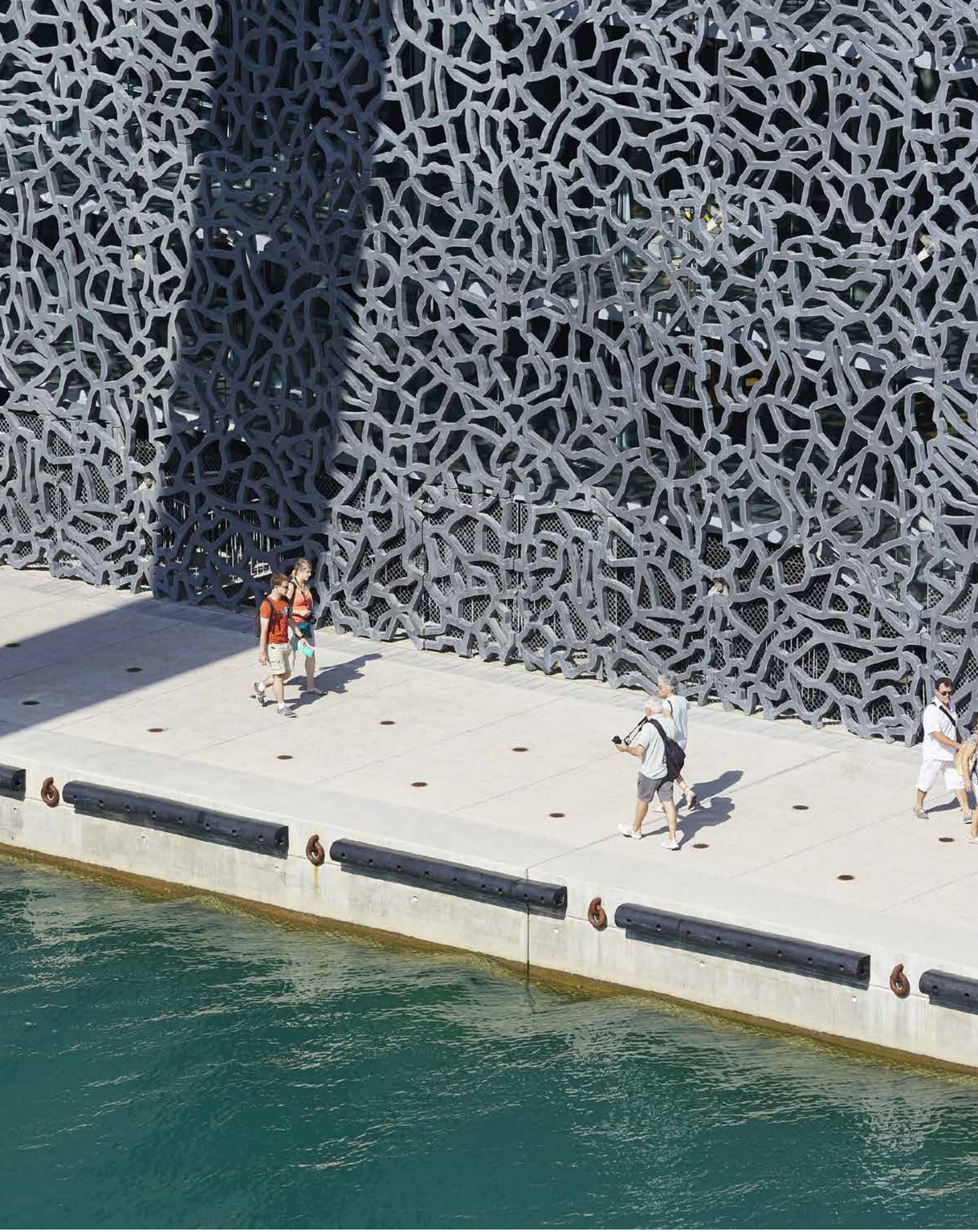
Global Economic Crime Survey 2016
Luxembourg Report

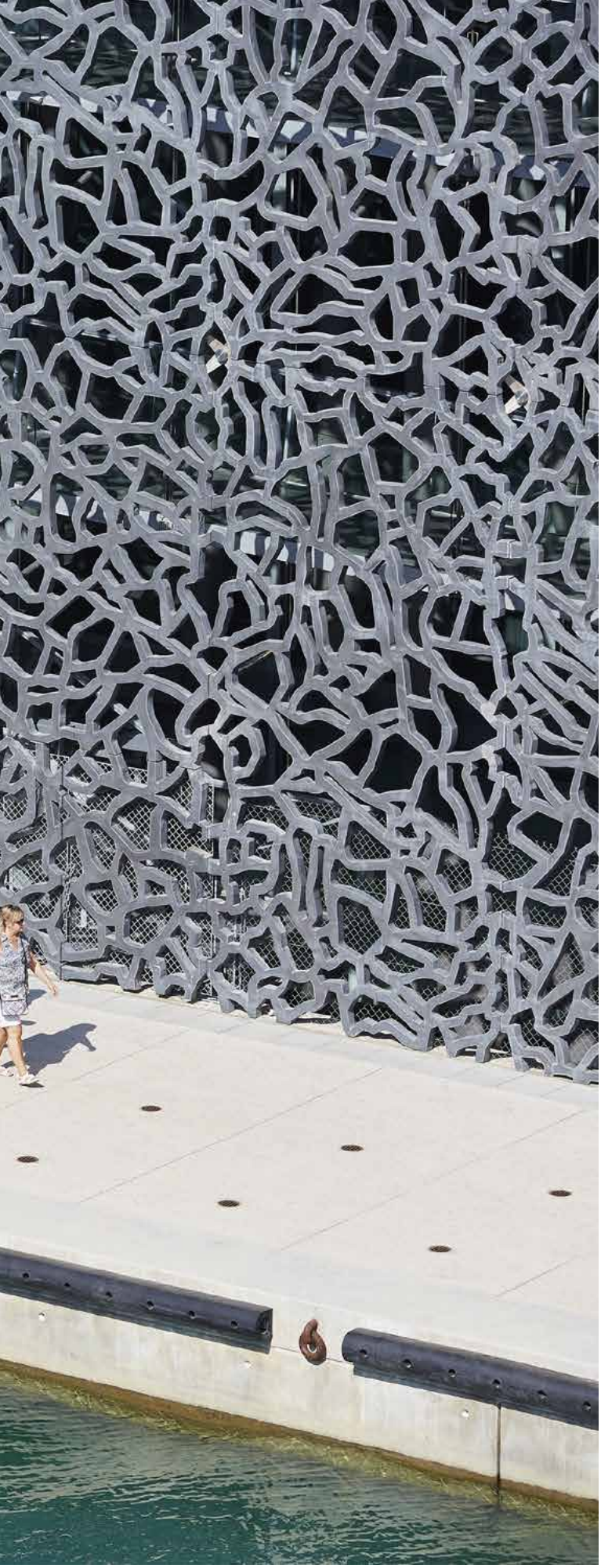
Economic Crime Threats in Luxembourg

The risks of the unknown

pwc

www.pwc.lu/forensic-services





Contents

Foreword

Michael Weis
Partner, Forensic Services &
Financial Crime Leader

Economic crime continues to be a dominant item on the business agenda and no industry sector, region or size of business is immune. As business operations develop new complexities so too do the ways in which criminals can infiltrate our systems. Now, more than ever before, both in Luxembourg and around the world, it is essential to understand the threats that companies face and to proactively protect against them.

The PwC 2016 Global Economic Crime Survey provides insight into the issues faced by businesses today. With more than 6,000 respondents from around the world, the survey provides a detailed picture of how financial criminals operate and how companies are responding to them. In 2016 we are proud to also be able to provide a specifically Luxembourg perspective due to the overwhelming increase in responses from our local market players. The majority of Luxembourg participants in the survey are from the financial services sector, in particular asset management organisations. 42% of these Luxembourg companies have experienced financial crime in the past 24 months – a result significantly higher than the global average – our report will provide vital information for those looking to understand the threats they face.

The 2016 Global Economic Crime Survey demonstrates that cyber-crime, money laundering and asset misappropriation remain significant concerns for all organisations. Instances of cyber-crime in particular continue to increase in frequency around the world and are a key concern for Luxembourg companies.

Regulatory scrutiny means that for Luxembourg companies money laundering is, and remains, also a major topical issue. The maturity of the Luxembourg Anti Money Laundering regulatory framework means that not only do local businesses have a strong awareness of money laundering risks but also a significant number of specialist staff. The survey indicates that this asset will continue to be important for Luxembourg as a major financial centre.

Alongside the global report, this Luxembourg-focused lens provides both data and analysis that will help you assess the risks to which your business is exposed. The combined results from Luxembourg respondents and global participants will allow you to position your risk exposure in the global context. This is crucial to a country with many multi-jurisdictional organisations such as Luxembourg. Should you require further details or explanation, our financial crime team on the ground in Luxembourg 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.

Economic Crime

A significant threat in Luxembourg

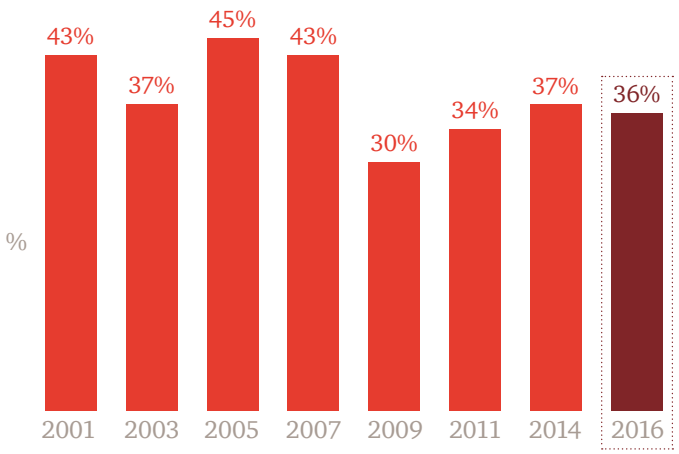
2016: Economic crime evolving

42% of Luxembourg organisations have experienced economic crime in the past 24 months. In a market dominated by the Financial Service industry this is perhaps not surprising since Financial Services companies have been the target of several high profile cases in recent years.

> *Notorious bank robber from the 1950s*
> *Willie Sutton*
> *"Reporter: Why do you rob banks?*
> *Willie Sutton: Because that is where the money is."*

The global rate of reported economic crime has been steadily increasing since 2009. However, this year's results show a slight decrease in the incidence criminal activity for the first time since the global financial crisis of 2008-9 (albeit marginally by 1%).

Fig 1: Global economic crime trend



One in ten economic crimes are discovered by accident.

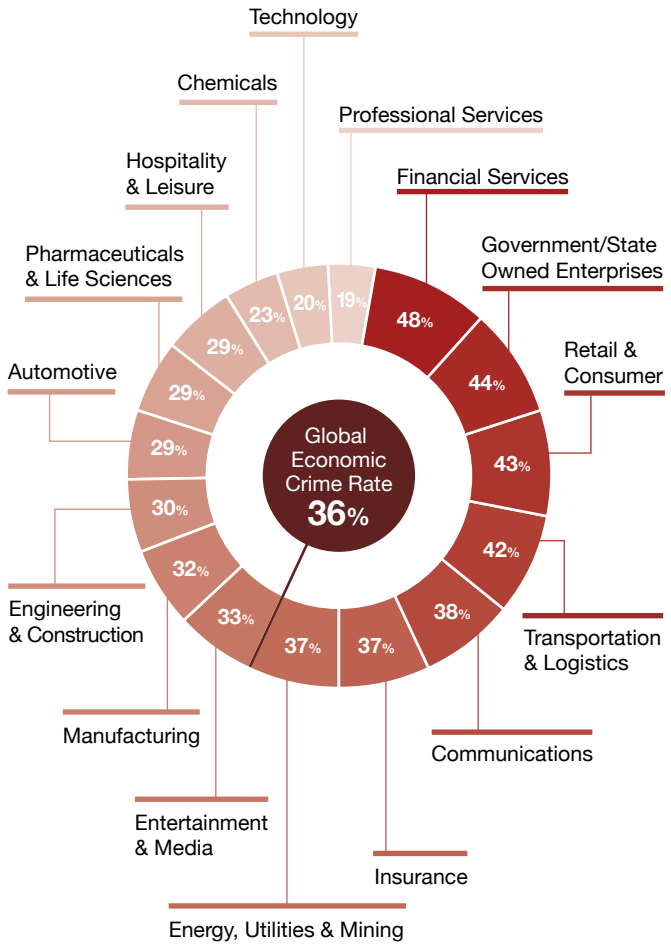
At first glance, this could look like a return on the investments in preventive measures that organisations have been making over the past few years. However, as we look at the global data more closely, we suggest this small decrease is actually masking a worrying trend - that economic crime is changing significantly, but detection and controls programmes are not keeping up with the pace of change. What's more, the financial cost of each fraud is on the rise globally.

Despite this evolving threat, we have seen a decrease in the detection of criminal activity through methods within management's control, with detection through corporate controls down by 7%. In addition, one in five organisations (22%) haven't carried out a single fraud risk assessment in the last 24 months. Considering the findings in PwC's 19th Annual Global CEO Survey - where two-thirds of chief executives agreed that there are more threats to the growth of their company than ever before - this points to a potentially worrying trend, where too much is being left to chance. In fact, our findings indicate that one in ten economic crimes are discovered by accident.

A passive approach to detecting and preventing economic crime is a recipe for disaster. To highlight this fact, our survey uncovered a widespread lack of confidence in local law enforcement - a phenomenon that goes beyond regions or levels of economic burden.

The message is clear: the burden of preventing, protecting and responding to economic crime rests firmly with organisations themselves.

Fig 2: Which industries are at risk?



The Luxembourg results of 42% are above the global average, probably because the highly exposed Financial Services industry represents the largest part of the country's economy. The global results show, however, that many of the non-FS organisations and companies are also likely to be victims of economic crime. There are few reasons to believe that, in Luxembourg these industries would be less exposed than at global level.

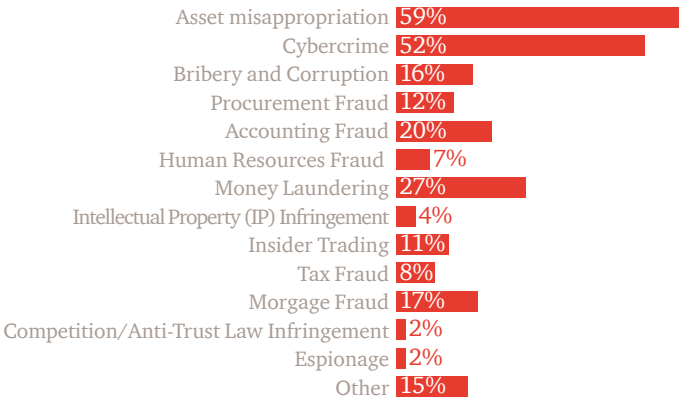
Types of fraud

The most pervasive economic crimes reported by global respondents for 2016 are highlighted in the figure below:

Fig 3: Top 3 most commonly reported types of economic crime in 2016

For Financial Services organisations, asset misappropriation is currently the most common form of economic crime experienced. This is not surprising for a sector processing money and given the low cost of conversion for fraudsters.

Fig 4: Most commonly reported types of economic crime by the Financial Services industry in 2016

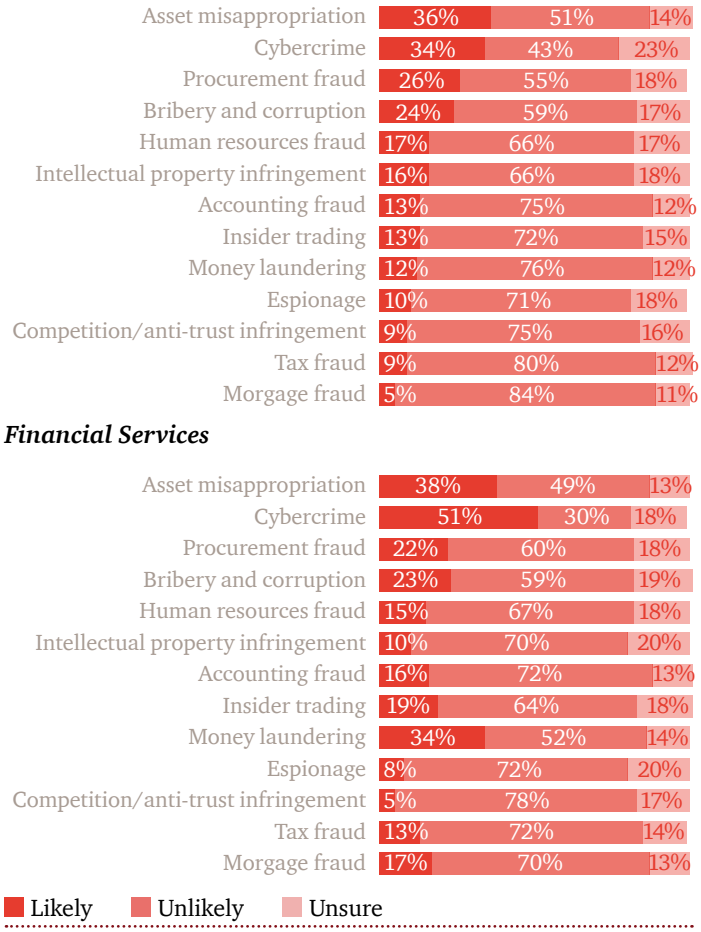


The non-FS and the FS sectors have different results for the prevalence of financial crime and the types of fraud likely to be experienced in the near future, as shown below. These inconsistencies are due to the particularities of the FS sector and are true for Luxembourg, too. For Financial Services, cybercrime seems to be the biggest area of concern looking forward, followed closely by asset misappropriation and money laundering.

"The importance of Anti-Corruption and Anti-Bribery frameworks should not be underestimated for organisations with international counterparts. Awareness and training of staff is a crucial element of effective compliance programs"

Karl Heinz DICK
Chief Financial and Administrative Officer
Luxembourg Institute of Health

Fig 5: Reported likelihood of economic crimes in the next 24 months



From a Luxembourg perspective, cybercrime and money laundering are certainly top of the agenda, as the recent study of ILA and PwC has revealed[1]. Money laundering is a topic already receiving significant attention locally, from various angles, including a very strong regulatory framework, and is therefore considered "under control". This is less true for cybercrime, where the risk awareness is not yet as widespread, although gaining in traction. The growing interest in corporate espionage and IP theft provide evidence of this.

It's interesting to note that classical crimes like bribery and corruption score very low in Luxembourg, compared to the global results. The threat of these issues would appear to be underestimated, since bribery and corruption qualify as primary offences for money laundering and, consequently, could indirectly become very relevant for Financial Services institutions. We see this in recent scandals, where Financial Services organisations suddenly face allegations of money laundering by processing bribes or other corrupt payments of formerly reputable organisations through their accounts. This illustrates a key feature of money laundering - it is a secondary crime. From an FS perspective, each crime in the above list qualifies as a primary offence, which makes money laundering a top concern for financial institutions.

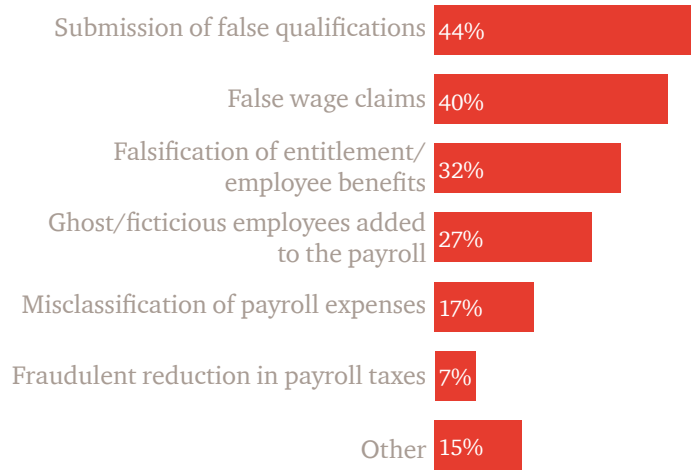
Given the prevalence of asset misappropriation, it's perhaps surprising that only 23% of Luxembourg respondents expect this to be an issue in the next 24 months. Conversely, significantly higher proportions of Luxembourg companies expect to be the victim of cybercrime (57%) and money laundering (39%).

Asset misappropriation has traditionally been regarded as the easiest type of fraud to detect. In Luxembourg however, it would appear to be one of the least anticipated, with cybercrime and money laundering holding the top positions. The heightened awareness of these two crimes could be related to their profile in the media. Since asset misappropriation doesn't garner as much press coverage, it is not as high on management's agenda.

Looking at the overall results for financial institutions, Luxembourg companies' expectations on the likelihood of asset misappropriation incidents is a bit optimistic. Therefore, we would advise Luxembourg-based organisations 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] "Luxembourg Fund Governance Survey 2014", PwC Luxembourg and Institut Luxembourgeois des Administrateurs, January 2015

Fig 6: Most commonly reported types of human resources fraud globally

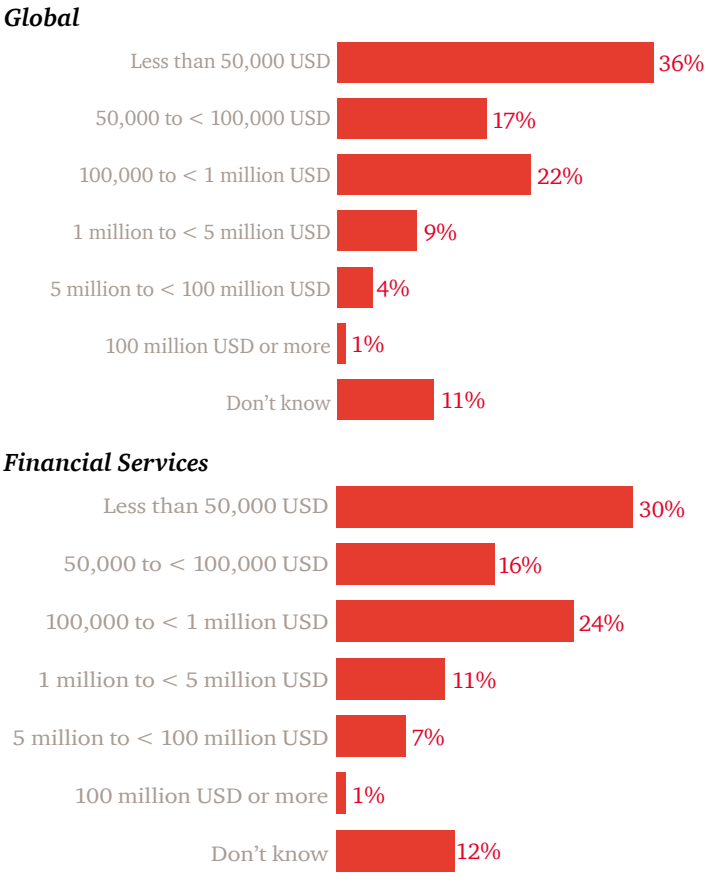


Human Resources fraud has been creeping up the agenda since the last survey introduced it as a stand-alone category in 2014. Most fraud risk assessments focus on external parties and vendors, but the internal threat should never be underestimated. Although not necessarily the cause of direct financial impact, the submission of false qualifications is increasing and often remains undetected, since few companies in Luxembourg perform systematic employee screening.

Impact of economic crime

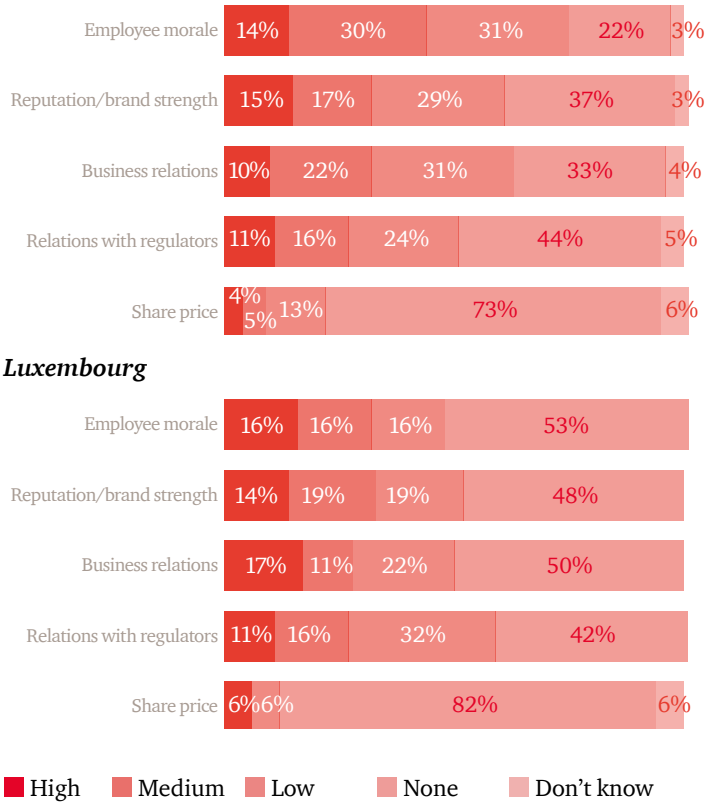
The financial impact of economic crime includes not only direct losses, but also, for example, the costs of remediation and mitigation. 35% of the participants in the global survey suffered costs between USD 100,000 and USD 100 million, with 42% of the FS sector experiencing similar levels of loss. From our Luxembourg experience, FS sector clients suffer significant financial losses from a small number of crimes or incidences of misconduct, while the non-FS sector has a greater number of incidences, but with a smaller impact.

Fig 7: Financial losses due to economic crime in the last 24 months.



When analysing the broader impact of economic crime on organisations, 53% of Luxembourg companies consider that it doesn't affect employee morale, compared to only 22% globally. Business relations are perceived as similarly less relevant in Luxembourg, with 50% of respondents claiming no impact, compared to only 33% globally. By contrast, differences in share price and relations with the regulator seem slightly more important in Luxembourg than at global level.

Fig 8: Impact of economic crime on business operations over the last 24 months

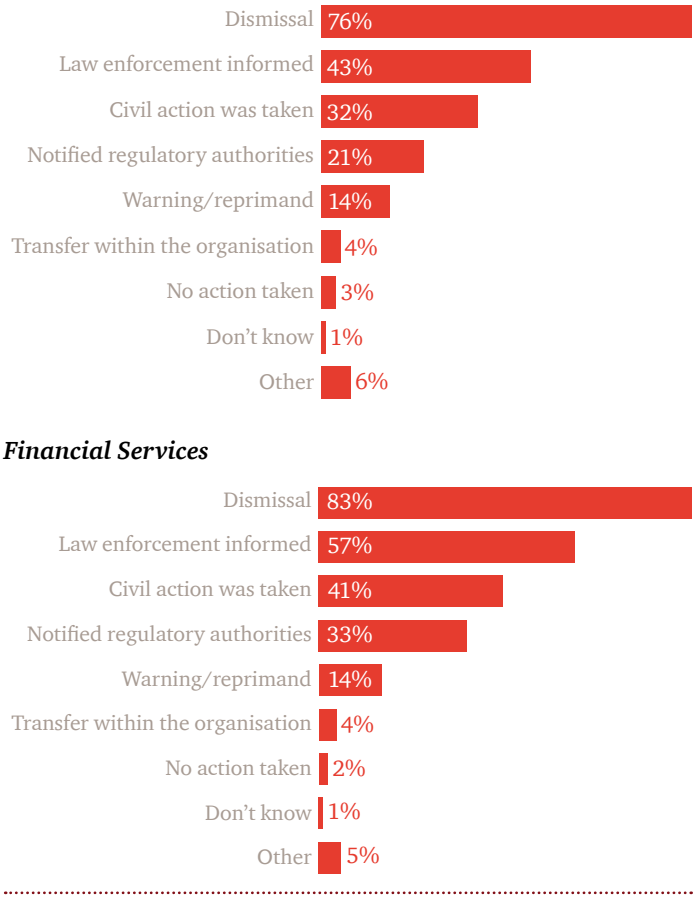


Employee morale is difficult to measure, but the low impact perception might be linked to the fact that Luxembourg has traditionally had fewer publicised incidences of economic crime than other countries. For the same reason, economic crime is perceived to have a smaller impact on business relationships in general. Furthermore, the importance of cross-border business for a small national market like Luxembourg is a key factor. Foreign customers can easily decide to do business elsewhere and are therefore likely to consider factual and objective criteria when choosing a company in Luxembourg. They tend to be less influenced by a company's potential economic crime record locally, if any.

The fraudsters, detection methods and investigators

The "enemy within" continues to be the biggest threat globally with 46% of reported economic crimes committed by internal actors compared to 41% by external actors. Inside jobs usually result in the biggest financial impact, as many historical cases prove (e.g. rogue trader cases). The bigger risk lies in the fact that an insider knows exactly how a company works and what weaknesses to exploit. Opportunity is the important factor here, and it means that internal controls might not be robust enough to prevent fraud.

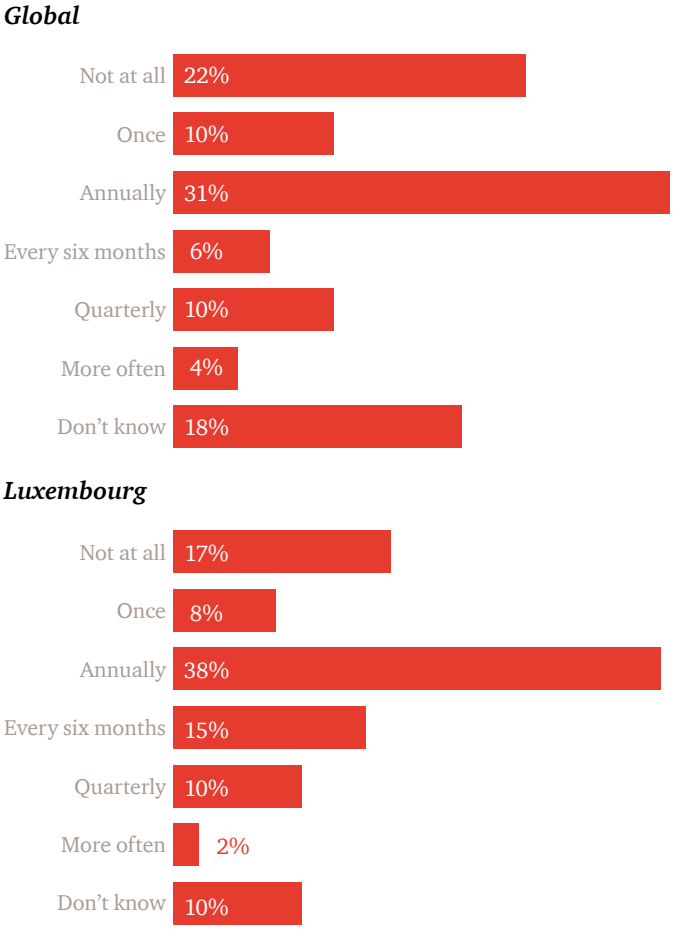
Fig 9: Reported actions taken against internal perpetrators by organisations



Legal actions taken against internal perpetrators are more severe in FS sector organisations. Such deliberate actions are likely connected to the strong regulatory oversight. Most companies in the non-FS sector often simply dismiss the rogue employee since no supervising regulator expects further actions, and thus avoid the publicity or other implications of a legal case.

Although no specific statistics are available for Luxembourg, global evidence suggests that incidents of economic crime committed by internal actors increasingly result in legal action and the involvement of law enforcement. Furthermore, key stakeholders such as regulators or shareholders are increasingly expecting such actions.

Fig 10: Reported frequency of fraud risk assessments



Luxembourg respondents have only reported economic crimes perpetrated by external actors. This situation not only seems very unlikely, but our experience doesn't support it. The fact that crimes committed by internal perpetrators are not commonly discovered indicates potential weaknesses in the internal controls designed to detect them. This is further supported by the fact that 17% of Luxembourg based respondents have never carried out a fraud risk assessment and a further 38% only carry out such an assessment annually. The main problem here is the lack of risk awareness. When "you don't know what you don't know", fraud can go undetected for quite a while and it remains unclear how sophisticated fraud risk assessments are when they are not formally required.

Luxembourg has already seen cases of the "bank in the bank" scenario, where rogue employees were maintaining their own "accounts" for customers, who were not aware of this fake set-up. Under certain conditions, such cases can go undetected for years. The mere fact that an organisation hasn't yet discovered an internally perpetrated fraud, shouldn't lead it to believe it will never happen. A lack of risk awareness and related control weaknesses create opportunities and, if the right circumstances overlap, employees will potentially commit fraud. It is not a question of "if", but a question of "when." Cybercrimes are most often externally perpetrated, not only for monetary gains but also for valuable information about individuals and companies, whereas asset misappropriation is more likely to be perpetrated by an internal agent. Low expectations regarding the risk of asset misappropriation and a low detection level for internal fraud are therefore likely to be linked.

Most likely characteristics of internal fraudster

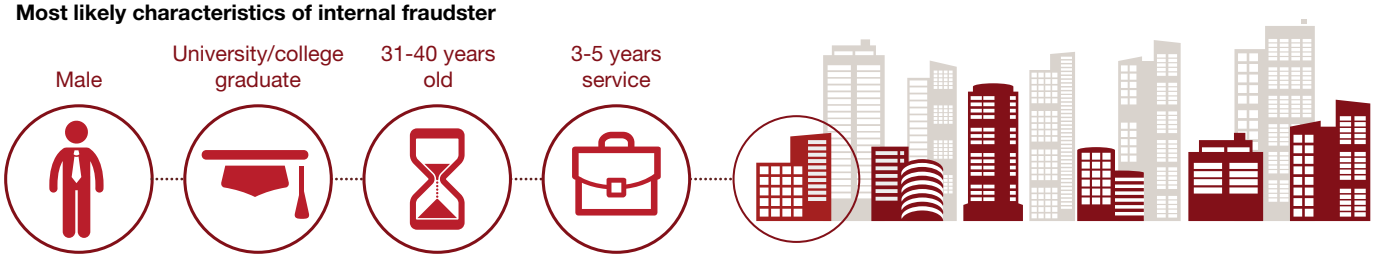
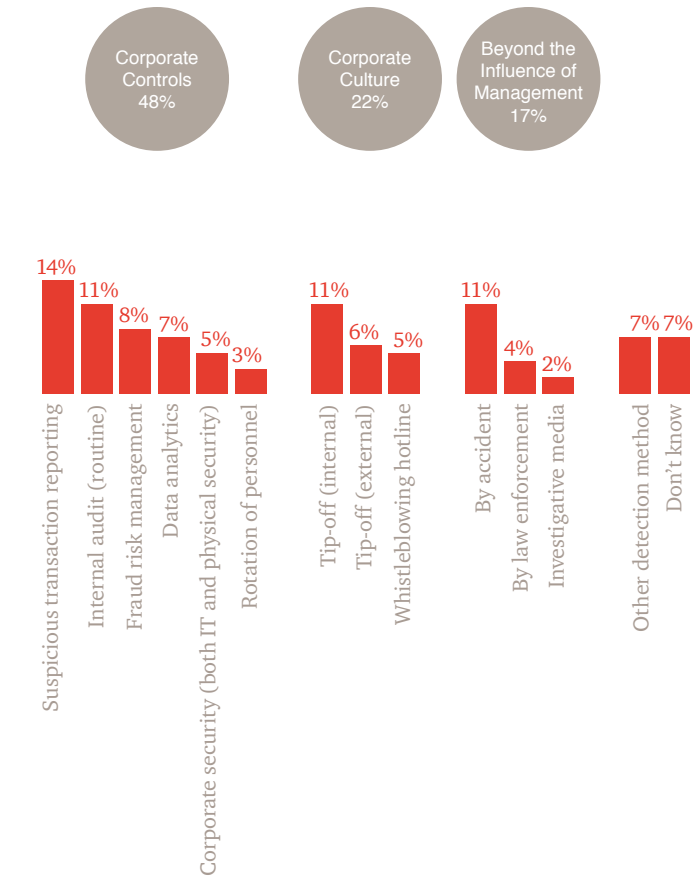
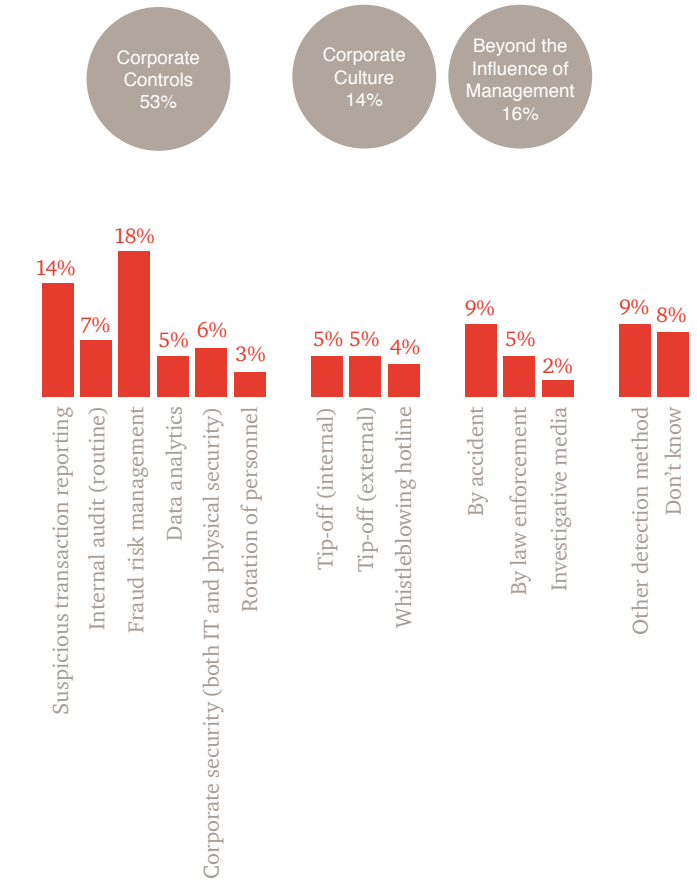


Fig 11: How economic crimes were detected globally across all organisations and in the Financial Services industry





Our survey results identify some very interesting distinctions between FS and non-FS industries when it comes to financial crime detection. Fraud risk assessments have become more pertinent and effective for FS organisations since global regulatory obligations have made them more sophisticated and often mandatory. This is not (yet) the case for the Luxembourg FS industry, as risk assessments rather focus on AML related issues. However since AML and fraud are closely linked, best practice AML risk assessments increasingly include in addition fraud related risks.

Conversely, respondents seem to consider data analytics less effective for FS 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 can improve crime prevention results and should always be considered.

Much of the recent debates around misconduct, following numerous FS scandals like LIBOR and others, have featured the compliance culture of organisations. It is therefore surprising that the FS sector only detected 14% of crimes through tip-offs or whistle-blowers, while for non-FS industries these account for 23%. It seems there is still a long way to go for the FS industry in relation to corporate ethics.

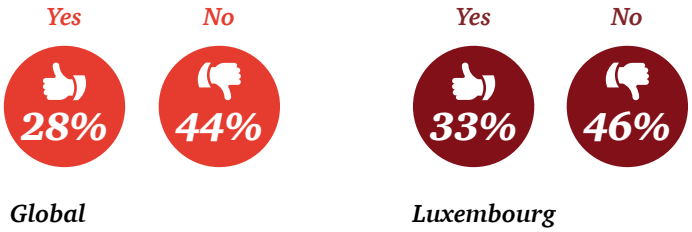
Considering the limited number of identified internal perpetrators, it seems Luxembourg companies trust their employees, a fact also confirmed through discussions with our clients. However, when a potential fraud is detected, Luxembourg companies are less likely to use internal resources to carry out an investigation - 57% compared to 72% globally. They prefer using the organisation's auditor, external legal advisors or specialised forensic investigators to make sure they get the right professional expertise. These results suggest that despite the relatively strict regulatory environment in which they operate, many companies don't have enough resources to detect, or to investigate economic crime, especially when internal investigations have to be performed.

Fig 12: Actions taken when incidents of potential fraud are identified

Perception of law enforcement

This year, the Global Economic Crime Survey also asked respondents to comment on whether they believed local law enforcement authorities are adequately resourced and trained to investigate and prosecute economic crime. The global response was overwhelmingly negative, showing organisations' limited trust in the expertise and resources of these agencies. Economic crime is often of complex technical nature and incurs specific aspects of accounting, tax or commercial law that are not always straightforward and require specialist knowledge in often under-equipped law enforcement organisations. Luxembourg law enforcement capabilities were rated higher than the global average.

Fig 13: Perception of law enforcement



Luxembourg ranks fifth among countries with low levels of confidence in the ability of local law enforcement to deal with cybercrime, with the UK and US only performing marginally better. The market perception is not positive even if it is better than the global average. However, the local police force has created a dedicated team of technology specialists to deal with such cases. An example of the concerted focus on cybercrime in Luxembourg is the government led initiative CIRCL (Computer Incident Response Centre Luxembourg) which provides interesting statistics on the trends.

The results suggest that global law enforcement agencies should continue to expand their expertise and resources and communicate more directly with the industry about their efforts to combat and investigate financial crimes.

Fig 14: Top ten countries that indicated no confidence in local law enforcement's ability to investigate cybercrime

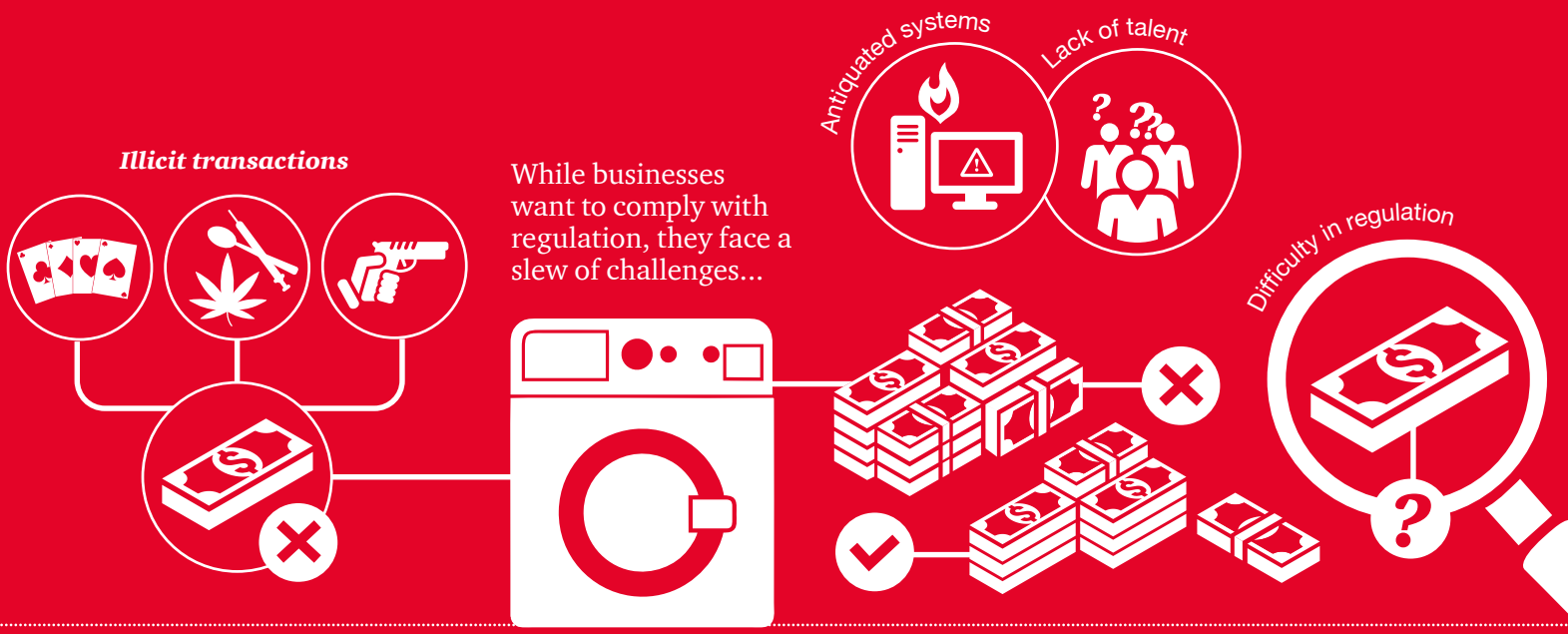
1	Kenya	**73%**
2	South Africa	**70%**
3	Zambia	**67%**
4	Nigeria	**62%**
5	Luxembourg	**59%**
6	United States	**58%**
7	Ukraine	**57%**
8	United Kingdom	**57%**
9	Mexico	**57%**
10	Turkey	**56%**

Luxembourg companies increasingly turn to external accounting and legal advisors to make their case, especially when there are no legal obligations to escalate incidences to the authorities. In a fast-paced, fast-changing world, these advisors, particularly in forensic technology, will be increasingly called upon in cases of economic crime.

What can you do?

- Assess your organisation's culture and management style and the adequacy of systems and monitoring controls.
- Review and challenge the existing risk spectrum to ensure a common, comprehensive agreed approach across your organisation.
- Implement processes to identify red flags for economic crime, as well as a set of methods for a robust investigation in case of a fraud.
- Last, but not least awareness is a key factor. Only organisations that acknowledge that they might be a target can effectively fight against such threats.

Anti-Money Laundering



Money Laundering destroys value

The global focus on Anti-Money Laundering (AML) and Counter Terrorist Financing (CTF) is understandable in light of increasing terrorist menaces. The reputational threat, as well as increasing fines make it crucial to set up and maintain cost-efficient AML/CTF compliance measures and solutions.

Money laundering destroys value. It facilitates economic crime and nefarious activities such as corruption, terrorism, tax evasion, as well as drug and human trafficking, by holding or transferring the funds necessary to commit these crimes. It can be detrimental to an organisation's reputation - and its bottom line.

Global money-laundering transactions were estimated at 2 to 5% of global GDP, or roughly USD 1-2 trillion annually. Yet, according to the United Nations Office on Drugs and Crime (UNODC)[2], authorities currently seize less than 1% of global illicit financial flows.

With the rising visibility of terrorist attacks, money laundering and terrorist financing become top priorities for governments across the globe. Over the last few years, in the U.S. alone, nearly a dozen global financial institutions received fines amounting to billions of dollars for money laundering and/or sanctions violations. There are strong indications that other countries will follow in substantive regulation and enforcement, like the UK for instance.

This issue doesn't only concern Financial Services institutions. Any organisation that facilitates financial transactions - including non-bank money service businesses such as digital/mobile payment services, life insurers and retailers, to name a few - are also coming within the scope of Anti-Money Laundering legislation worldwide. Alarmingly, but not surprisingly, many of these new participants are not yet up to speed with the requirements they must meet or on the compliance programmes they need.

As regulation deepens in complexity and scope, the cost of compliance continues to rise. According to new figures from WealthInsight[3], global spending on AML compliance is set to grow to more than USD 8 billion by 2017 (a compounded annual growth rate of almost 9%). However, many balk at the increasing compliance spending - notwithstanding the cost of enforcement actions and large-scale penalties resulting from compliance failures.

Pace of regulatory change

Local and global regulatory regimes are active in the face of these growing threats and enforcement actions are increasingly punitive and challenging. Our survey results show that the pace of regulatory change is the largest concern for our global and local respondents. Nearly a third of Luxembourg organisations (29%) named regulatory changes as their primary concern. A further quarter of respondents cited the complications of complying with the AML requirements of multiple jurisdictions. The multi-jurisdictional concern is obvious, when looking at the international scale of business done from Luxembourg. As a global cross-border distribution centre for investment funds, companies have to deal with multiple jurisdictions and, implicitly, their requirements. This is also applicable for the banking industry in general, since cross-border transactions are the norm in Luxembourg, compared to large domestic markets like in the USA. This international exposure obviously increases the complexity of regulatory obligations for local actors, especially when compared to more domestic focussed businesses.

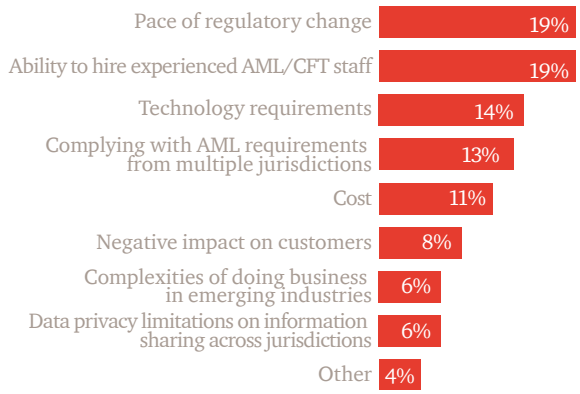
It's not the regulatory compliance itself that is most problematic, but the differences between jurisdictions and the ever-changing nature of regulation. One of the key risks in this respect is the extraterritorial reach that organisations face from US regulations such as OFAC (Office of Foreign Asset Control) or related regulations for the FS industry like the BSA (Banking Secrecy Act). Financial Services organisations falling in the scope of OFAC often experience pressure relating to AML/CTF regulations as well.

[2] "Estimating illicit financial flows resulting from drug trafficking and other transnational organized crimes", United Nations Office on Drugs and Crime, October 2011

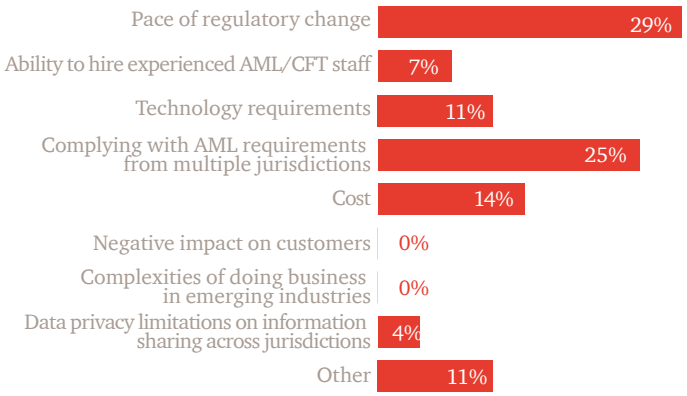
[3] "2020 Foresight Report: The Impact of Anti-Money Laundering Regulations on Wealth Management", WealthInsight Ltd, July 2013

Fig 15: Reported challenges in relation to AML/CFT requirements

Global



Luxembourg



Certain governments have imposed fines - and in some cases, pursued criminal actions - against financial institutions that haven't implemented sufficient controls to monitor their global transactions. More recently, these same governments have reiterated the need to pursue individual criminal prosecution in addition to the corporate fines and settlements they have imposed. In short, they are looking for personal responsibilities around these failings. The days when individuals were protected by corporate settlements will soon be gone. They already face potential jail time if they are found to be complicit in illicit business practices or even for substantive compliance failures.

Some financial institutions have already come into the crosshairs of regulators in one country for illicit business practiced in another. Questions often arise as to which country institutions are allowed to transact in, while sanctioned by other countries.

Inspections and remediation are on the rise

As FS organisations grow by acquisition (as many have done of late), their legal vehicles, businesses and markets are not immediately consolidated into group processes or standards. Many still struggle in the aftermath of regulatory actions or sanctions. All of these factors increase the risk profile for AML enforcements. Our survey indicates that globally 18% of banks have recently experienced enforcement actions by a regulator.

The market participants in Luxembourg are keenly aware that a strong risk assessment and corresponding risk based approach are the basis for effective AML processes. This is significantly above the global average for the FS industry and clearly demonstrates the maturity of the Luxembourg regulatory framework on AML. The 4th EU Anti-Money Laundering Directive adds further requirements particularly on risk assessment. For example, in line with FATF recommendations issued in February 2012, rules on customer due diligence are refined and may vary depending of the risk: enhanced vigilance where the risks are greater, simplified measures where risks are lower. The Luxembourg regulation CSSF 12-02 has already implemented most of the FATF recommendations in this respect, confirming the appropriate standard of AML regulation in Luxembourg.

4th Anti-Money Laundering directive

The Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC has been published on 5 June 2015. This publication ends a legislative process initiated in February 2013 with two Commission proposals aiming at strengthening EU rules on Anti-Money Laundering and terrorism financing by taking into account the 2012 Recommendations of the Financial Action Task Force (FATF). The 4th AMLD publication also comes with a revamped Regulation (EU) 2015/847 on information accompanying transfers of funds as part of a single "package".

What's in it?

- Focus on risk assessment and corresponding risk based approach;
- Increased transparency through creation of beneficial owners' national central registers;
- Supra national and national risk assessment;
- Tax crimes now within predicate offences;
- Extension of scope to the whole gambling sector;
- Customer due diligence waiver for certain e-money products;
- Third country policy.

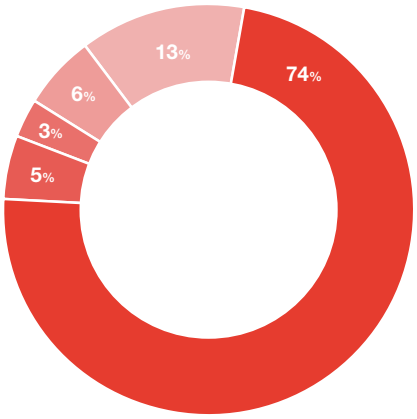
Who does it impact?

The Directive is applicable to all "obliged entities" as defined in Art. 2.1 of the Directive, i.e.:

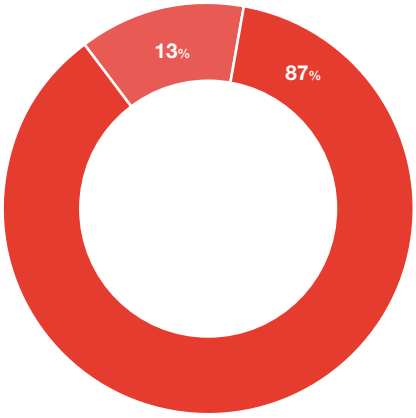
- Credit institutions;
- Financial institutions;
- Auditors, external accountants and tax advisors;
- Notaries and other independent legal professionals (under specific conditions);
- Trusts or company service providers;
- Estate agents;
- Traders in goods making or receiving payments above EUR 10,000;
- Providers of gambling services.

Fig 16: Frequency of AML/CFT risk assessments reported by organisations

Global



Luxembourg



The 4th AMLD contains explicit lists of risk factors to be taken into consideration by entities when performing their internal risk assessment and in particular determining application of simplified or enhanced due diligence measures. The European Supervisory Authorities (i.e. EBA, EIOPA and ESMA) will release more guidelines in this area by 26 June 2017.

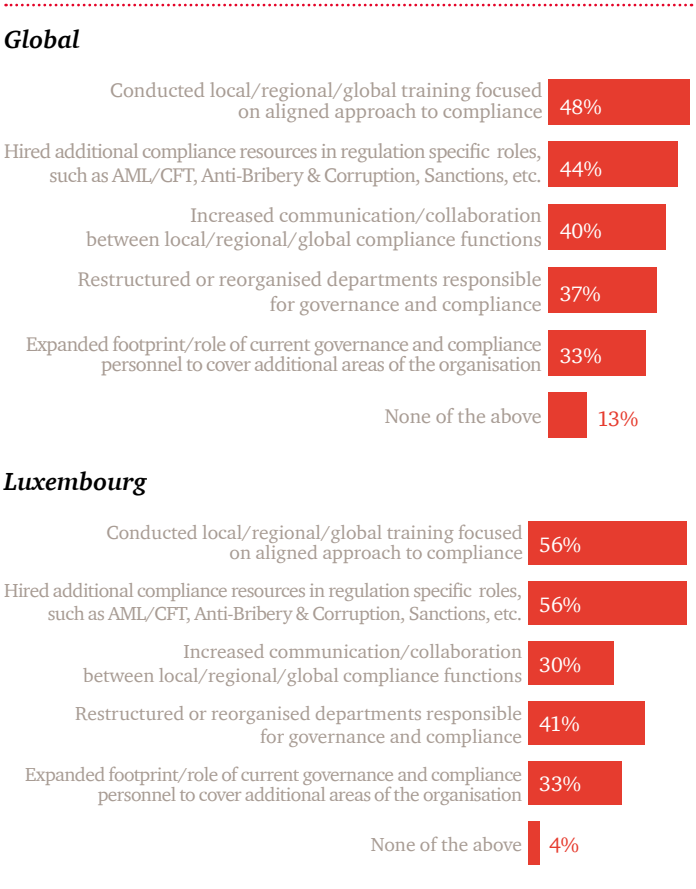
The high level of local regulatory standards doesn't mean that Luxembourg financial institutions are being, or can be, complacent. With regulations changing all the time, organisations must continually review and update their AML compliance procedures. Global compliance is not just a matter of following the laws of a single jurisdiction. The regulatory frameworks of the major financial centres - e.g. Hong Kong, Singapore, London and New York - are converging, requiring institutions to incorporate the highest standards, both internationally and in their home jurisdictions by acting global and complying locally.

The lower response rate for collaboration with compliance functions in Luxembourg compared to other countries might be explained by the importance and strict requirements of the banking secrecy traditionally applied in the Grand Duchy. Although regulatory obligations always allowed the collaboration with group wide compliance functions under certain conditions, local market players often chose to increase and focus on their local capabilities rather than simply relying and outsourcing to group functions.

From a more global perspective, another challenge for organisations wrestling with global AML/CFT compliance is that regulatory expectations are increasingly replacing clear legal requirements. This is most prominent in the areas of customer due diligence and transaction monitoring, where examiners may apply a standard on one institution based on the practices of another. This so-called "regulation by examination" challenges the well-known risk-based approach concept that organisations and their stakeholders are expected to apply.

In response to increased regulatory pressure on the Financial Services industry, respondents in Luxembourg appear to have reacted similarly to their global peers. However, less than one third of the Luxembourg respondents (30%) increased their communication and collaboration with the regional and global compliance functions and by far preferred to conduct training (56%) as well as recruit additional resources to re-inforce their compliance function (56%).

Fig 17: People measures introduced to address increased regulatory expectations



Monitoring and controls

The Luxembourg investment fund and banking industries operate a cross-border business model. Luxembourg has recently introduced specific regulatory requirements currently being implemented in the market. The local market is less concerned with a possible shortage of qualified staff than the global results show, which probably links to the long-term focus on AML compliance and the existing qualification initiatives of the Luxembourg House of Training and other providers like PwC's Academy.

From a Luxembourg perspective, suspicious transaction monitoring through automated tools is not necessarily always the most effective method, according to survey respondents. This procedure strongly depends on the scale and the nature of the transactions. The volume, amount and type of counterparty reviewed differ significantly between retail banking, private banking and investment funds.

Another important aspect is the nature of transactions/counterparties. A simple cross-border transaction might qualify as suspicious or risky from the perspective of financial institutions in large domestic market countries like France or Germany. In Luxembourg however, this is often the standard situation, since the majority of transactions occur cross-border making transaction monitoring scenarios more complex. The local organisations are thus much more alert to the subtleties and challenges of such transactions. Luxembourg financial institutions and compliance professionals are more used to dealing with complex foreign legal structures than the average professional in larger jurisdictions.

The transactions of the investment fund industry often deal with institutional counterparties and global distribution networks. Standard monitoring tools available previously and designed for banks were not always able to address the requirements of these organisations effectively. However, since the Luxembourg regulations have not imposed the use of automated systems in the past, companies were free to use other types of solution as long as they could demonstrate their ability to prevent and detect the money laundering risk appropriately. This is especially the case for smaller market participants, who use internally developed less automated approaches.

Fig 18: Activities implemented globally and in Luxembourg to reduce AML/CFT risks

Today, the CSSF regulation 12/02 requires regulated entities to use automated solutions and only allows non-automated solutions under certain circumstances (e.g. low transaction volumes). From our experience, many players in Luxembourg have implemented state of the art scenario-based and automated transaction monitoring tools. However, the annual CSSF reports still present weaknesses in transaction monitoring processes, so it remains an area of focus.

Over half of the Luxembourg respondents have increased their KYC requirements for certain types of clients (63%) and the controls in place to reduce their AML/CTF risks (67%). In addition, 63% of them have reinforced their compliance monitoring escalation process, and one third have conducted transaction monitoring data validation, reflecting the global trends.

Luxembourg shows a clear focus on increasing controls and their quality assurance, which is significantly above the global results. We can easily say that risk awareness, related controls and the regulatory framework for money laundering and terrorist financing matters are very strong and significantly higher than in peer jurisdictions.

The tools used for the identification of suspicious activity in trade based money laundering are similar for both global and Luxembourg respondents, according to the survey. Specialised analytical procedures are the least utilised methods in the detection of unusual transactions in both cases. Both global and Luxembourg respondents reported increased customer due diligence for sectors identified as risky by their regulators. Survey participants have also performed focused periodic reviews on their identified high-risk clients and this seems to be the preferred monitoring method for the Luxembourg respondents. Periodic reviews performed correctly provide more comfort for Luxembourg respondents over high-risk clients than the one-off customer due diligence used elsewhere.

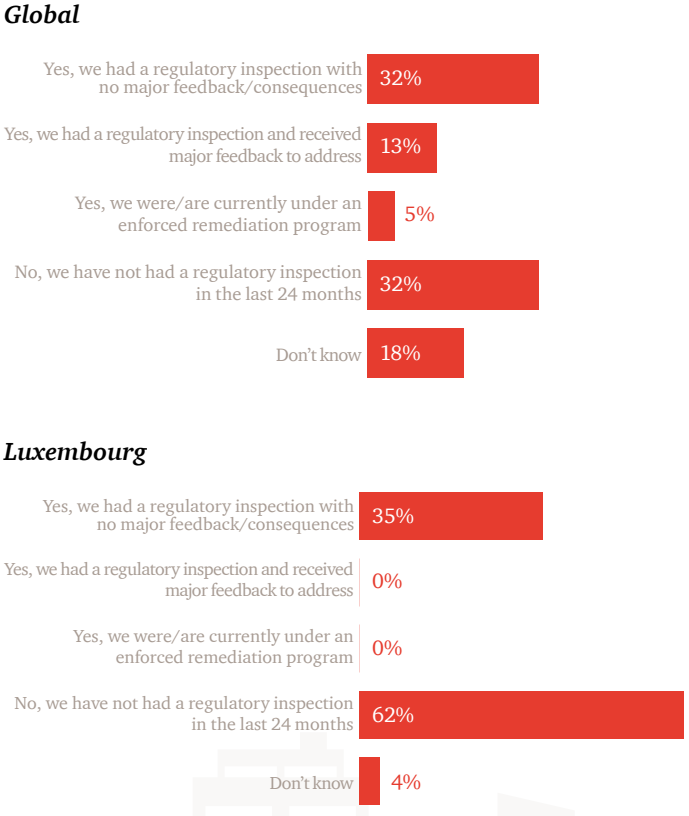
Fig 19: Activities implemented to detect and deter trade based money laundering

	Global	Luxembourg
Increased customer due diligence requirements in industries targeted by regulators for increased scrutiny	*64%*	*52%*
Conducted focussed periodic review of holistic activity for clients involved in high risk businesses or jurisdictions	*43%*	*67%*
Conducted specialised analytics to identify unusual trade practices and/or patterns consistent with undervaluation or over invoicing of goods/services	*40%*	*37%*
Other	*3%*	*4%*
None of the above	*17%*	*11%*

"Luxembourg funds are worldwide leaders in fund distribution and are experienced to deal with complex AML issues. Strict regulations as well in depth technical knowledge by market participants help us meet the challenge."

Enrico Turchi
Managing Director
Conducting Officer
Pioneer Asset Management S.A.

Fig 20: Reported regulatory enforcement / inspections in relation to AML in the last 24 months



Although AML/CTF onsite inspections of CSSF have increased in recent years, 62% of Luxembourg respondents have not had a regulatory inspection in the last 24 months. In addition, none of those respondents that reported having an inspection had major points to address. These responses don't follow the global trend, where only 32% said they had not had an inspection in the last two years and 13% of respondents admitted having had major points to address following the inspection.

Global compliance is not just a matter of following the laws of a single jurisdiction. Regardless the home jurisdiction, organisations should understand that AML/CFT are globally regulated and act accordingly, because:

a) FATF sets international standards for AML/CFT risk management and enforcement. Thus, it forms the basis for national regulations - and the obligations of banks and other regulated institutions.

b) OFAC administer sanctions programmes - and by design focus on the movement of goods, services and funds overseas and across borders. Other countries and organisations such as the EU and Her Majesty's Treasury (HMT) administer similar sanctions programmes.

c) It is almost impossible for financial institutions to avoid the laws of the jurisdictions administering major global currencies such as the U.S. dollar and British Pound. The mere act of clearing a single transaction in the U.S., or with U.S. dollars - or of contacting a person in the U.S. by telephone or email - can be enough to establish nexus and clear the way for prosecutions in the U.S.

Global AML organisations and Regulators

- ***The Financial Action Task Force on Money Laundering (FATF).*** **An inter-governmental policy-making and standard-setting body, whose current mission is to promote policies to combat money laundering and terrorism financing by monitoring global AML and CFT trends, and setting international standards. FATF established "Forty Recommendations" - a global minimum standard for an effective Anti-Money Laundering system, currently adopted by 34 member countries as part of their Anti-Money Laundering regulation and legislation.**
- ***The United Nations Security Council*** **issues resolutions containing inter alia lists of persons against which sanctions have been imposed, such as known terrorist organisations. These lists are often used by participating governments to support measures against terrorist activity.**
- ***The Office of Foreign Assets Control (OFAC),*** **an entity under the U.S. Treasury Department, maintains and administers a number of U.S. economic sanction programmes and embargoes.**

Taken together, from a global perspective, these fast-changing, unpredictable developments can lead to a kind of strategic inertia, as institutions try to predict the future regulatory landscape they will face. In practice, this will translate into a great deal of professional expertise being required to design financial crime compliance programmes.

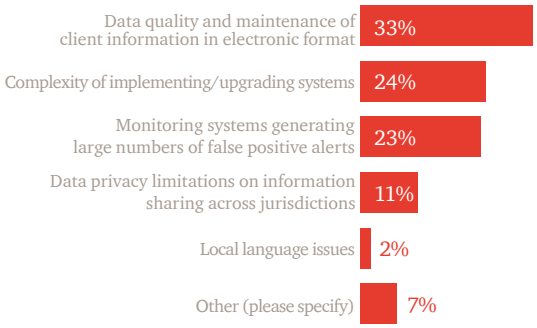
With low impacts of economic crimes on customers and a supply of experienced staff, financial institutions in Luxembourg seem well placed to try and get ahead of the curve going forward. Large FS organisations should keep trying to anticipate upcoming regulatory changes, implement responses to new regulations early and tweak their transaction monitoring tools to ensure that the highest global standards are in place across their organisations. Recent trends demonstrate that global FS organisations have performed or are planning reviews of their AML framework across their group.

Technology

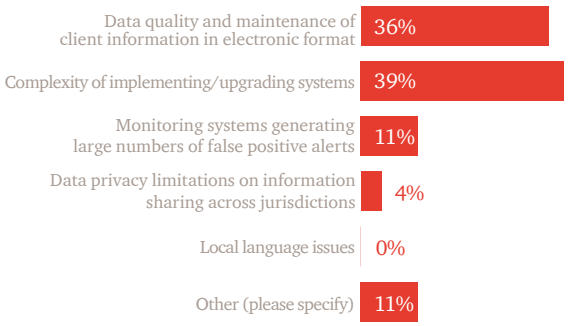
Financial institutions in Luxembourg, as well as those in the rest of the world, rely on AML and CTF systems for the information required to make judgements on potential and existing clients. Technological developments have made the most recent data analytical systems able to facilitate significant efficiency savings and allow for more strategic decision making. While these systems can be costly, older systems can also be burdensome for clients as they require regular upgrades, particularly in the face of a regulatory system that is constantly revolving.

Fig 21: Most significant challenges in relation to AML/CFT systems

Global



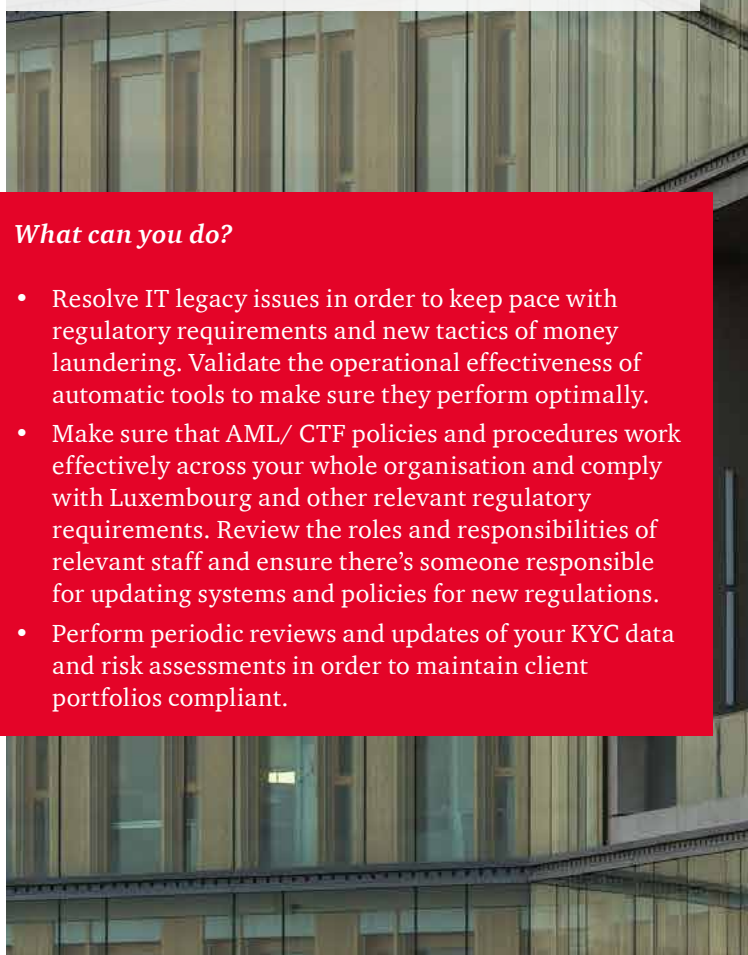
Luxembourg



Indeed, the complexity of maintaining or upgrading their systems is the primary AML technological challenge for Luxembourg FS respondents to our survey (39%). Such systems are, of course, only as good as the underlying data. The survey results prove this, with 36% of respondents listing data quality and the maintenance of client information as a key concern. This is and will continue to be one of the crucial areas for strong AML/CTF systems. Although technology is developing fast Luxembourg respondents report that, legacy systems and their data are the key struggle for large organisations. A robust monitoring system needs to combine and integrate not only transactional data, but also dynamic KYC and risk assessment data on a large scale, which can be challenging.

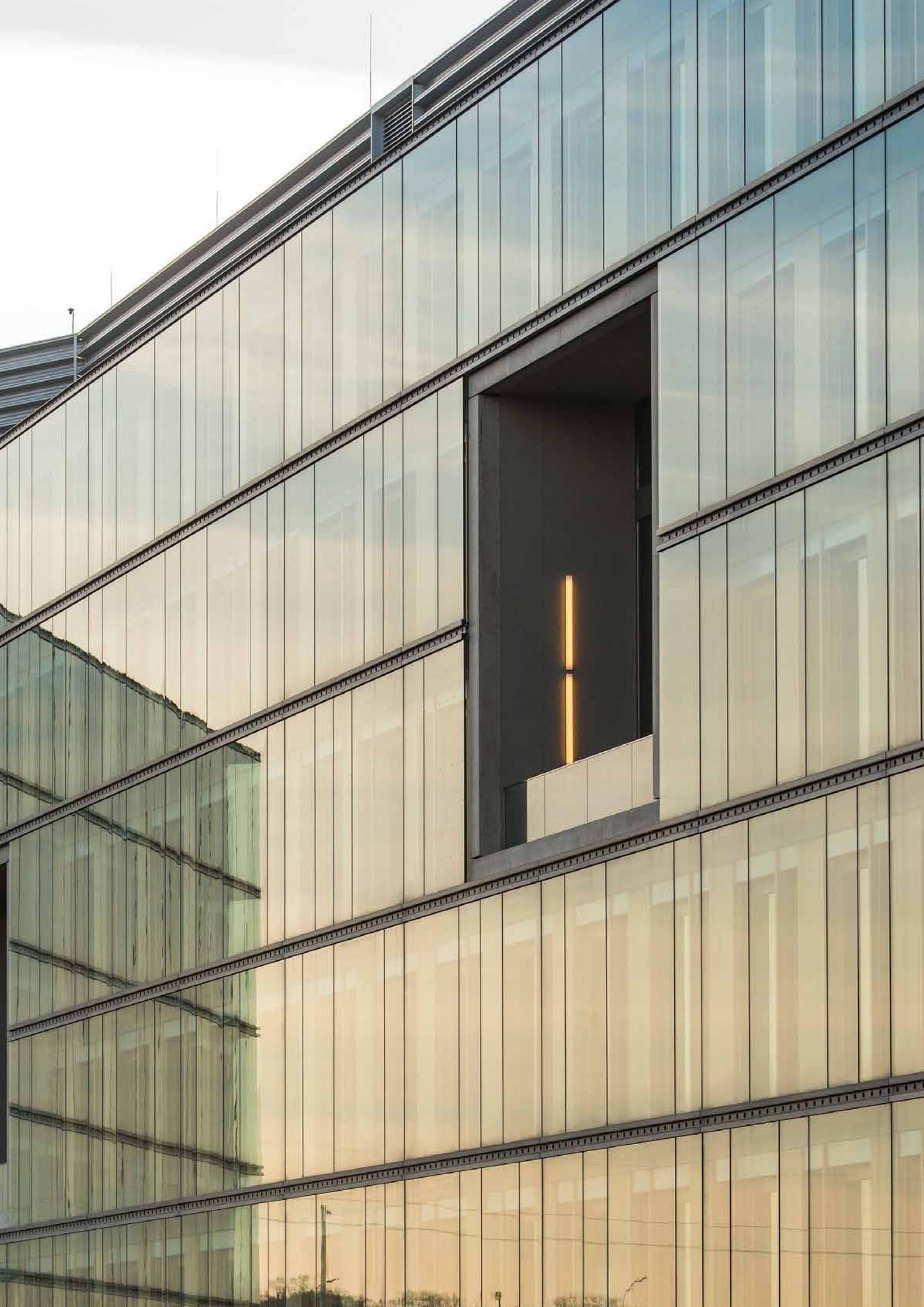
Despite their concerns about maintaining systems and their underlying data, Luxembourg respondents do not seem as worried as global participants about false positives-only 11% listed them as the largest challenge in Luxembourg, compared to 23% globally.

Luxembourg market players utilising cross-border business models are used to dealing with significant volumes of complex data. They understand that mastering the complexity is key to the efficiency and effectiveness of prevention or detection measures for financial crime.



What can you do?

- Resolve IT legacy issues in order to keep pace with regulatory requirements and new tactics of money laundering. Validate the operational effectiveness of automatic tools to make sure they perform optimally.
- Make sure that AML/ CTF policies and procedures work effectively across your whole organisation and comply with Luxembourg and other relevant regulatory requirements. Review the roles and responsibilities of relevant staff and ensure there's someone responsible for updating systems and policies for new regulations.
- Perform periodic reviews and updates of your KYC data and risk assessments in order to maintain client portfolios compliant.



Cybercrime

Although military assets are assumed to be highly secure, hackers have found that low risk suppliers have gaps in their security, which can be easily exploited and used to track the destination of these supplies.

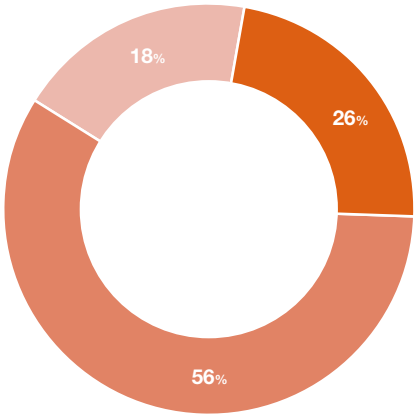
A boundless threat

It is quite remarkable that more than half of Luxembourg respondents report having suffered a cybercrime attack in the last 24 months. Even more remarkable is the fact that 24% of respondents in Luxembourg do not know if they have been affected! Considering the rising number of such attacks, we would expect companies to quickly start investing in cyber-attack identification capabilities. For the 24% who believe they were not affected, the question is whether their basis to say "no" is solid enough - do they have the right processes and tools in place to be so sure? A lack of awareness of where the real risk resides is true not only for cybercrime, but also for economic crime in general. If an organisation has no robust detection and reporting framework, it might already be a victim without knowing it.

> *"There are known knowns. These are things we know that we know. There are known unknowns. That is to say, there are things that we know we don't know. But there are also unknown unknowns. There are things we don't know we don't know."*
>
> **Donald Rumsfeld**
> Former US Secretary of Defence

Fig 22: Organisations affected by cybercrime in the past 24 months

Global



Luxembourg

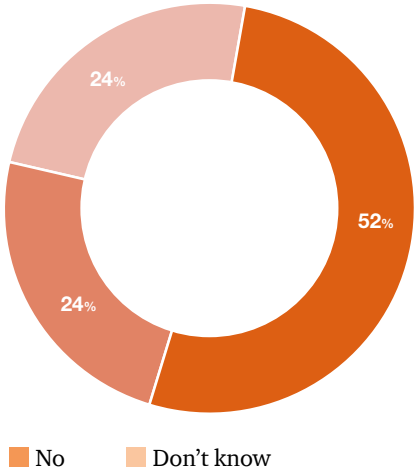
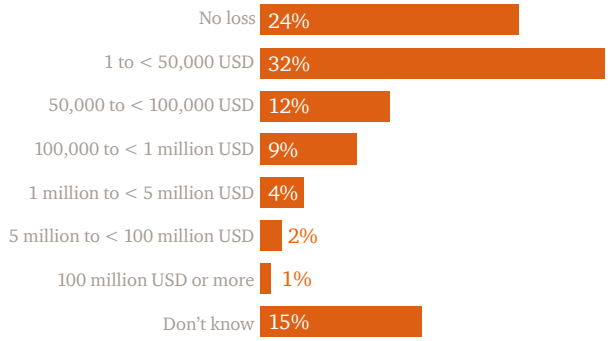
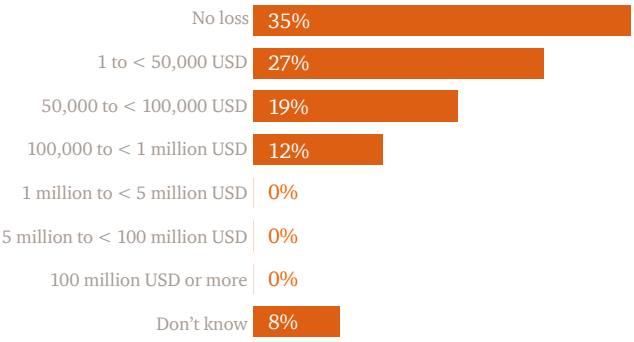


Fig 23: Reported losses through cybercrime in the last 24 months. Global and Luxembourg results

Global

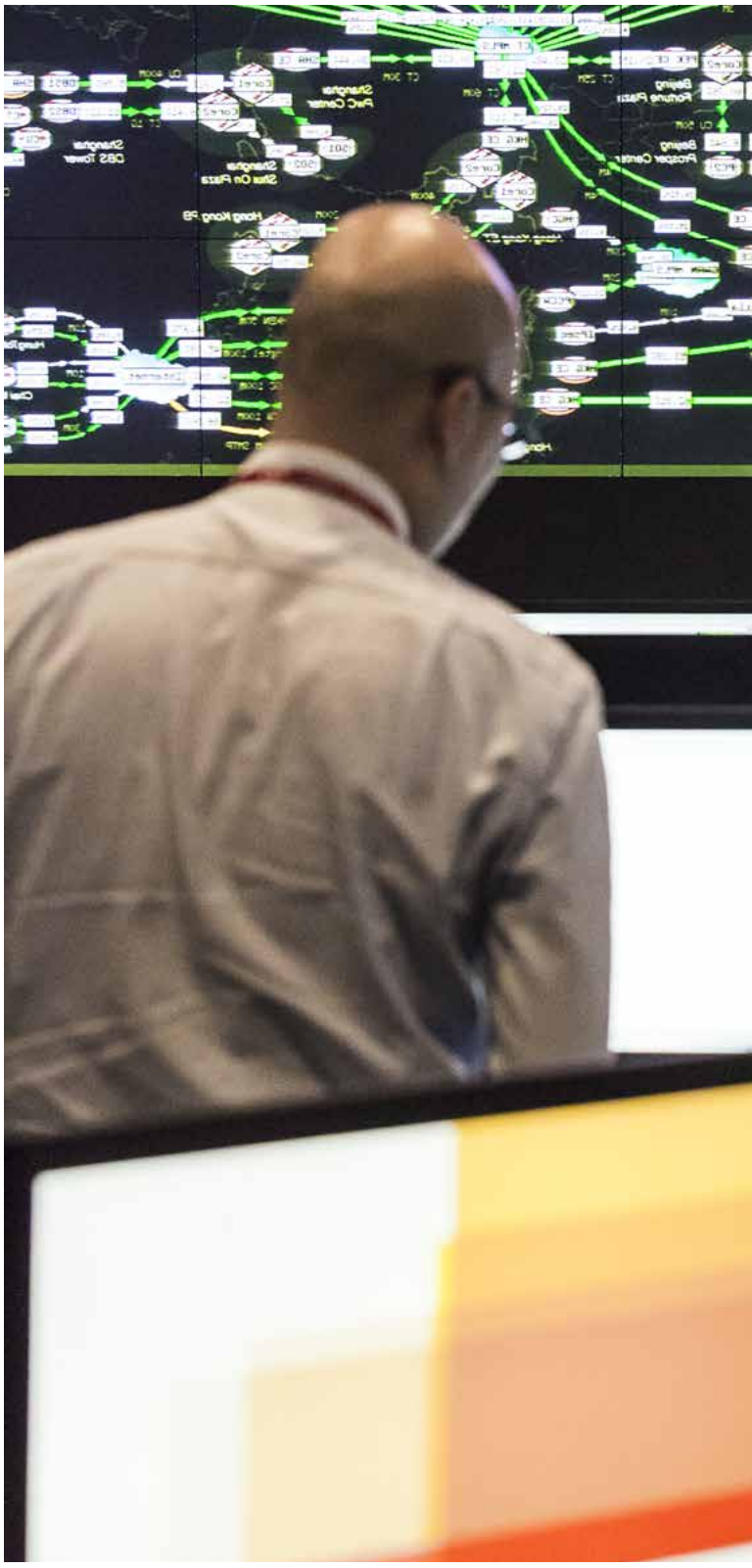


Luxembourg



In Luxembourg, 35% of respondents who have been victims also consider that they did not suffer any loss, a significantly higher percentage than at global level. This response is certainly linked to the problem cited above: you don't know what you don't know. We might also question their definition of "loss" - direct loss linked to customer complaints, regulatory fines or others. In our view, there are many aspects to consider: the cost of efforts dedicated to investigation and remediation, the indirect impacts on customers and reputation, as well as non-financial impacts.

A company should take into account these wider impacts of a cyber-breach even if its appropriate response and good communication have actually reinforced its reputation. Of course, we expect most of the respondents not to publicise any incidents if they were not required to. Considering the regulations to come (e.g. General Data Protection Regulation and Network and Information Security Directive) and that these regulations will increase notification obligations and fines, Luxembourg companies should increase their detection, response and remediation capabilities.

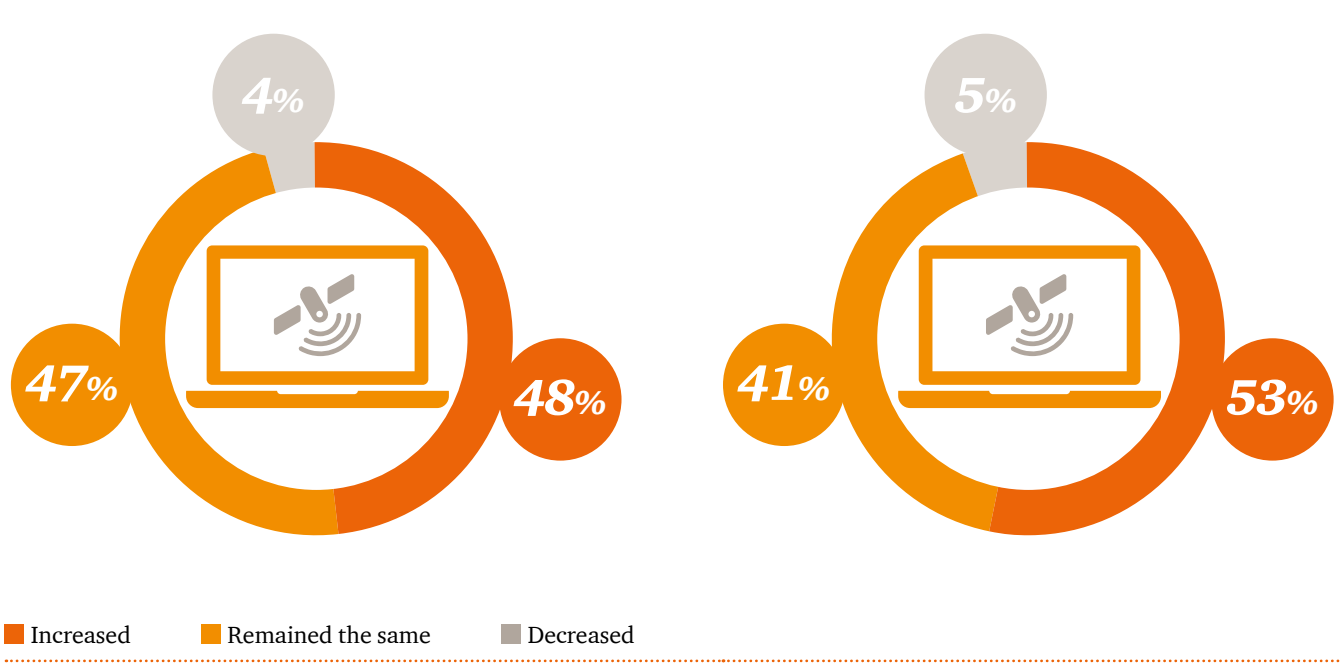


Awareness

Over half of our global survey respondents (53%, up 10% since 2014) see an increased risk of cyber threats, perhaps also due to intensifying media coverage.

When it comes to risk perception, many companies understand the growing cybercrime trend and realise that they could be a victim in the coming years. The perception of risk from Luxembourg respondents is increasing overall (68%) and 57% expect to be the victim of cybercrime in the next 24 months, a figure much higher than at global level. Other surveys such as the 2015 ILA study on the fund industry[4] or the Insurance banana skins review 2015[5] have confirmed that cybercrime is a very hot topic on the corporate agenda. From a Luxembourg perspective, the long history of banking secrecy has helped to create a heightened awareness of risks and confidentiality related to cybercrime.

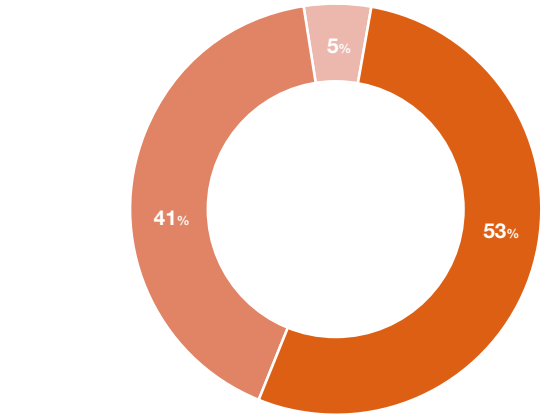
Fig 24: Perception of cybercrime risk based on global responses



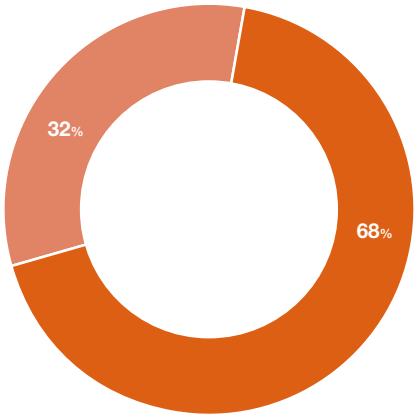
[4] "Luxembourg Fund Governance Survey 2014", PwC Luxembourg and Institut Luxembourgeois des Administrateurs, January 2015
[5] "Insurance Banana Skins 2015", PwC and Centre for the Study of Financial Innovation, July 2015

Fig 25: Awareness of cybercrime over the last 24 months

Global



Luxembourg



Increased | Remained the same | Decreased

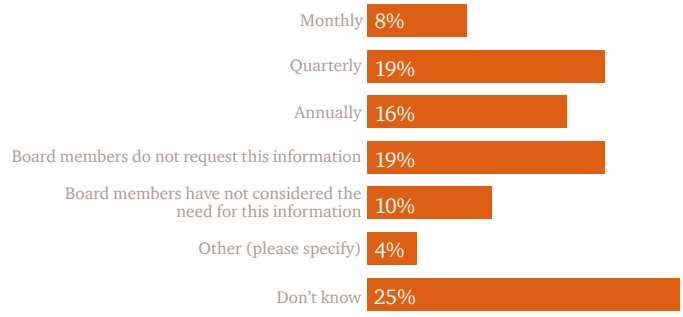
Increased | Remained the same

Executive boards in Luxembourg appear to be more interested in cybercrime than in other countries. 57% of participants request information about their organisations' readiness to address cyber threats, compared to only 43% globally. A result confirmed by the ILA governance study on fund boards[6]. This level of awareness is a very good indication of how seriously companies take the threat of cybercrime and suggests that new initiatives would be welcome. However, it is also important to understand the level of detail of the information provided to Boards and what companies mean by "readiness".

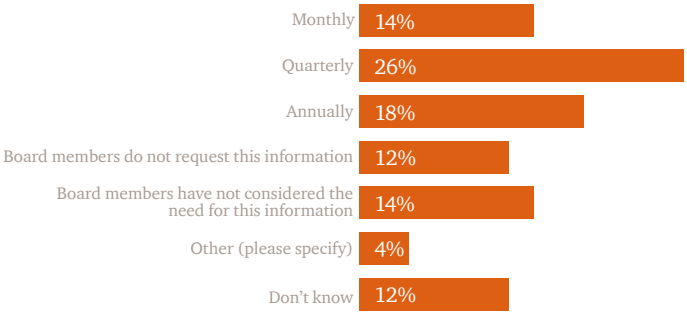
[6] "Luxembourg Fund Governance Survey 2014", PwC Luxembourg and Institut Luxembourgeois des Administrateurs, January 2015

Fig 26: How often do Board members request information regarding the organisations state of readiness to deal with cyber incidents?

Global



Luxembourg



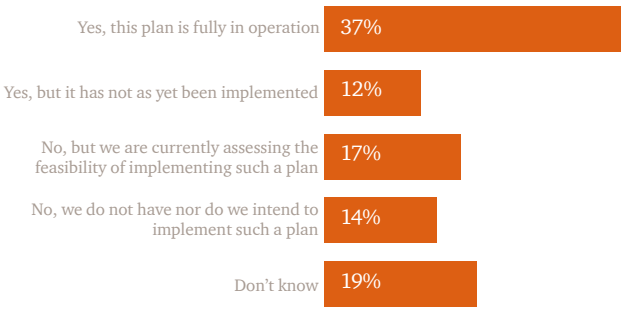
Luxembourg respondents again reported an inherent trust in their staff when it comes to cybercrime. 71% of respondents believe that external agents are more likely to be the source of a cybercrime attack than internal ones, with a further 22% reporting that they expect threats from both internal and external agents. Actually, the threats to IT infrastructures and databases are constantly evolving and they can come from any type of source, be it external or internal, hostile or trusted. Organisations able to respond quickly and forensically to a cyber-breach will also be able to avoid many of its worst consequences.

Readiness

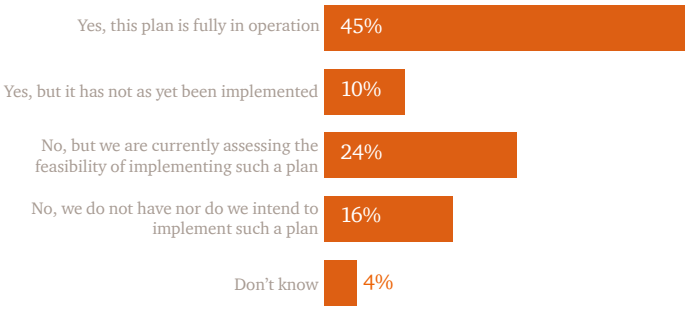
The mounting complexity of cybercrimes and means to combat or prevent them makes it difficult for IT teams to handle the fall-out by themselves. Responsibility for redressing cyber vulnerabilities starts at the top, so it's vital for Boards to include cybercrime in their routine risk assessments. Luxembourg companies, in general, appear to have made positive moves in this direction. However, they also need to protect the systems and information on which their growth depends to avoid significant financial losses and irreparable damage to their reputation. First-response personnel must be able to mitigate all these risks and, sometimes, the inclusion of finance personnel, human resources and even public relations expertise would limit the immediate fall-out.

Fig 27: Does your organisation have an incident response plan to deal with cyber attacks?

Global



Luxembourg

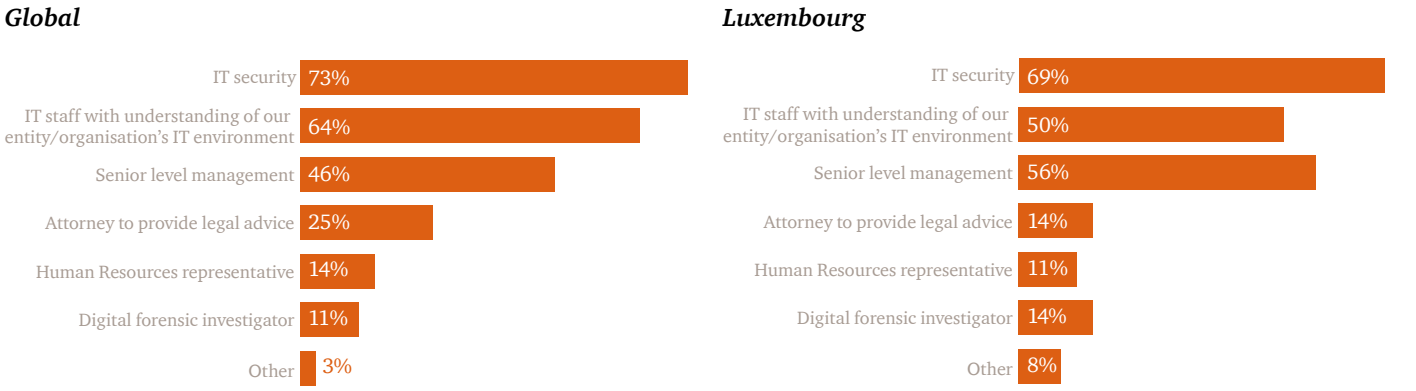


In Luxembourg, more than 55% of respondents report having a cyber-incident response plan. Although these plans might not be fully implemented, the percentage of companies reporting operational plans is above the global average. A customised cyber-incident response plan is crucial and requires strong coordination not only internally, but also externally. Despite these positive results a number of questions remain. How do companies assess the level of implementation: do they rely on self-assessment, do they ask for an external assessment, or they simply use the plan during incidents? Having a plan is a crucial first step, but that does not mean it is working effectively or as expected. In this sense, the more general approach of Disaster Recovery Plans or Business Continuity Plans (DRP/BCP), which are a formal regulatory requirement based on historical best practice for financial institutions in Luxembourg, might work better. Even with comprehensive plans in place, in our experience, the operating effectiveness is not always comprehensively tested. We can see that risk awareness is there, but it doesn't systematically translate into relevant testing and verification measures.

74% of respondents in Luxembourg reported having assigned dedicated personnel to cyber incident response, compared to 62% at global level. Clearly adequate Board level attention makes the setup of teams to implement response plans easier. Senior level management are involved in first response teams in more than half of the responses, again showing slightly more involvement than seen at a global level. IT security is the most common expertise reported, but Luxembourg companies prove to have fully understood that incident management includes other areas of expertise as well and requires quick decisions. This is an indication that cyber incident response has been thoroughly considered, since almost all business processes and operations are now either completely digitised or at least influenced by IT systems.

Since the speed of response is such a key element, some organisations have even included external advisors in their first response teams. This enables them to mobilise an investigation on pre-agreed terms and at short notice.

Fig 28: Make up of first responder teams to cyber attacks

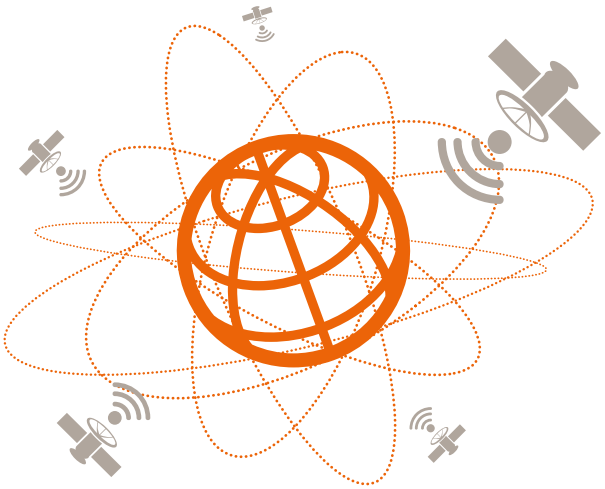


Threat vectors: the five categories

Nation-states
threats include espionage and cyber warfare; victims include government agencies, infrastructure, energy and IP-rich organisations

Insiders
not only your employees but also trusted third parties with access to sensitive data who are not directly under your control

Terrorists
still a relatively nascent threat, threats include disruption and cyber warfare; victims include government agencies, infrastructure and energy



Organised crime syndicates
threats include theft of financial or personally identifiable information (sometimes with the collusion of insiders); victims include financial institutions, retailers, medical and hospitality companies

Hacktivists
threats include service disruptions or reputational damage; victims include high-profile organisations and governments; victims can include any kind of organisation

What can you do?

- Ensure you have in place fundamental safeguards for effective cyber security - including ongoing monitoring, up-to-date personal or sensitive data inventory, a back-up policy and business continuity plans.
- Be connected. Actively monitor cybercrime/cyber security related information which might affect your company, by subscribing to or developing a threat intelligence monitoring service.
- Educate employees at all levels about cyber threats. Cybercrime is not simply and IT problem and all staff should know what to do in the event of a breach.
- Pro-actively bring cybercrime response planning to the attention of the board of directors in order to get their buy-in for developing incident response capabilities further.
- Discover the unknown. Identify whether you have been the victim of a cyber attack by performing a breach indicator review of your IT systems.

Your Luxembourg contacts

Forensic Services & Financial Crime

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

Cyber Security

Vincent Villers
Partner, Cyber Security Leader
t: +352 49 48 48 2367
e: vincent.villers@lu.pwc.com

Anti-Money Laundering

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

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

Industry leaders

Rima Adas
Partner, Financial Sector Leader
t: +352 49 48 48 2101
e: rima.adas@lu.pwc.com

Philippe Pierre
Partner, Public Sector Leader
t: +352 49 48 48 4313
e: philippe.pierre@lu.pwc.com

Gilles Vanderweyen
Partner, Commercial and industrial companies Leader
t: +352 49 48 48 5826
e: gilles.vanderweyen@lu.pwc.com

Notes

www.pwc.lu/forensic-services

PwC Luxembourg (www.pwc.lu) is the largest professional services firm in Luxembourg with 2,600 people employed from 58 different countries. PwC Luxembourg provides audit, tax and advisory services including management consulting, transaction, financing and regulatory advice. The firm provides advice to a wide variety of clients from local and middle market entrepreneurs to large multinational companies operating from Luxembourg and the Greater Region. The firm helps its clients create the value they are looking for by contributing to the smooth operation of the capital markets and providing advice through an industry-focused approach.

The PwC global network is the largest provider of professional services in the audit, tax and management consultancy sectors. We are a network of independent firms based in 157 countries and employing over 208,000 people. Talk to us about your concerns and find out more by visiting us at www.pwc.com and www.pwc.lu.