scenarios often suggested by software vendors are not always meeting the Luxembourg market requirements sufficiently and here more regulatory guidance could be helpful. In jurisdictions such as the USA, there is an increasingly heavy focus on the effectiveness of transaction monitoring systems and it can be expected that such trends will soon find their way into Europe.

Unlike 2016, where only 11% of the participants were concerned about a high production of alerts or false positive, in 2018 37% of the Luxembourg respondents are worried about false positives or alerts. Globally, the concern about false positives grew from 23% to 25%. A wider adoption of technology and larger sample populations might explain the growing concern, as more participants push to use technology to fight fraud/economic crime in response to regulatory requirements.

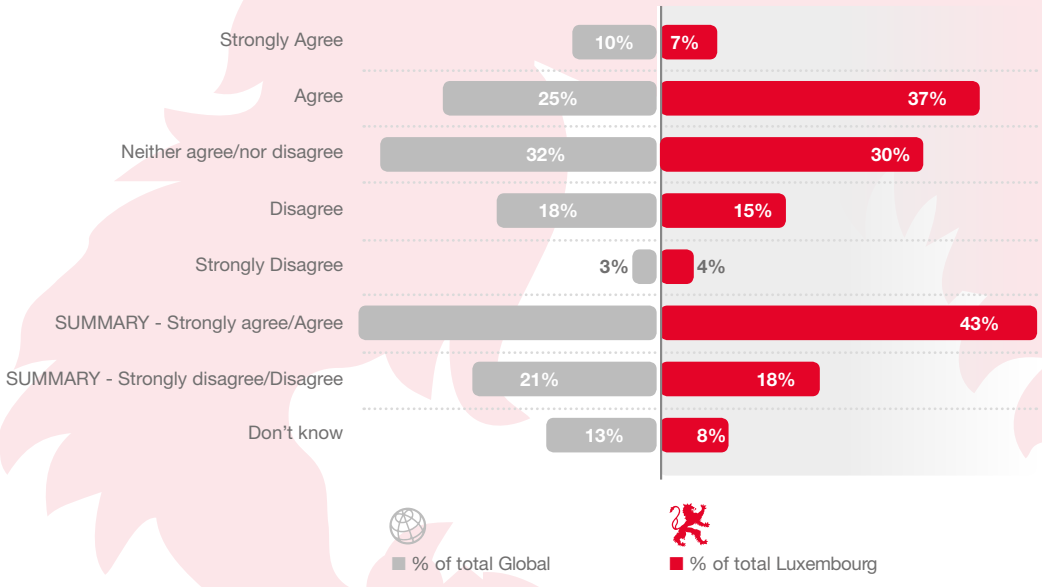
What can you do? Take away questions

- **Have you completed a fraud risk assessment recently? If not, why not?**
- **Do you know the norms for ethics and compliance in your industry?**
- **Does your ethics and compliance programme explicitly target fraud?**
- **Are your incentives consistent with regulations? Are they consistent with doing the right thing for your customers and your people?**
- **Do you have an open-door policy or hotline that could serve as an early-warning sign of internal fraud?**
- **Have you probed your internal culture for potential trouble spots?**

"It is no surprise, considering how embedded technology is in organisations and the increasing number of external connections/ interactions with partners, suppliers, outsourcers and clients, that Cybercrime can penetrate the core of a company's business and can impede its capacity to function, says **Vincent Villers**, PwC Luxembourg Cybersecurity leader."

Boards and Management teams must understand the utmost need to perform Cybercrime risk assessments as part of their overall strategy building and implementation.

Exhibit 21: Use of technology



Q. To what extent do you agree with the following statements regarding your organisation's use of technology in combatting fraud and/ or economic crime? *"Produces too many alerts or false positives."*

Source: PwC's 2018 Global Economic Crime and Fraud Survey

Finding the technology sweet spot

When it comes to fraud, technology is a double-edged sword. It is both a potential threat and a potential protector. Thus, as companies come to view fraud as first and foremost a business problem which could seriously hamper growth, many have made a strategic shift in their approach to technology. These companies are making a business case for robust new investments in areas such as detection, authentication and the reduction of customer friction.

"An effective anti-money laundering program isn't one that can find a suspicious transaction among millions, but rather a program that never allows that transaction to enter the financial system."

Gregory Coleman
Former FBI Special Agent, Asset Forfeiture/Money Laundering Team

29%

of companies said they spent at least twice as much on investigating and preventing fraud as was lost through the most disruptive economic crimes

42%

of companies said they have increased funds used to combat fraud and/or economic crime

Today, organisations have access to a wealth of innovative and sophisticated technologies with which to defend themselves against fraud, aimed at monitoring, analysing, learning and predicting human behaviour. These include machine learning, predictive analytics and other artificial intelligence techniques. And our survey shows companies are using these technologies, to varying degrees, depending on the industry sector. Technology is expensive to buy and to adopt across a large organisation – prohibitively so, for some. And the decision about what to purchase, and when, is a delicate one. Some invest in emerging or disruptive technologies that they don't use optimally, for instance. Others adopt technology too late and find themselves behind the curve.

The use of innovative technologies to combat fraud is now a worldwide phenomenon. Indeed, our survey shows that companies in developing territories are actually investing in advanced technologies at a faster rate than those in developed territories. We found 27% of companies in developing territories said they currently use or plan to implement artificial intelligence to combat fraud, while just 22% of companies in developed territories said the same. For those developing territories, this approach could represent an effective means of catching up in an area in which other nations have already sunk considerable infrastructure costs.

In the end, the ubiquity of technology creates a double challenge for all organisations: how to find the sweet spot between a technology's effectiveness and its cost while remaining ahead of the fraudsters.

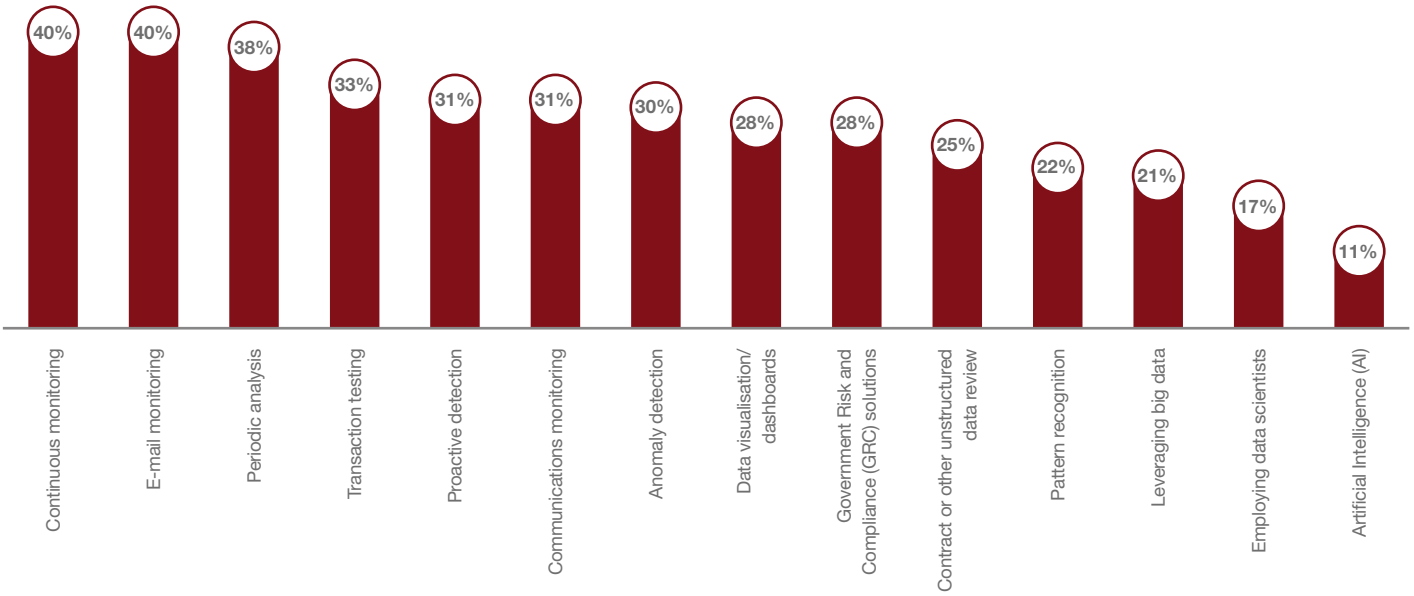
With regards to these technology trends, Luxembourg certainly has room for improvement, since we have not yet a general trend in that direction. Some organisations are very progressive in leveraging new aspects like Robotic Process Automation (RPA), biometrics or Video Identification approaches to KYC but this is still in an early growing phase.

It is also important that various technologies that are used globally or in developing countries do not have the regulatory blessing that we could require in Luxembourg.

34%

of respondents said they thought their organisation's use of technology to combat fraud and/or economic crime was producing too many false positives

Exhibit 22: Organisations are beginning to derive value from alternative and disruptive technologies in combatting fraud



Q. To what degree is your organisation using and finding value from the following alternative/disruptive technologies and techniques in your control environment to help combat fraud and/or economic crime? (% of respondents who said their organisation uses and derives value)

Source: PwC's 2018 Global Economic Crime and Fraud Survey

Customers aren't just one consideration of your business – they are your business

Customers are the lifeblood of any business. But, as business models continue to evolve through the digital revolution, many of those customers are being exposed to payment fraud for the first time. How an organisation handles that fraud will profoundly affect its outcomes. Here are some of the characteristics and challenges of today's digital fraud:

New digital products are creating new attack surfaces

To bring products to market, companies once followed an established B2B process involving resellers, distributors and retailers. On today's innovative B2C digital platforms, there is a much wider attack surface – and much more room for fraud to break through.

Industry lines are blurring

Non-financial services companies are venturing into payment systems. These relative newcomers sometimes lack the anti-fraud and Anti-money laundering experience and know-how of traditional financial services companies, making them, and their third-party ecosystems, susceptible to both fraud and regulatory risk.

The technical sophistication of external fraudsters continues to grow

Digital fraud attacks are becoming more and more sophisticated, thorough and devastating. Single ransomware attacks can cripple organisations
and fraudsters manage to move billions of dollars between bank accounts every day.

You can change your credit card number, but you can't change your date of birth

The knowledge-based authentication tools long used to control fraud are outdated and new techniques – such as digital device ID and voice biometrics – are now necessary to protect customers' assets. But most companies are yet to adopt them. This is important because a major data theft is nothing like the loss of a replaceable asset like cash. Rather, what is lost is an individual's unique, deeply personal, permanent identity markers (such as date of birth or social security number). Because this is the very data that knowledge-based authentication tools use to verify identity and prevent fraud, its theft opens the door for fraudsters to take over a person's identity.

41%

of executives surveyed said they spent at least twice as much on investigations and related interventions as was lost to cybercrime

Cybercrime: a disconnect between ends and means

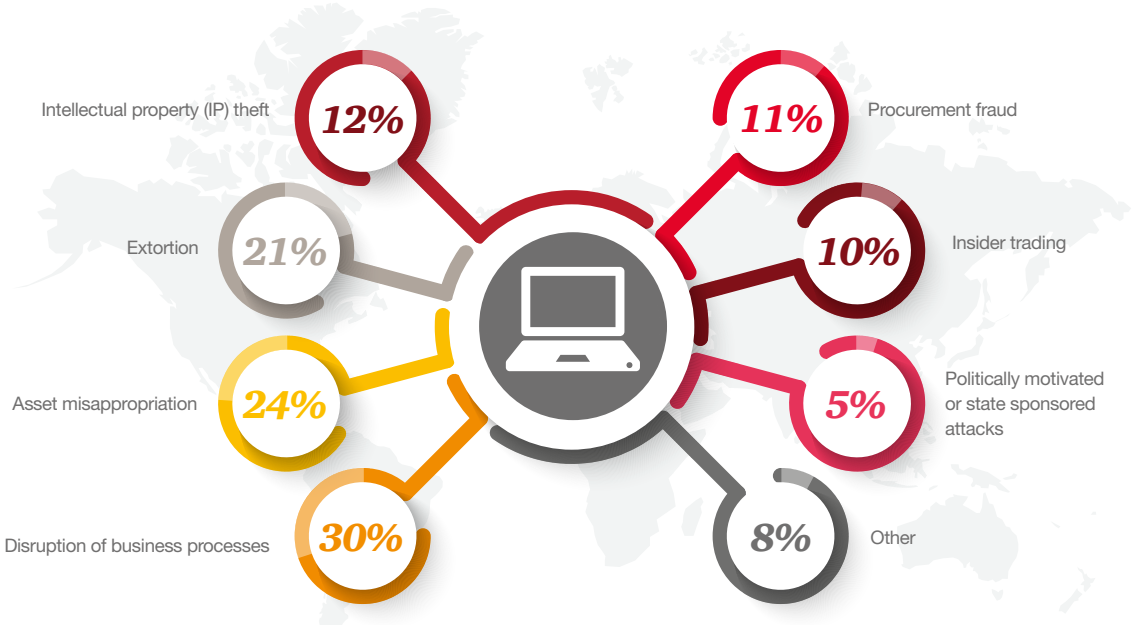
Cybercrime has long passed beyond infancy and adolescence. Today's cybercriminals are as savvy and professional as the businesses they attack. This maturity calls for a new perspective on the multifaceted nature of cyber threats and accompanying frauds.

Often, the first sign an organisation gets that something systemic is amiss is the detection of a cyber-enabled attack, such as phishing, malware or a traditional brute force attack. The increasing frequency, sophistication and lethality of these attacks are spurring companies to look for ways to pre-empt them. This approach has the added benefit of enabling a deeper focus on fraud prevention.

Although it can be difficult for companies to accurately measure the financial impact of cyber-attacks, 14% of survey respondents who said cybercrime was the most disruptive fraud told us they lost over USD 1 million as a result, with 1% indicating they lost over USD 100 million.

Cybercrime was more than twice as likely than any other fraud to be identified as the most disruptive and serious economic crime expected to impact organisations in the next two years (26% of respondents said they expected a cyber-attack in the next two years and that it would be the most disruptive; 12% said they expected bribery and corruption to be most disruptive; while 11% said the same about asset misappropriation). In fact, cyber-attacks have become so pervasive that measuring their occurrences and impacts is becoming less strategically useful than focusing on the mechanism that the fraudsters used in each case.

Exhibit 23: Types of fraud that organisations were a victim of through a cyber-attack



Q. Which of the following types of fraud and/or economic crime was your organisation victim of through a cyber-attack?
Source: PwC's 2018 Global Economic Crime and Fraud Survey

34%

of the organisations victim of cyber attacks in Luxembourg have experiences asset misappropriation fraud and 39% disruption of business processes

While all digital fraud is fraud, not all fraud is digital. It can therefore be helpful to distinguish two forms of cybercrime:

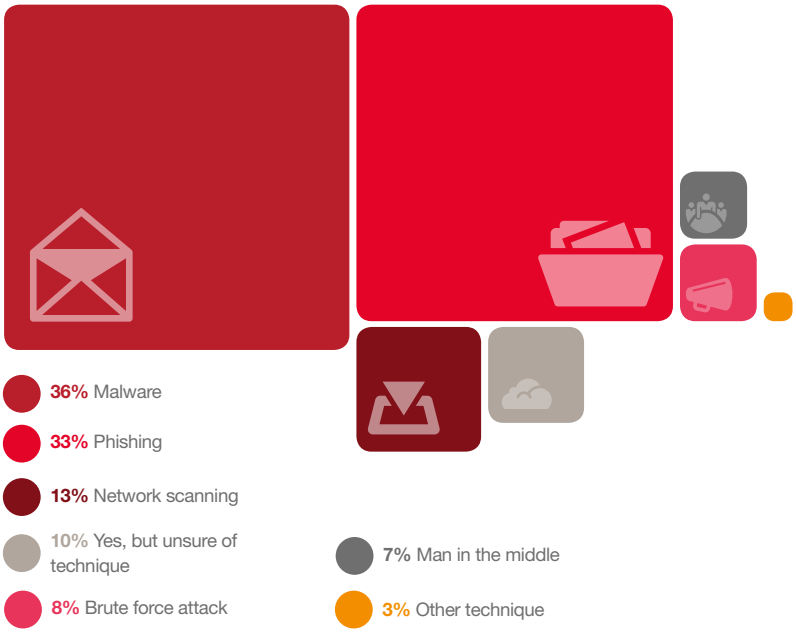
(1) As digital theft (the stolen goods, not the smashed door). This type of attack could include stealing cash, personal information, and intellectual property, and could involve extortion, ransomware, or a host of other crimes.

(2) As digital fraud. This type of attack is in many ways the more long-lasting and disruptive, because the fraudster penetrates an open door (typically, but not always, a customer- or employee-facing access point) and uses the company's own business processes to attack it. To combat this type of fraud, the organisation must use digital methods – both as a vaccine and as a remedy.

54%

In Luxembourg with a result of 54%, phising is the most popular type of cyber-attack followed by malware.

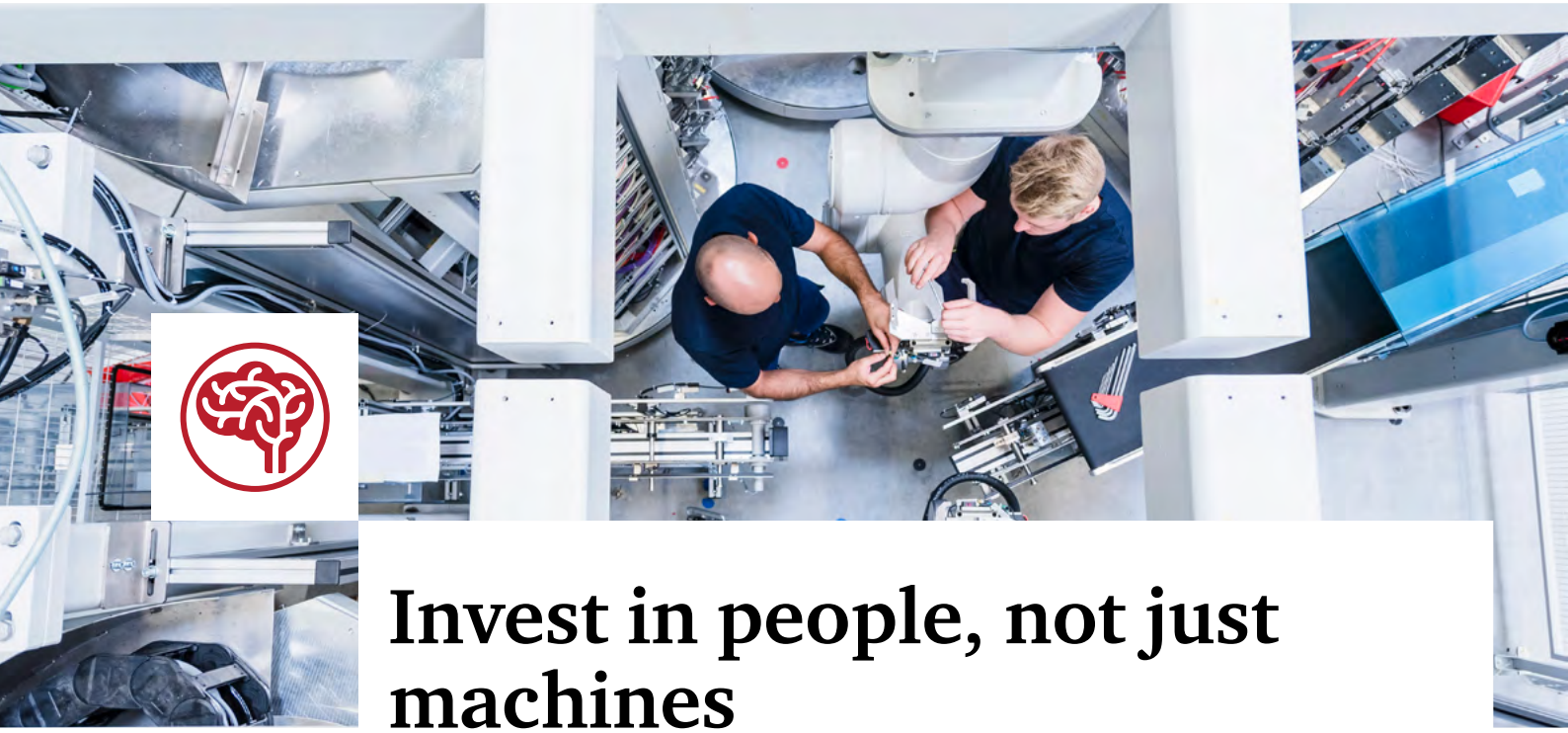
Exhibit 24: Cyber-attack techniques used against organisations



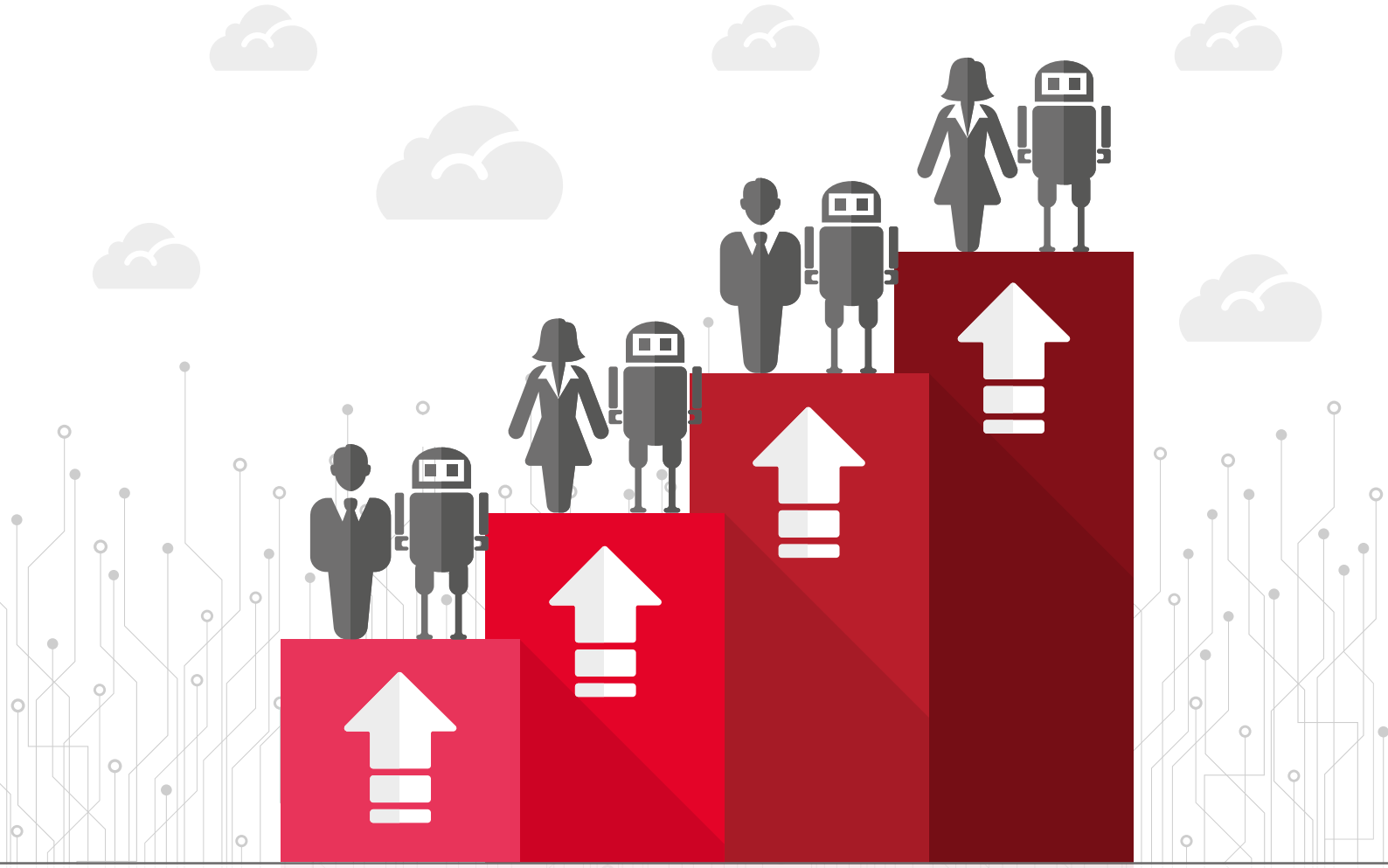
Q. In the last 24 months, has your organisation been targeted by cyber-attacks using any of the following techniques?

Source: PwC's 2018 Global Economic Crime and Fraud Survey

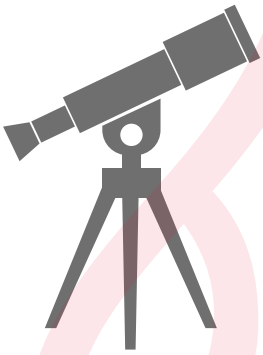
Over a third of all respondents have been targeted by cyber-attacks, through both malware and phishing. Most of these attacks, which can severely disrupt business processes, also lead to substantive losses to companies: 24% of respondents who were attacked suffered asset misappropriation and 21% were digitally extorted.



Invest in people, not just machines



The fraudsters



82%

of the frauds in Luxembourg were perpetrated by external actors, which explains the large number of limited value damage cases.

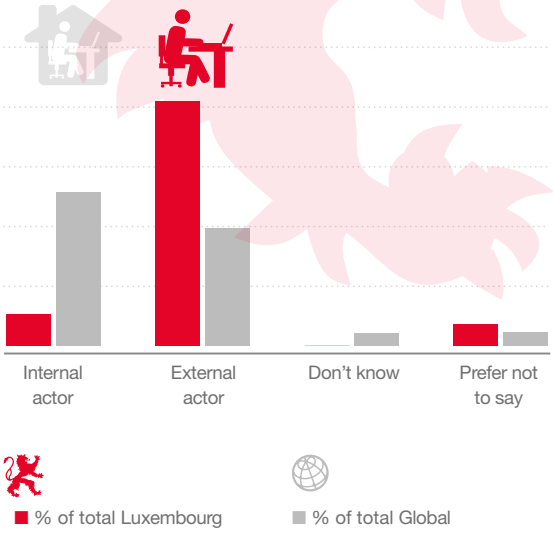
Globally, it is the "enemy within" who poses the biggest crime threat. Inside jobs usually have the biggest financial impact. The insider knows exactly how a company works and precisely what weaknesses to exploit.

Cybercrime is by definition committed by external actors. However, as confirmed by forensic investigations, it is internal actors who cause more serious damage than external actors. The fact that crimes committed by internal actors are not commonly discovered implies a potential weakness in the internal controls of the organisation. The importance of such inside jobs is also reflected in the newly create category of misconduct where our recent forensic investigation work in Luxembourg has often been focused. Misconduct may not demonstrate immediate financial damage, however, it is a breach of rules and regulations that can have a significant impact on organisations. Interestingly, cases of misconduct often correlate with senior management involvement.

While 35% of Luxembourg respondents identified external perpetrators as hackers, an alarming 22% of the respondent did not know anything about the perpetrator. This anomaly flags a weakness in company internal analysis procedures that should be rectified.

One of the biggest threats are the people you have invited to do business with. While internal actors were 30% more likely than external actors to be the perpetrator of the most disruptive fraud (52% versus 40%, respectively), even when the fraudster was external, a sizable percentage of that "external" group includes so-called frenemies: third parties – agents, vendors, and shared service providers – and customers. In other words, people and entities with whom one would expect a certain degree of mutual trust, but who are actually stealing from the company.

Exhibit 25: Who committed the fraud?



Q. Who was the main perpetrator of this fraud?

Source: PwC's 2018 Global Economic Crime and Fraud Survey

Most likely characteristics of the internal fraudster

> **Don't get blindsided by your blind spots**
>
> If you don't know it is here, you don't look for it. If you don't look for it, you don't find it. If you don't find it, you can't make the business case to look for it.

Detection methods

It is remarkable that only 4% of the frauds are discovered through internal audit, 10% less than the global rate.

The internal audit of organisations has a key role in monitoring, and preventing frauds. It is often a top priority for internal audit teams, considering that a low detection rate might indicate a weakness in the internal audit processes. Respondents seem to consider data analytics less effective for financial organisations. Investigative analytics using dedicated software solutions and tools is a core element of PwC's forensic investigations approach, and it is crucial to most cases. Applied properly at the prevention stage, it effectively improves crime prevention results.

Considering the limited number of identified internal perpetrators, it seems Luxembourg companies trust their employees, a fact also confirmed through discussions with our clients. When a potential fraud is detected, Luxembourg companies are likely to use internal resources to carry out an investigation — 87% compared to 79% globally. They are also using external legal advisors to make sure they get the right professional expertise. These results suggest that due to the relatively strict regulatory environment in which they operate, many companies reinforce their staff to have enough resources to detect, or to investigate economic crime. For more significant cases it would however be important to involve the right professional expertise and specialists from the start, since most of the decisions and steps performed at the beginning of an investigation largely influence the outcome an success. From our experience this is often underestimated and in particular when it comes to apply procedures that would be court-proven. It is not about what to do, but rather how to do it!

One of the most important things that an organisation can do is to make sure that everyone understands both the big picture of fraud risk management and how their own function fits into that puzzle. Many companies are adopting a centralised fraud detection team to help them gather sources of information from wherever they may arise (whistle-blowers, investigations, alerts, etc) and piece together the connections between the incidents for investigations, compliance and remediation.

But here, an entreprise-wide fraud function can create a false sense of security, where, once again, fraud is someone else's responsibility and the first lines of defence in the business don't play up that role. Also, since fraud can manifest in as many forms as there are functions, every organisation should be cautious of one-size-fits-all-solutions.

4%

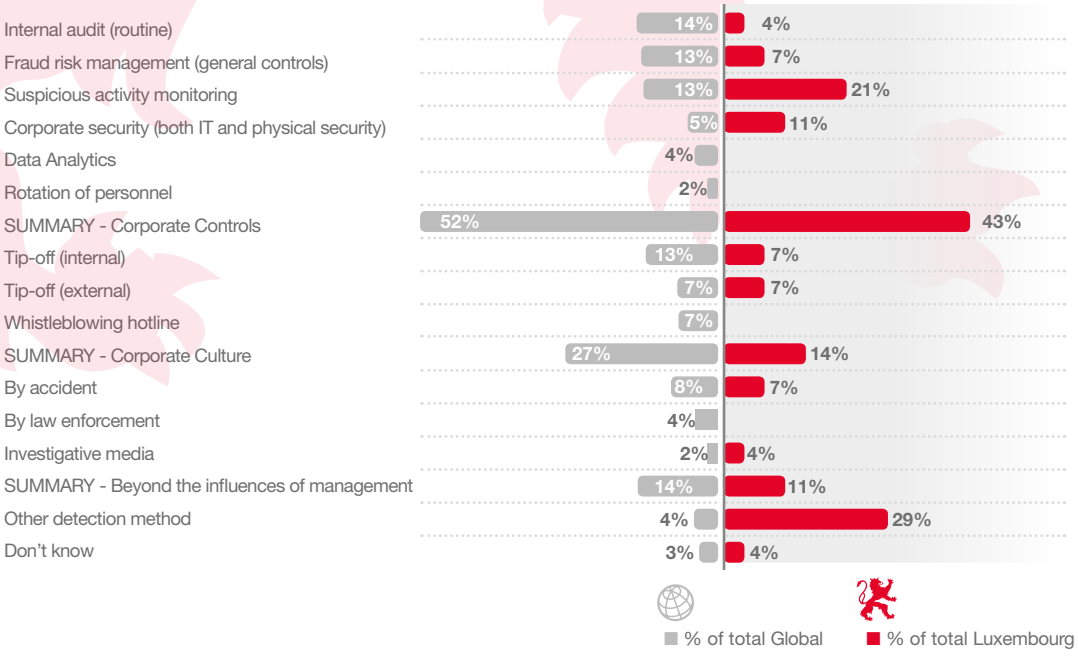
of the frauds are discovered through internal audit, 10% less than the global rate.

"It is important to recognise that, while AML controls in many organizations might be sufficient to tick the box to meet some regulatory expectations, you must incorporate significant, effective and experienced human resources in a meaningful AML program to effectively identify and mitigate real "money laundering risk"

Robert Mazur

Former U.S. Federal Agent
Author of The Infiltrator (a memoir about his undercover life as a money launderer)

Exhibit 26: Fraud detection methods



Q. How was the most disruptive fraud and/or economic crime initially detected?

Source: PwC's 2018 Global Economic Crime and Fraud Survey

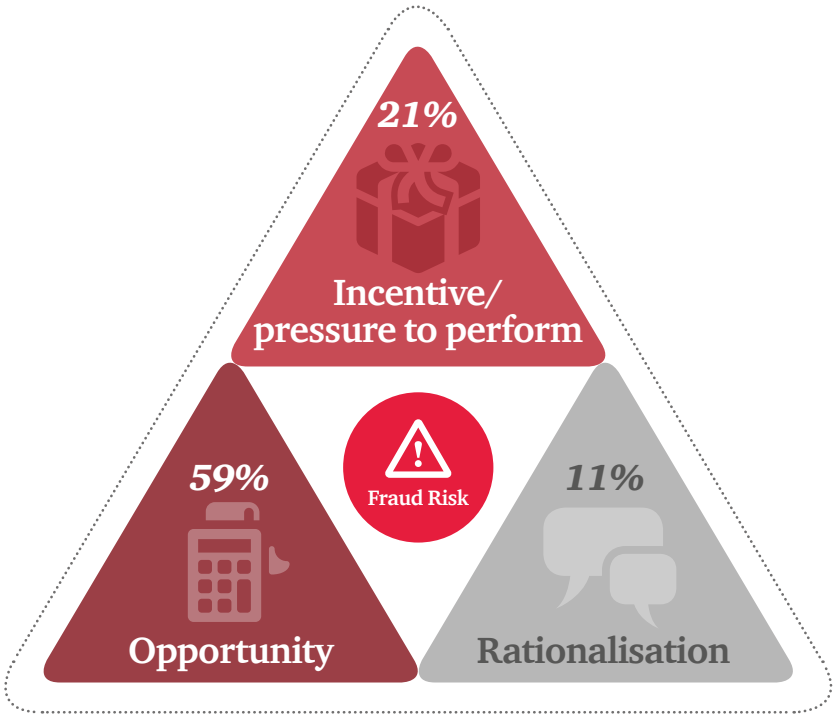
A small investment in people can pay huge dividends

Confronted with the seeming intractability of dealing with fraud, many organisations decide to pour ever more resources into technology. Yet these investments invariably reach a point of diminishing returns, particularly in combatting internal fraud. So, while technology is clearly a vital tool in the fight against fraud, it can only ever be part of the solution.

This is because fraud is the result of a complex mix of conditions and human motivations. The most critical factor in a decision to commit fraud is ultimately human behaviour – and this offers the best opportunity for combatting it. There is a powerful method for understanding and preventing the three principal drivers of internal fraud – the fraud triangle.

The fraud triangle starts with an incentive (generally a pressure to perform from within the organisation) followed by an opportunity, and finally a process of internal rationalisation. Since all three of these drivers must be present for an act of fraud to occur, each of them should be addressed individually.

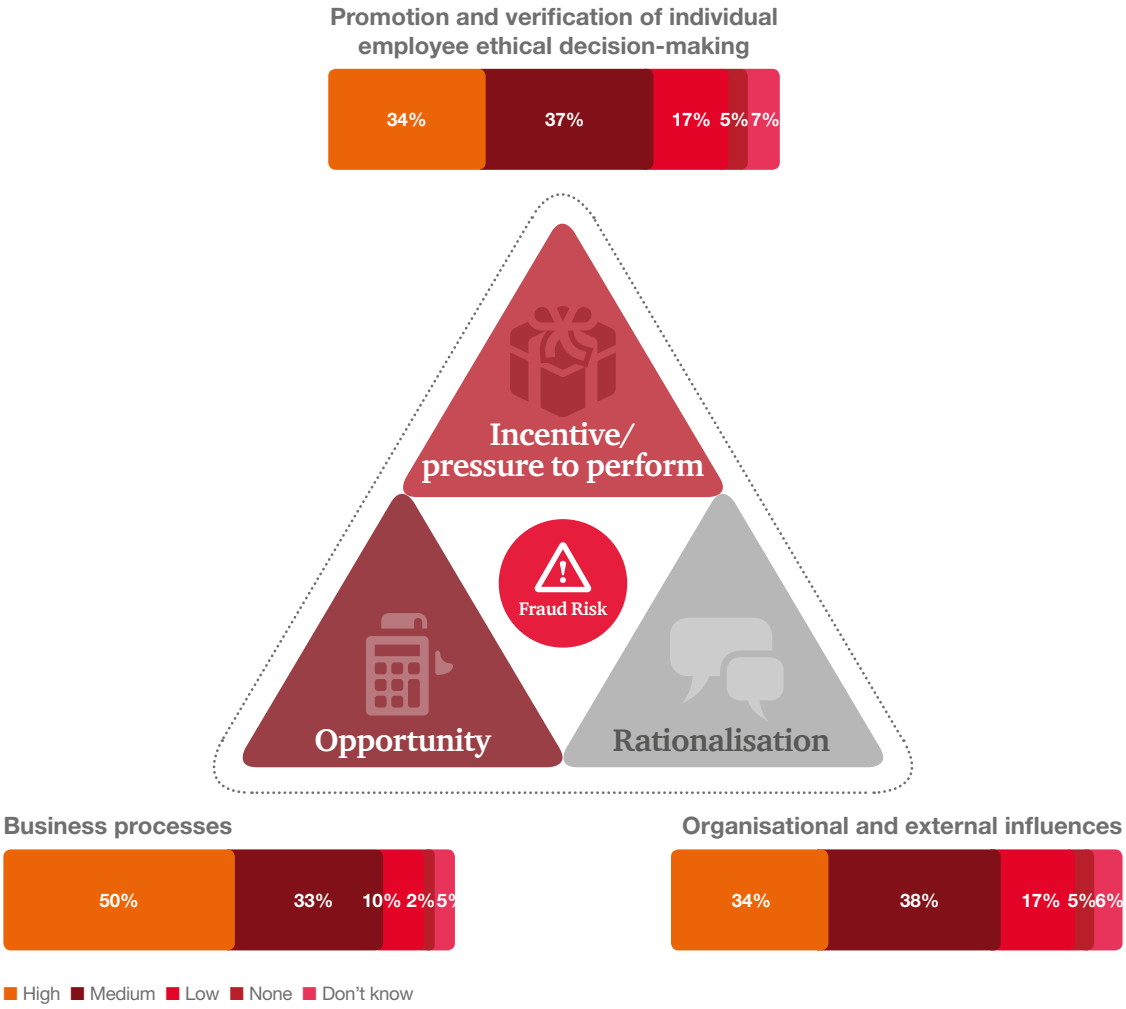
Exhibit 27: The fraud triangle: what makes an employee commit fraud?



Q. To what extent did each of the following factors contribute to the incident of fraud and/or economic crime committed by internal actors? (% of respondents who ranked the factor as the leading contributing factor to internal fraud)

Source: Global Economic Crime and Fraud Survey 2018.

Exhibit 28: The level of organisational effort required to combat internal fraud



Q. What level of effort does your organisation apply to the following categories in order to combat fraud and/or economic crime internally?

Source: PwC's 2018 Global Economic Crime and Fraud Survey

Preventing the opportunity: controls

Most organisations' anti-fraud efforts in recent years have been focused on reducing the opportunities for fraudulent acts: 50% of survey respondents said they expend a high degree of effort in building up business processes, such as internal controls, that target opportunities to commit fraud. And, while 59% of respondents ranked opportunity as the leading contributor to the most disruptive frauds committed by internal actors, this was 10 percentage points lower than the equivalent figure in 2016 (69%). This is evidence that technology has a key role to play – and, more to the point, that companies are generally employing it effectively. For Luxembourg or European countries it has to be noted that our very strict privacy laws make it difficult to implement certain technology driven controls that are widely used in the USA for instance, e.g. systematic staff behavior monitoring.

Unfortunately, companies are putting significantly less effort into measures to counteract incentives and rationalisation, with only 34% indicating they spent a high level of effort targeting these factors. Our survey highlights the result of these choices: 21% of respondents ranked incentives/ pressure as the leading contributing factor of the most disruptive fraud committed by internal actors, twice the amount reported in 2016 (11% identified rationalisation as the leading motivating factor – the same proportion as in 2016).

This under-emphasis on cultural/ethical measures points to a potential blind spot, and indeed may be one reason why internal fraud is so resilient. Because fraud is the result of the intersection of human choices with system failures, it is important to be wary of the false sense of security that internal controls, even well-designed ones, can bring.

Indeed, there is a fundamental flaw with the belief that internal technology-driven controls alone can catch fraud: it assumes that management will always behave ethically. In fact, experience shows that virtually every significant internal fraud is a result of management circumventing or overriding those controls. Our survey backs this up: it reveals that the share of reported serious internal fraud committed by senior management has risen dramatically – by 50% – over the past two years (from 16% of respondents in 2016 to 24% in 2018). We can confirm for Luxembourg that the recent serious cases of fraud or misconduct we worked on always had a direct link to very senior and experienced employees. To overcome this structural problem, organisations need to create controls that actually account for management override or collusion in targeted areas.

Preventing the incentive: openness

Corporate-sized frauds are generally connected to corporate pressures – and the pressure to commit fraud can arise at any level of the organisation. Our survey shows that 28% of organisations that experienced fraud in the last two years suffered business conduct/misconduct fraud (incentive abuse), and 16% of global organisations with offices in other territories experienced business conduct/misconduct fraud in those other territories. Meanwhile, 24% of respondents indicated that senior management was responsible for the most disruptive crime experienced.

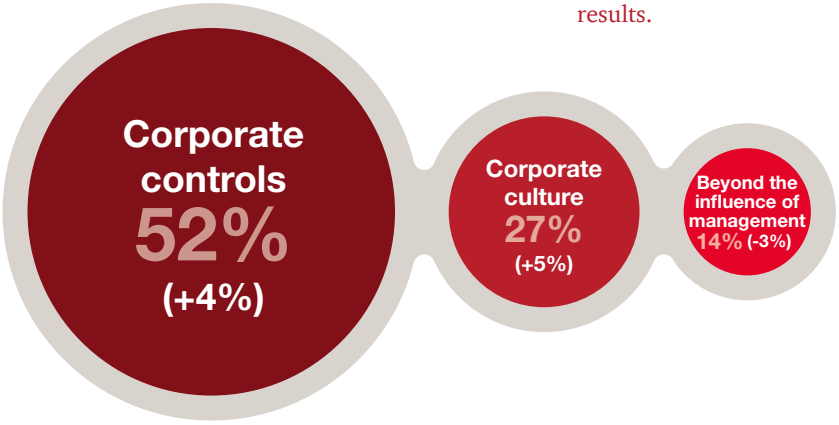
It is important not to over-emphasise financial incentives when considering what drives a person to commit fraud. Fear and embarrassment about having made a mistake may be equally important. Thus, the incentives coming from the top of the organisation must be examined: to what extent do they align with regulations and with "doing the right thing"?

In addition, short-term bespoke controls can serve as useful checks on whether aggressive sales programmes are leading to fraudulent behaviour. A well-publicised open-door or hotline policy can also provide a valuable early-warning system of potential problems in an organisation.

43%

of the Luxembourg respondents, have declared that the most disruptive frauds were detected by corporate controls, as global results.

Exhibit 29: Just over half of the most disruptive frauds were detected by corporate controls



Includes		Includes		Includes	
Internal audit (routine)	14%	Tip off (internal)	13%	By accident	8%
Fraud risk	13%	Tip off (external)	7%	By law enforcement	4%
Suspicious activity monitoring	13%	Whistleblowing hotline	7%	Investigative media	2%
Corporate security	5%				
Data analytics	4%				
Rotation of personnel	1%				

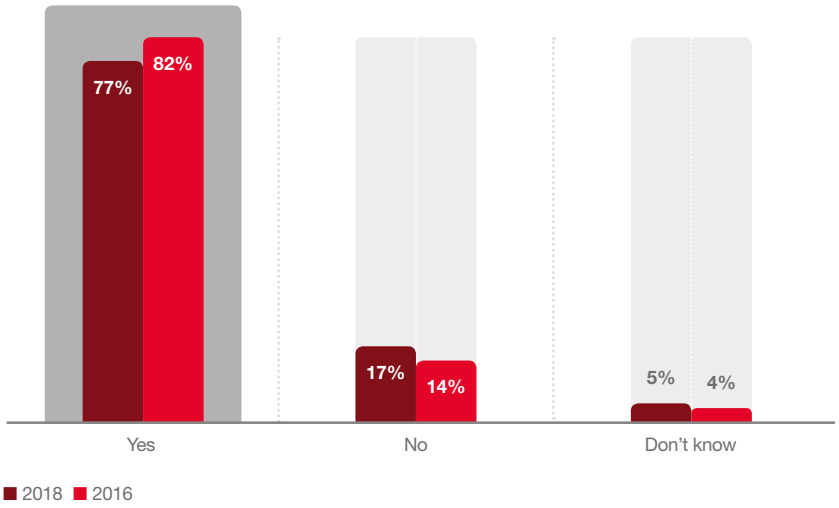
Q. How was the most disruptive fraud and/or economic crime initially detected?

Source: PwC's 2018 Global Economic Crime and Fraud Survey

Fraud can occur with the best of intentions

Fraud needn't necessarily be a malicious or selfish act. From a legal point of view, there are actually two kinds of fraud – fraud committed for personal gain (such as embezzlement, or false reporting intended to boost compensation) and fraud committed for "corporate motives" (such as the survival of the company, or the protection of the workforce). The latter could occur with the best of intentions set on increasing the company's success. For example, what might start as a sales strategy designed to increase market share and profitability (to the benefit of employees) might ultimately morph into fraudulent sales tactics. Either way, the result is the same: the executive suite will be held responsible.

Exhibit 30: Fewer companies report having ethics and compliance programmes



Q. Do you have a formal business ethics and compliance program in your organisation?

Source: PwC's 2018 Global Economic Crime and Fraud Survey

Preventing rationalisation: culture

While incentives and opportunities can be influenced and managed, preventing the rationalisation of a fraudulent act is more of a challenge. This is a process that occurs entirely within the human mind and is thus far harder to influence.

One of the peculiarities of internal fraud is that those who commit it often see it as a victimless crime and cannot visualise any person who will be directly harmed by their actions. This helps explain why nearly three-quarters of survey respondents told us that an internal actor was the main perpetrator of the following most disruptive economic crimes, including human resources fraud (81%), asset misappropriation (75%), insider trading (75%), accounting fraud (74%) and procurement fraud (73%).

The first step in preventing rationalisation is to focus on the environment that governs employee behaviour – the organisational culture. Surveys, focus groups and in-depth interviews should therefore be used to assess the strengths and weaknesses of that culture. Consistent training is also key. If people clearly understand what constitutes an unacceptable action – and why – rationalising fraudulent activity will be harder.

Indeed when interviewing people that had been involved in committing fraud or misconduct, they are often believe that they had some sort of right to do this, or that there was some corporate justification.

However, our survey found a decreasing number of organisations investing in the kind of training that can make a material difference to fraud prevention. The percentage of respondents who indicated they have a formal business ethics and compliance programme has dropped from 82% to 77% since our 2016 survey. And only 58% of companies with such a programme indicated that programme has specific policies targeting general fraud.

The task of detecting and preventing economic crime or fraud is undoubtedly a complex one. It means finding the right blend of technological and people-focused measures, guided by a clear understanding of the motivations behind fraudulent acts and the circumstances in which they occur. Organisations need not resign themselves to the belief that technology is the only solution, or that a certain amount of fraud is simply part of the cost of doing business. Rather, by establishing a culture of honesty and openness from the top down, they can imbue their organisations with a spirit of open accountability – and pull fraud out of the shadows.

Conclusion

> It is always people who commit fraud, not computers
>
> **Michael Weis**, PwC Luxembourg Forensic Services and Financial Crime Leader.

Be prepared. Face the fraud. Emerge stronger.

Fraud, misconduct and financial crime don't rest. They continue to thrive in a fog of limited awareness and under-reporting.

Luxembourg, with its large Financial Sector and concentration of data centres, remains a prime target for criminals, and despite continued efforts of regulators, law enforcement and businesses, increased measures are at best managing to keep the crime rate stable as our findings show; half of the companies in Luxembourg over the past 24 months were subjected to phishing or malware attack.

The most commonly reported, financial crimes in Luxembourg are Asset Misappropriation, Cybercrime, Money laundering and Tax Fraud. Reported Tax Fraud incidents in Luxembourg are 5 times higher than the global average. This is linked to the fact that Tax Fraud is now seen as a predicate offense to money laundering and terrorist financing, and thus falls under much greater regulatory scrutiny.

Meanwhile, 33% of our respondents in Luxembourg declared having a regulatory inspection in the 24 past months, but with no major feedback nor consequences. Whilst this is encouraging, during the same period we faced a significant increase of fines issued by the CSSF, leaving no place for complacency.

Concerns over asset misappropriation and misconduct in Luxembourg, relative to the rest of the world, are remarkably low. However, organisations would be well advised to make sure that their staff is sensitised to remain vigilant, and not to underestimate those crimes.

The financial impact of crime is felt directly with the loss, and then through remediation, mitigation and inestimably through damages to reputation. In addition, there may be significant financial consequences imposed by regulators as recent CSSF fines confirmed. The Luxembourgish experience is that financial sector clients suffer significant losses from a small number of crimes or incidences of misconduct, while the non- financial sector has a greater number of incidences, but with smaller impact.

Our global survey revealed a significant increase in the share of economic crime committed by internal actors and a dramatic increase in the proportion of those crimes attributed to senior management Indeed, internal actors were a third more likely than external actors to be the perpetrators of the most disruptive frauds. In Luxembourg 82% of the fraud were perpetrated by external actors, but the fewer high impact crimes were always linked to an insider or at best based on gross negligence of employees.

Humans are the first vector of cyber-attack and ideal prey for malicious individuals who want to compromise an organisation. 35% of Luxembourg respondents identified external perpetrators as hackers, an alarming 22% of the respondent did not know anything about the perpetrator. This anomaly flags a weakness in company internal analysis procedures that should be rectified.

Indeed the human factor is not to be underestimated. Humans will always be a core target from increasingly sophisticated attackers, but also internally, they need to be prepared to identify or prevent the misconduct of others, since traditional controls are easy to circumvent by insiders. Education and awareness, therefore, remains a top priority.

Contacts

Want to know more about what you can do in the fight against fraud? Contact one of our subject matter experts

Forensic Services, Financial Crime & AML

Michael Weis
Partner, Forensic Services & Financial Crime Leader
PwC Luxembourg
+352 49 48 48 4153
michael.weis@lu.pwc.com

Cybersecurity

Vincent Villers
Partner, Cybersecurity Leader
PwC Luxembourg
+352 49 48 48 2367
vincent.villers@lu.pwc.com

Anti-Money Laundering

Roxane Haas
Partner, Anti-Money Laundering Leader
PwC Luxembourg
+352 49 48 48 2451
roxane.haas@lu.pwc.com

Birgit Goldak
Partner, Anti-Money Laundering Distributor Due Diligence
PwC Luxembourg
+352 49 48 48 5687
birgit.goldak@lu.pwc.com

Tax

Murielle Filipucci
Partner
PwC Luxembourg
+352 49 48 48 3118
murielle.filipucci@lu.pwc.com

Notes

About the survey

PwC's 2018 Global Economic Crime and Fraud Survey was completed by 7,228 respondents from 123 territories. Of the total number of respondents, 52% were senior executives of their respective organisations, 42% represented publicly-listed companies and 55% represented organisations with more than 1,000 employees.

www.pwc.lu/financial-crime