pwc

Shining a light on fraud

Irish Economic Crime Survey 2018

Contents

Executive summary

I am delighted to present the findings of the PwC 2018 Irish Economic Crime and Fraud Survey. The research is conducted every two years and is part of a comprehensive global initiative, gathering valuable data from more than 7,200 respondents across 123 countries. The survey aims to shed much needed light on some of the latest trends on how fraud and economic crime is impacting businesses. In Ireland, some 77 organisations participated representing all key sectors and industries.

The survey highlights that economic crime and fraud is a major business concern. Reported economic crime and fraud in Ireland has increased significantly. Similar to global levels, almost half of Irish organisations revealed that they had suffered economic crime or fraud in the last two years, up from 34% two years ago.

The survey further reveals that the cost of economic crime has also increased with some very significant frauds occurring. For example, over one in ten (11%) respondents said that the cost of the most substantial fraud experienced in the last two years was in excess of €4m, compared to 7% globally and just 3% back in 2016. The clean-up costs are also substantial, with nearly seven out of ten respondents confirming that they had spent the same or more on the subsequent investigations compared to the actual crime itself. Interestingly, the survey also suggests that many Irish business leaders do not fully appreciate the impact of fraud on employee morale, business relations and on their reputation/brand.

The incidence of cybercrime in Ireland has also significantly increased - 61% of Irish organisations reported to have suffered cybercrime in the last two years, up from 44% in 2016 and is now double that compared to global companies (31%). Cybercrime is also expected to be the most disruptive economic crime into the future. The search for cybercrime in Ireland is also high on the radar with the vast majority performing cyber-attack vulnerability risk assessments, and is higher than global companies.

Irish organisations are more vigilant than global peers in the search for fraud. For example, over half of participants revealed that they had spent more funds on combatting economic crime and fraud compared to four out of ten globally. Similarly, Irish respondents confirmed that they undergo more fraud risk assessments compared to global peers. However, this also represents that four out of ten still do not perform these assessments, which are critical in the prevention of fraud.

Technology presents a real opportunity in areas such as fraud prevention, detection and authentication. However, the survey highlights that Irish organisations lag their global peers when it comes to investment in this area. For example, just one in ten respondents said that they are using fraud detection technology to monitor economic crime and fraud compared to a quarter globally. Just 15% say that they are leveraging data analytics and only 6% are using Artificial Intelligence to help combat fraud, and is well below global levels.

Most economic crimes in Ireland were detected through corporate controls (55%) including fraud risk assessments, suspicious transaction reporting and corporate security. No frauds were detected via data analytic techniques.

In an era of unparalleled public scrutiny, a lack of fraud-awareness in an organisation is highly dangerous. The important question is not: is your

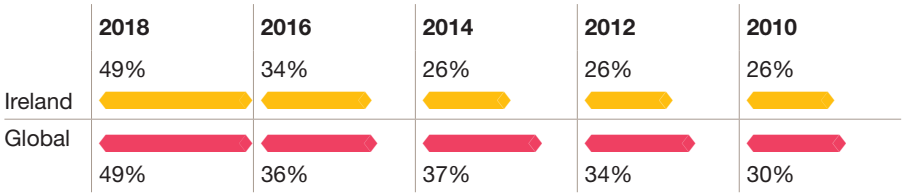
organisation the victim of fraud? Rather, it's: are you aware of how fraud is touching your organisation? While there is growing awareness of the perils of economic crime, few companies are fully aware of the individual risks they face. Technology has advanced in leaps and bounds, to help prevent and detect fraud; technology has also assisted fraudsters become more strategic and sophisticated in their actions. Regulatory regimes have also become more robust, with their enforcement intensifying, often in cross-border co-operation. We see more and more organisations now recognising that fraud can hold them back from competing – and it has simply become too costly to ignore.

We would like to thank the Irish participants for taking the time to complete the survey. We hope that you find the report of interest and useful in your campaign to address economic crime.

Pat Moran
PwC Ireland Cyber Leader

SECTION 1. Understanding the cost of fraud

Fig.1: Reported rate of economic crime



PwC's 2018 Irish Economic Crime and Fraud Survey reveals that the rate of economic crime in Ireland has increased significantly since 2016, and now matches the rate that global organisations face.

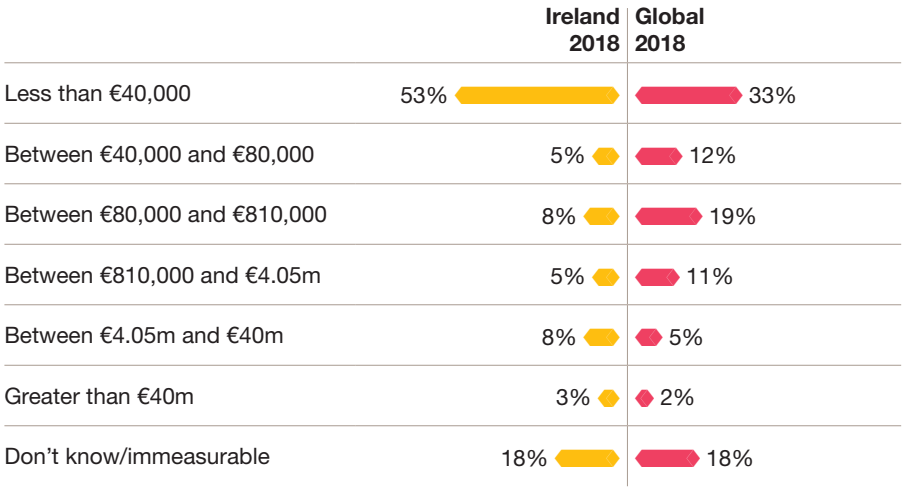
Half of Irish respondents in the survey reported that they were victims of fraud or economic crime, up from a third of respondents in 2016. This rise can be explained not only because more frauds are being detected, but also because more fraud and economic crime is happening – including specifically, cybercrime.

As the value of transactions over the internet increases exponentially year on year, fraudsters are turning to new ways of re-directing funds and are successfully achieving their goals.

49% of Irish organisations reported to suffer from fraud/economic crime, up from 34% in 2016

The cost of economic crime and fraud

Fig 2: Cost of the most disruptive economic crime or fraud suffered by your organisation in the last two years



Although most economic crime and frauds in Ireland cost less than €80,000 to the businesses concerned, over one in ten (11%) survey participants have lost over €4m and is higher than the global figure of 7%. This may suggest that Irish organisations may be more vulnerable and perhaps even a softer target for fraudsters compared to global companies.

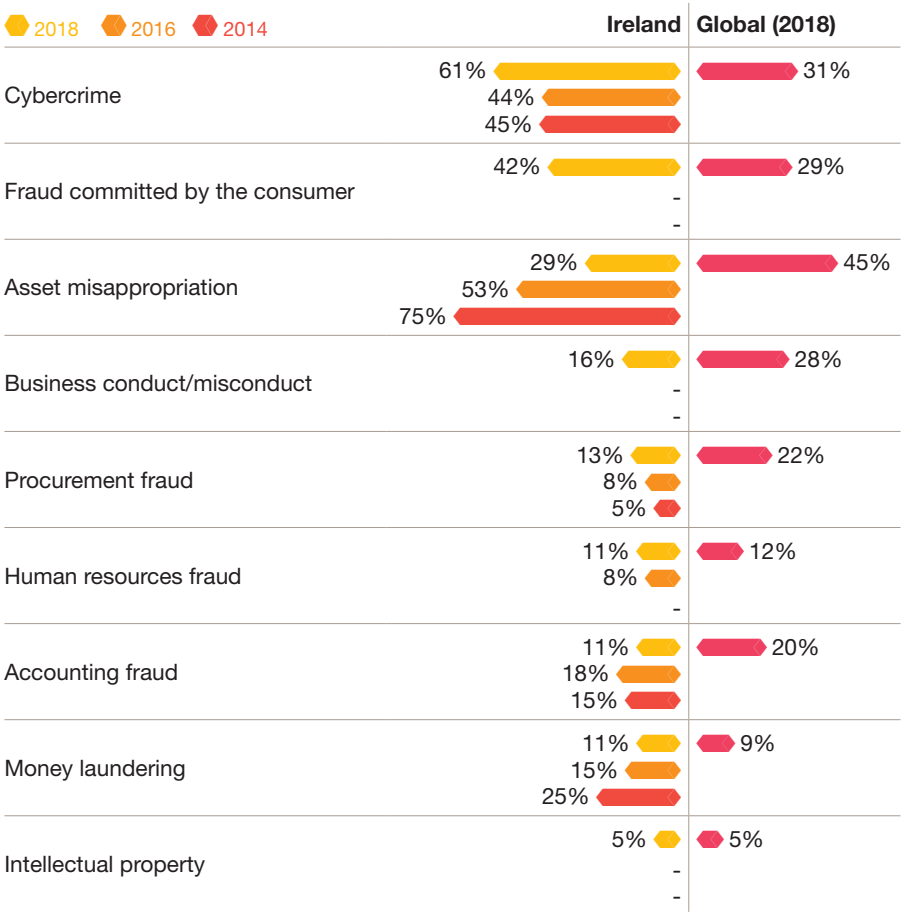
The direct cost of economic crime and fraud can be substantial

11% suffered losses in excess of €4m and is up from 3% in 2016

Though many organisations still feel that Ireland is not a target for economic crime, these statistics clearly tell another story. It is also worrying that nearly one-fifth of Irish respondents (18%, up from 6% in 2016) admitted to either not knowing how much the economic crime and fraud had cost them, or said the loss was immeasurable.

Cybercrime, consumer fraud and asset misappropriation most frequently reported frauds

Fig 3: Types of economic crime reported



The incidence of cybercrime in Ireland is double that of global counterparts

In Ireland, cybercrime has taken over from asset misappropriation as the most prevalent economic crime. In fact, the incidence of cybercrime (61%) in Ireland is double that experienced by global companies (31%).

Within the last two years we have seen over half of Irish respondents become victims of cybercrime despite an increased level of awareness and more resources being spent on addressing the risks.

It is a concern for Ireland's digital economy and for investors looking at Ireland as a business destination. Significant measures are needed by Government and industry to give confidence to the outside world.

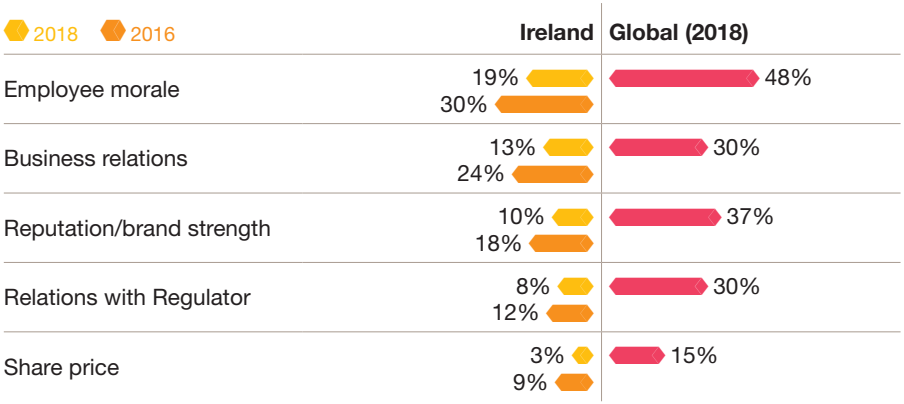
Consumer fraud and business conduct fraud, which we have seen grow in prominence, are measured in the survey for the first time this year.

- Consumer fraud is any type of deceptive practices that result in financial or other losses for consumers in the course of seemingly legitimate business transactions.
- Business conduct fraud is any type of employee action that fails to deliver fair customer outcomes or risks market integrity. Unlike operational breakdowns or external threats, business conduct risk requires a more holistic response.

Irish organisations may not fully appreciate the non-financial cost of fraud

The non-financial costs of economic crime and fraud

Fig 4: How did fraud/economic crime impact the following aspects of your business (% who said 'high' and 'medium' impact)

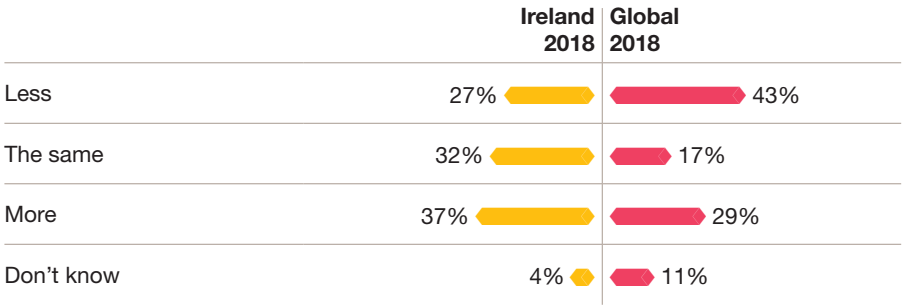


The survey suggests that Irish companies may not fully appreciate the non-financial impact of economic crime or fraud on their organisation and are less concerned than they were in 2016. Just a fifth (19%) viewed employee morale to be impacted by economic crime or fraud, compared to 30% in 2016 and 48% globally.

Economic loss is not the only concern that companies face when they have been a victim of an economic crime or fraud. Global respondents are more concerned than their Irish counterparts about the non-financial damage they had suffered and what impact economic crime had on their employee morale, reputation/ business relations and relations with the Regulator.

The cost of cleaning up

Fig 5: What was the amount spent by your organisation on investigations and/or interventions as a result of economic crime or fraud compared to the amount lost?



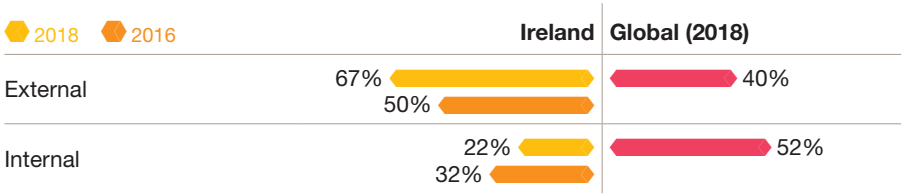
Over two-thirds (69%) of Irish respondents who suffered economic crime spent the same or more as the amount they lost on the subsequent clean-up. This is significantly higher than global counterparts (46%) which may suggest that Irish organisations are not adequately prepared for an event like this.

The cost of the subsequent clean-up of fraud is also significant. Clearly, it can often be difficult to assess the damage done when economic crime/fraud has been discovered. It is often too difficult to grasp just how long the crime has been going on. The costs of falling victim to economic crime go far beyond the financial damage.

69% of Irish respondents spent the same or more than the fraud itself on the clean-up

Who is committing economic crime and why?

Fig 6: Who committed the crime?



As we saw two years ago, the greatest share of economic crime and fraud in Ireland is committed by external perpetrators.

The incidence of external economic crimes or fraud has increased since 2016. The survey highlights that of the external crimes, 42% was perpetrated by customers, 33% by hackers and 25% was committed by organised criminals. Globally, the majority of fraud/economic crime is committed by internal perpetrators.

Often, one of a company's biggest fraud 'blind spot' is the people with whom it does business: third parties with whom companies have regular and profitable relationships, agents, suppliers, shared service providers and customers. In other words, people and organisations with whom a certain degree of mutual trust is expected may actually be stealing from the organisation.

Most fraud in Ireland is perpetrated by external fraudsters

SECTION 2. Catching and preventing fraud

Fig 7: How has/is your organisation adjusting the amount of funds spent to combat fraud/economic crime?

	Last 2 years		Next 2 years	
	Ireland	Global	Ireland	Global
Significant increase	14%	16%	12%	13%
Some increase	37%	26%	47%	31%
About the same level	49%	54%	40%	51%
Decrease	-	4%	1%	5%

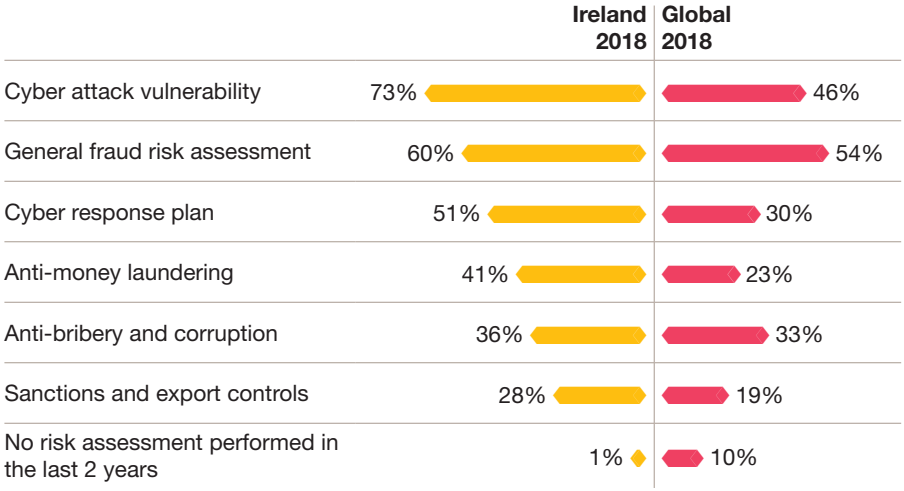
Not only is reported economic crime and fraud up since 2016, so too has the amount that companies are spending to fight it. The survey highlights that more Irish firms have increased their level of spending to combat fraud compared to their global counterparts.

- 51% of Irish respondents reported that their organisation has increased spending on combatting economic crime and fraud over the past two years (Global: 42%)
- 59% of Irish respondents said that they plan to increase this spending over the next two years (Global: 44%)

Irish organisations have stepped up their investment in attempting to prevent and detect economic crime and fraud. This is evident in the emergence of more effective governance, risk management frameworks, technology and 'three lines of defence' models. This investment needs to continue over the next two years as the rate, complexity and sophistication of economic crime and fraud increases.

Irish companies are spending more funds to combat fraud and economic crime compared to global counterparts

Fig 8: What are the methods that you choose to address fraud risk? (% who said 'yes')



Although the survey suggests that Ireland is doing better at performing fraud risk assessments compared to global companies, there is still room for improvement:

- 40% of Irish respondents are still not performing general fraud risk assessments (Global: 46%)
- Half of Irish respondents do not operate a cyber response plan.
- Over half have not conducted risk assessments in critical areas such as Anti-money laundering, anti-bribery and export controls.

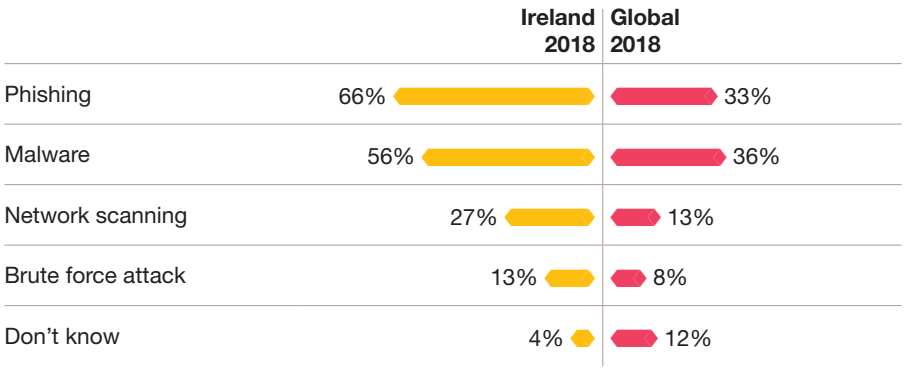
Conducting fraud risk assessments, which are the first step in preventing fraud before it takes root, plays a vital role in the prevention and detection of economic crime. Fraud risk assessments can help organisations prevent fraud by identifying the specific frauds they need to look for. Also, these assessments are increasingly looked on favourably by Regulators during their audits or enforcement actions.

Nearly three-quarters of Irish respondents said that they have conducted a cybercrime risk assessment in the last two years, compared to less than half of their global counterparts. This is encouraging and demonstrates effective risk management and foresight.

Irish businesses are performing more targeted fraud risk assessments than global counterparts

SECTION 3. Beating the cyber criminals

Fig 9: In the last two years has your organisation been targeted by cyber attacks using any of the following techniques?



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. The increasing frequency and sophistication of these attacks are spurring companies to look for more effective ways to mitigate them. These measures include technology-enabled techniques to pre-empt where the next attack will come from. This approach has the added benefit of enabling a deeper focus on fraud prevention and results in clear efficiencies.

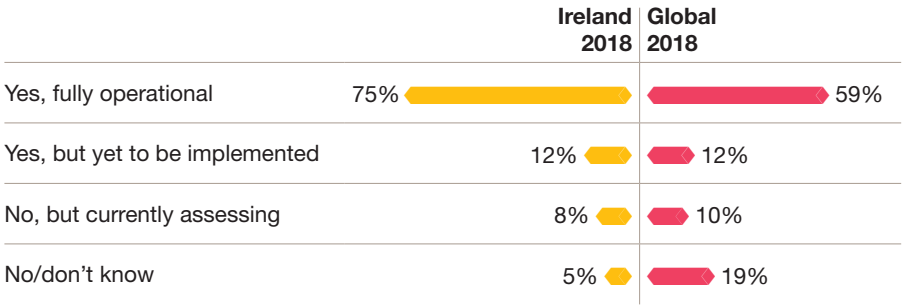
61% of Irish organisations experienced cybercrime, up from 44% in 2016

Two-thirds of Irish respondents have been targeted by cyber attacks through phishing, compared to 33% globally. Over half were targeted through malware (which includes ransomware), compared to 36% globally. These statistics are worrying as it is clear that Ireland is being targeted by cyber criminals and using malicious email links as a deliberate technique to steal funds.

Irish organisations have experienced around twice the number of phishing and malware attacks compared to global companies

Cybercrime detection and prevention

Fig 10: Does your organisation have a cybersecurity program (preventative/ detective) to deal with cyber attacks?

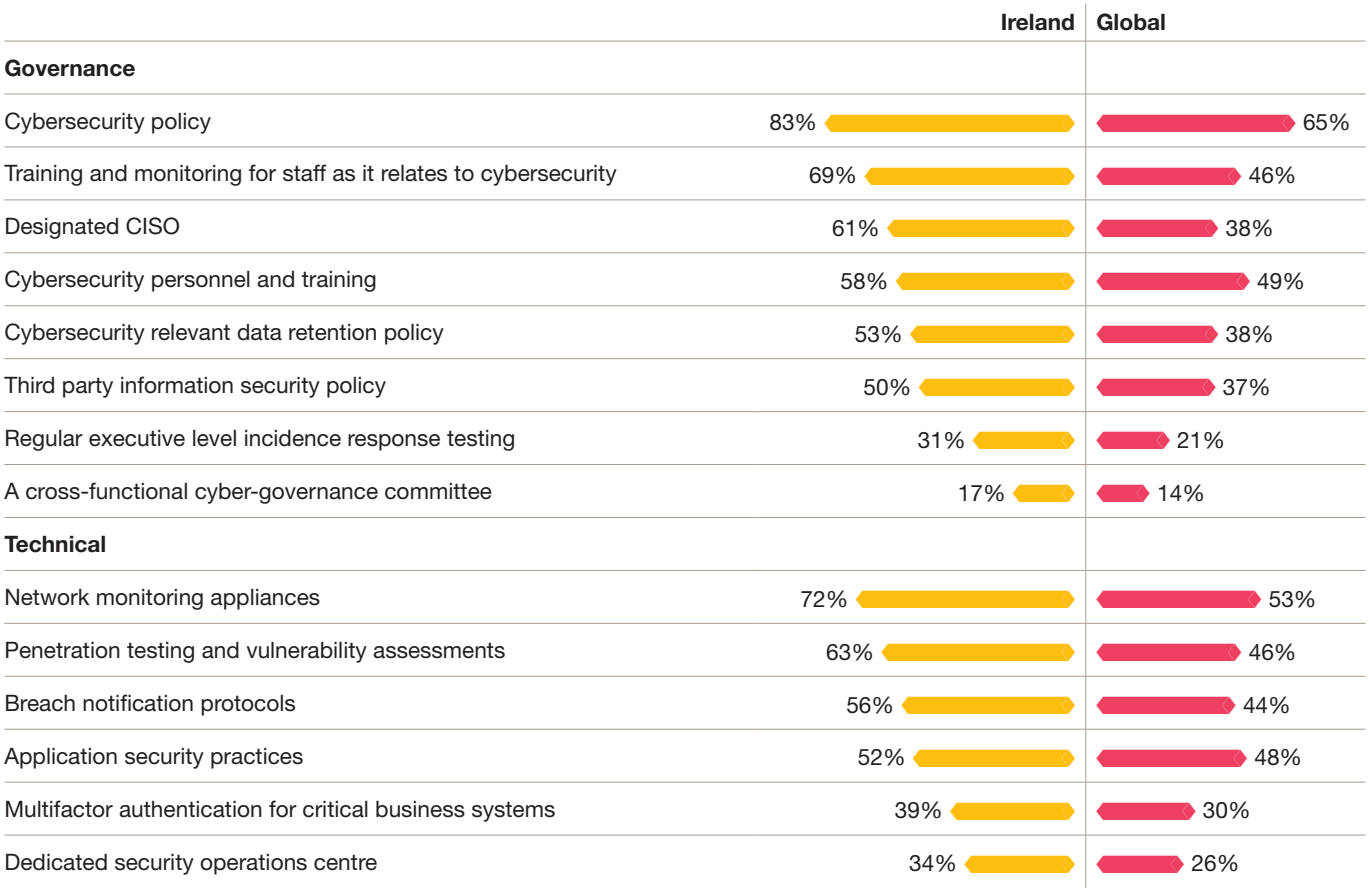


The survey reveals that three-quarters of Irish organisations operate cybersecurity programs to combat cyber attacks, compared to 59% globally. This is encouraging and demonstrates that Irish businesses are investing in designing a deliberate strategy to curb cyber threats.

Regulators and boards will be pleased to learn of this. However, it is critical that organisations have some way of measuring how successful these programmes are and can measure their success through simple and meaningful metrics.

More Irish firms operate cybersecurity programs to deal with cyber attacks than global counterparts

Fig 11: What are the key elements of your cybersecurity program?



More focus needed on third party information security

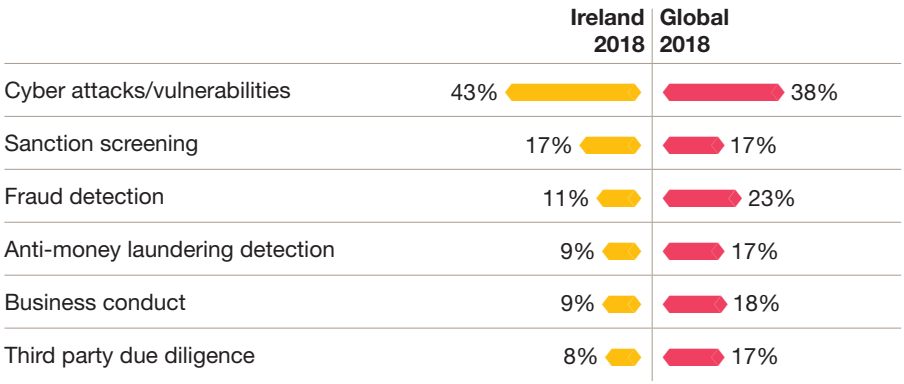
The survey highlights that common elements of a cybersecurity program in Ireland include: Cybersecurity policies (83%); Network monitoring appliances (72%); Staff training and monitoring (69%) and Penetration testing (63%).

This is consistent (but slightly ahead) with the global findings, which should give confidence to Irish companies that they are focusing on the right areas. It is disappointing, though, that not enough focus is being put on third parties where a number of threats are commonly found. The survey suggests that half of Irish companies are ignoring third party information security policies.

With GDPR now very present in people's minds, improvements in managing third party risk, distributing breach notifications and relying on robust authentication procedures will become extremely important for all businesses.

SECTION 4. Harnessing the power of technology

Fig 12: To what extent do you use technology as an instrument to monitor economic crime and fraud in each of the following areas? (% who said 'primary monitoring technique')



When it comes to fraud, technology is a double-edged sword. It is both a potential threat and a potential protector. There is a fine balance between technology's effectiveness and its cost while remaining ahead of the fraudsters. As companies come to view fraud as a business problem which could seriously hamper growth and, indeed, their sheer existence, 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 fraud prevention, detection and authentication.

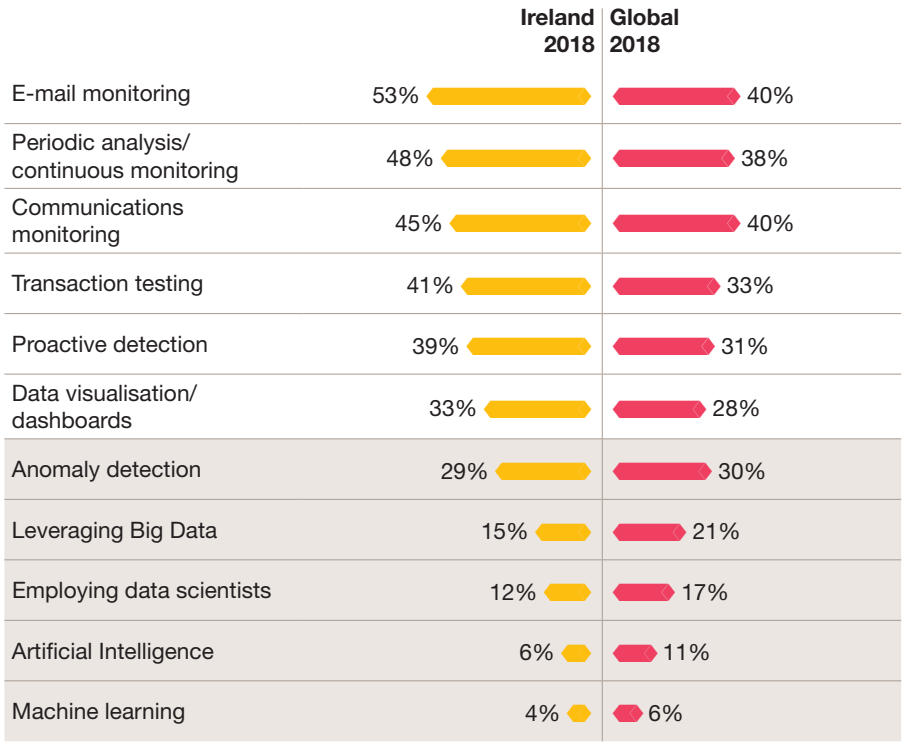
Today, organisations globally have access to a wealth of innovative and sophisticated technologies with which to defend themselves against fraud, aimed at monitoring, analysing, learning and predicting human behaviour. These include machine learning, predictive analytics and other artificial intelligence techniques.

Only 11% of Irish respondents admitted to using technology as their primary monitoring technique to detect fraud, compared to 23% globally. Just 13% strongly agreed that their organisation uses technology to provide robust reporting capability in the combat of economic crime and fraud, compared to 21% globally.

Irish companies lag global counterparts in the use of many technologies to combat economic crime and fraud

The survey shows that Irish companies lag global counterparts in using Artificial Intelligence and Big Data to detect and combat fraud

Fig 13: To what extent is your organisation using and finding value from the following alternative/disruptive technologies in your organisation's control environment to help combat economic crime and fraud? (% who said 'using and finding value')



Only 15% of survey participants said that they are finding value and using Big Data in their control environment to help combat fraud compared to 21% globally; just 6% are using Artificial Intelligence compared to 11% globally while only 4 % are using machine learning. This represents a big opportunity for organisations to leverage innovative and cloud-based techniques to identify suspicious patterns and pre-empt economic crime and fraud.

We are starting to see companies provide this service through the cloud and effectively harness global data and the increased processing power it delivers. Integrating these developments into legacy systems will represent a challenge for some organisations, which will give a competitive advantage to emerging technology companies.

SECTION 5. Getting the culture right

Role of management in setting the tone from the top

Fig 14: Who has primary responsibility for the business ethics and compliance program in your organisation?

	Ireland 2018	Global 2018
Chief Compliance Officer	34%	30%
Chief Executive officer	24%	17%
General Counsel	12%	10%
Human Resources Director	10%	11%
Chief Risk Officer	7%	7%
Chief Financial Officer	2%	2%
Chief Operating Officer	2%	2%
Total C-suite responsibility	**91%**	**79%**

77% of Irish respondents confirmed having an ethics and compliance program

The 'tone from the top' and the expectations set by management play a critical role in the detection and prevention of economic crime and fraud.

A company's ethics and compliance program has a critical role in shaping an organisation's culture including protocols around economic crime and fraud.

Effective and transparent reporting channels are extremely important when it comes to economic crime to allow senior management to have complete oversight of all risks detrimental to the business. This not only allows the organisation to react as efficiently and quickly as possible, but also assists in the protection of personnel.

It is an interesting development that today's businesses are increasingly embedding their fraud prevention and detection measures into the fabric of their first line of defence: executive management. Economic crime and fraud cannot just be the responsibility of the second or third lines of defence. In a world where fraudsters are looking for vulnerabilities and weak links, this is an important development.

The survey confirms that executive management (the CEO and executives) are responsible for the business ethics and compliance program (91%), thus being held accountable by the Board for fraud detection and prevention. Global executive management are perceived to have less responsibility (79%). Nearly a quarter (24%) expect the CEO to have primary responsibility for their organisation's ethics and compliance program.

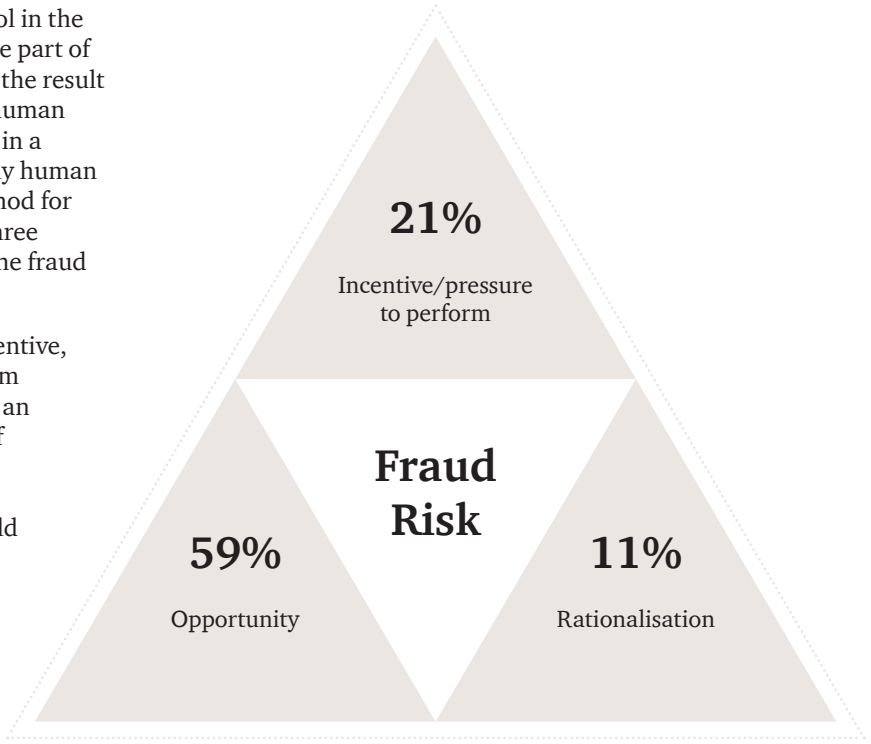
With the financial costs of fraud hitting the bottom line of a business, it's only natural for the Board and shareholders to want explanations from senior management. But senior management needs to know about the fraud in the first place.

The survey further reveals that nine out of ten (89%) Irish respondents said that serious frauds are reported to senior management. This puts a sharp spotlight on crisis management and the extent to which senior management are, or are not, adjusting their risk profiles accordingly.

The right behaviours – the fraud triangle

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 behaviours. 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.** While all three of these drivers generally are present for fraud to occur, they should all be treated differently.



Extent of contribution of above factors to fraud/economic crime (global respondents)

We look at each of the principal drivers of internal fraud below:

1. 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. The survey highlights that 16% (Fig 3, page 8) of Irish respondents who experienced economic crime and fraud suffered business conduct or misconduct fraud.

At the same time, 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 service as useful checks on whether aggressive sales programmes are leading to fraudulent behaviour. A well-promoted open-door or hotline policy can also provide a valuable early warning system of potential problems in an organisation.

2. Preventing the opportunity: controls

47% of Irish respondents said that changes in the geopolitical landscape will increase the opportunities for fraud

Three-quarters (74%) of Irish respondents expect changes in the geopolitical landscape to have a greater impact on the regulatory environment over the next two years (Global: 54%). Nearly half (47%) said that changes in the geopolitical landscape will increase the opportunities for fraud (Global: 28%), while 55% said it would increase their organisation's appetite to spend more resources to fight economic crime and fraud (Global: 38%).

Corporate controls - a lever to prevent the opportunity

The survey shows that most economic crime and frauds were detected through corporate controls such as fraud risk controls, suspicious transaction reporting and corporate security (Fig 15, page 24). Internal audit and data analytics were not successful in detecting fraud in Ireland in 2018. Tip-offs resulted in the detection of crime in 22% of cases.

Over half of frauds/ economic crimes were detected by corporate controls

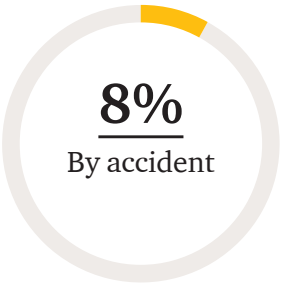


Fig 15: How was the economic crime or fraud initially detected?

2018 2016 2014	Ireland	Global (2018)
Corporate Controls		
Internal audit (routine)	- 10% 7%	14%
Fraud risk management	22% 15% 13%	13%
Data analytics	- 3% -	4%
Suspicious transaction reporting	19% 21% 38%	13%
Corporate security (IT and physical)	14% 3% 6%	5%
Rotation of personnel	- - 7%	2%
TOTAL 2018	**55%**	**51%**
Corporate culture		
Tip-off (external)	11% 15% -	13%
Tip-off (internal)	11% 6% 6%	7%
Whistleblowing	- - -	7%
TOTAL 2018	**22%**	**14%**
Beyond the influence of management		
By accident	8% 8% 5%	8%
By law enforcement	- - 5%	4%
Investigative media	- - -	2%
TOTAL 2018	**8%**	**14%**

3. Building the right culture: Rationalisation

The first step in building the right culture is to focus on the environment that governs employee behaviour. 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 understand what constitutes an unacceptable action – and why – rationalising the fraud will be harder. A corporate ethics and compliance program in place can go a long way towards ensuring the people in the organisation understand what is acceptable behaviour.

With over three-quarters (77%) of Irish organisations having an ethics and compliance program, the survey suggests that the majority of Irish businesses are investing in the kind of training that can make a material difference to economic crime and fraud prevention.

The task of detecting and preventing economic crime or fraud is 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 should not resign themselves to the belief that technology is the only solutions or that a certain amount of fraud is simply part of the cost of doing business. Rather, establishing a culture of honesty and openness from the top down, they set the tone for an organisation with a spirit of open accountability.

Appendix: Survey methodology and key contacts

The PwC 2018 Irish Economic Crime and Fraud Survey is conducted every two years and is part of a comprehensive PwC global initiative, gathering valuable data from more than 7,200 respondents across 123 countries. The survey aims to shed much needed light on some of the latest trends on how fraud and economic crime is impacting businesses.

In Ireland, 77 organisations participated in 2018 representing all key sectors and industries including: Communications, Education, Engineering, Entertainment & Media, Financial Services, Healthcare, Manufacturing, Insurance, Pharma, Retail, Technology and Real Estate.

Key contacts are:

Pat Moran
Partner - Cyber Leader

+353 1 792 5308
pat.moran@pwc.com

Declan McDonald
Partner

+353 792 6092
declan.mcdonald@pwc.com

Leonard McAuliffe
Director

+353 1 792 8632
leonard.mcauliffe@pwc.com

Eoghan Linehan
Senior Manager

+353 21 425 4058
eoghan.linehan@pwc.com

www.pwc.ie