***sNews release***

| | |
|---|---|
| *Date* | **0001 GMT 22 February 2018** |
| *Contacts* | Rowena Mearley, PwC Global Communications<br>Mobile: +44 207 213 4727 / + 44 7730 598 643<br>Email: Rowena.w.mearley@pwc.com |
| *Pages* | 3 pages |

# Reported global economic crime hits record levels; cybercrime, cost and accountability concerns rising

- *49% report their company suffering fraud in last two years, up from 36% in 2016*
- *The majority of external perpetrators (responsible for 40% of fraud) are "frenemies" of the organisation – agents, shared service providers, vendors and customers*
- *41% have spent at least twice as much as they lost to cybercrime, on investigations and other interventions*
- *64% estimate losses linked to most disruptive frauds at up to $US1m; 16% say between $US1m and $US50m*
- *Cybercrime is predicted to be the most disruptive fraud for organisations in the next 24 months*

A much wider awareness and understanding of the range, threat and cost of fraud in business has driven reported economic crime to its highest level recorded in PwC's bi-annual survey of business crime.

The Global Economic Crime and Fraud Survey examines over 7200 respondents from 123 countries.

Overall, 49% of respondents, said their companies had suffered fraud in the last two years, up from 36% in 2016. Regionally Africa (62% up from 57%), North America (54% up from 37%) and Latin America (53% up from 28%) reported the highest levels of economic crime.

Asset misappropriation (45%) continues to lead in economic crime experienced by organisations in the last 24 months, cybercrime (31%), consumer fraud (29%) and business misconduct (28%) are close behind.

This year's survey revealed a significant increase (+6% to 52%) in the share of economic crime committed by internal actors. There was also a jump in the percentage of those crimes attributed to senior management (from 16% in 2016 to 24% in 2018). However there are regional variations. In Australia (64%), the UK (55%), Canada (58%); Argentina (44%) and the US (48%), most reported crime was committed by external actors.

The results underline the greater awareness and understanding of the types of fraud, perpetrators, the role of technology, and fraud's potential impacts and costs for a business, comments Kristin Rivera, PwC Global Forensics Leader:

"We can't equate higher levels of reported crime with higher levels of actual crime. What the survey is showing us is that there is far more understanding of what fraud is and where it is taking place. It's particularly true of cybercrime, where there's a much greater understanding of the issues, investigations, analysis, and greater investment in controls and prevention.

"However, despite the progress in understanding and reporting, the fact that just over half (51%) of respondents say they have not, or don't know if they have experienced fraud in the past two years, suggests blind spots still exist in many organisations."

Amongst the key findings:

- The top three types of crime reported were asset misappropriation (45%), cybercrime (31%) and consumer fraud (29%).
- 18 countries reported cybercrime to be more disruptive than the global average (15%), including Ireland (39%), Belgium (38%), South Korea (31%), Canada (29%), the UK (25%), and the US (22%) all reporting higher than the global average.
- Employee morale, business relations, damage to reputation and brand strength are the top three impacts reported.
- Reports of disruption from consumer credit card and financial fraud were higher than the global average (29%) amongst regions including Africa (36%); Eastern Europe (36%); and North America (32%).
- Cybercrime is likely to be the most disruptive economic crime in the next two years, with respondents saying it is twice as likely as any other fraud to be identified to potentially impact organisations. It's also reflected by a rise in the number of people reporting having a cyber prevention and detection plan in place and fully operational (59%, up from 37% in 2016).

**Cost of fraud and prevention**
As awareness, and the profile of fraud and economic crime has risen, so too have investments to combat it, linked also to the direct financial losses reported in the past two years. In the coming two years, 51% will maintain investment levels, and 44% will increase them.

Nearly two thirds (64%) of respondents said losses from the most disruptive frauds they experienced could reach up to $US1 million; 16% said between $US1 million and $US50 million. 42% (+3%) of respondents indicated their companies increased their financial commitment to combating economic crime over the past two years.

Didier Lavion, Principal, Forensic Services, PwC US comments;

"The funds allocated to crime detection and prevention are increasing, and that has a multiplier effect in terms of understanding and detection of fraud. Put simply, the impact of fraud is no longer an acceptable cost of business."

68% of external perpetrators (responsible for 40% of fraud) are "frenemies" of the organisation – people the organisation works with, including agents, shared service providers, vendors and customers.

"Fraudsters are more strategic in their goals, and more sophisticated in their methods," continues Lavion. "It's a big business in its own right. It is an enterprise that is tech-enabled, innovative, opportunistic and pervasive – like the biggest competitor you didn't know you had."

Respondents to the survey admitted secondary costs such as investigations and interventions can increase overall costs. 17% of respondents said they had spent the same amount again as they had lost on investigations and/or interventions of their most disruptive fraud and 41% said they spent at least twice as much as they lost to cybercrime on investigations and other interventions.

**Fighting fraud**
With the public's tolerance for corporate and personal misbehaviour declining, in addition to beefing up their internal controls, many respondents reported addressing fraud prevention through corporate culture initiatives (via internal or external tip offs or hotlines) through which 27% of frauds were detected.

Respondents also reporting using technologies like artificial intelligence (AI) and advanced analytics as part of their efforts to combat and monitor fraud. The survey shows that companies in emerging markets are currently investing in advanced technologies at a faster rate than their counterparts developed nations: 27% of organisations in developing markets currently use or plan to implement AI to combat fraud, versus 22% in developed markets.

Despite higher levels of understanding and reporting of fraud, blind spots still prevail. 46% of respondents globally said their organisation have still not conducted any kind of risk assessment for fraud or economic crime. Additionally, the percentage of respondents who indicated they have a formal business ethics and compliance programme has dropped from 82% to 77%.

"Fraud is the product of a complex mix of conditions and motivations, only some of which can be tackled by machines," comments Kristin Rivera, PwC Global Forensics Leader.

"While technology has a strong role to play in monitoring and detection, when it comes to blocking that 'last mile' to fraud, the returns from people initiatives are likely to far exceed those from investing in another piece of technology."

"It's particularly relevant when you consider a sizable percentage of the 'external' perpetrators is made up of third-parties with whom companies have regular relationships: agents, vendors, shared service providers, customers and more. Everyone in the business must be vigilant about who it allows in to access its systems and processes."

Download the report at www.pwc.com/fraudsurvey

**Notes**

1. In PwC's 21st Annual CEO Survey, 59% of CEOs reported higher levels of pressure from stakeholders to hold individual leaders to account (59%), including for misconduct. In the Banking and Capital Market (65%), Healthcare (65%) and Technology sectors (59%), the profile of leadership accountability was higher than average. So too were expectations in the US (70%), Brazil (67%), and the UK (63%).
2. Highest levels of Fraud: Insurance (62%); Agriculture (59%); the Communications (including telecoms) sector (59%); Financial Services (58%), Retail and Consumer Goods (56%) and Real Estate (56%) were amongst those sectors reporting the highest levels of fraud.
3. Cybercrime: Over two thirds of cyber-attacks were caused by phishing (33%) and malware (36%). It was the most common form of fraud in countries including US, Canada, and the UK.
4. 18 countries reported cybercrime to be more disruptive than the global average (15%): Ireland (39%), Belgium (38%), Netherlands (33%), South Korea (31%), Canada (29%), Romania (28%), Italy (26%), UK (25%), Switzerland (23%), France (22%), US (22%), Luxembourg (21%), Portugal (21%), Sweden (21%), United Arab Emirates (21%), Australia (20%), Israel (18%), New Zealand (16%)

**About PwC**

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 158 countries with more than 236,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.