

FRAUD ON THE RISE






For the eighth year running, The Economist Intelligence Unit, commissioned by Kroll, surveyed senior executives from around the world operating in a wide variety of sectors and functions in order to assess the current fraud environment.

The overall observation is that fraud has continued to increase, with three quarters (75%) of companies reporting they have fallen victim to a fraud incident within the past year, an increase of 14 percentage points from just three years ago. The number of businesses suffering a financial loss as a result of fraud has also increased, from 64% in the previous survey period to 69% this year.

The report reveals some key trends:

Firms feeling more vulnerable to fraud

Theft of physical assets was the most common fraud experienced in the past year, cited by 22% of respondents. Vendor, supplier or procurement fraud (17%) and information theft (15%) are the next two most frequent types of fraud experienced.



But the reported incidents just tell part of the story, with the vast majority of respondents (80%) believing their organizations have become more vulnerable to fraud in the past year. One of the areas identified by executives as being of particular concern is information theft. More than half of executives (51%) believe they are highly or moderately vulnerable to information theft risks such as cyber incidents.

This increased awareness level has led to growth in the number of companies proactively looking after their information security posture. Two-thirds (67%) of companies report that they regularly conduct data and IT infrastructure assessments, and a majority now report that they have an up-to-date information security incident response plan (60%) and have tested it in the past six months (59%), both representing an increase from the previous survey.

The globalization of business increases fraud risk

In a global marketplace where many international businesses have thousands of companies in their supply chain, risks become more difficult to identify and keep under control. Companies feel particularly at risk of threats such as vendor, supplier or procurement fraud, with half of respondents (49%) feeling highly or moderately vulnerable to it.

Logically, larger companies that are more likely to have bigger supply chains felt significantly more vulnerable to this type of fraud, with 20% of businesses with a turnover of more than \$500 million considering themselves highly vulnerable to it, compared to just 14% of firms with a turnover of less than \$500 million.

CHART 1
COMPANIES AFFECTED BY FRAUD AND VULNERABLE TO IT

TYPES OF FRAUD	PERCENTAGE OF COMPANIES AFFECTED BY THIS IN THE PAST 12 MONTHS	PERCENTAGE OF COMPANIES DESCRIBING THEMSELVES AS HIGHLY OR MODERATELY VULNERABLE TO THIS
Theft of physical assets	22%	62%
Vendor, supplier or procurement fraud	17%	49%
Information theft	15%	51%
Management conflict of interest	12%	36%
Regulatory or compliance breach	12%	40%
Corruption and bribery	11%	40%
Internal financial fraud	9%	43%
Misappropriation of company funds	7%	40%
Money laundering	4%	34%
IP theft	4%	37%
Market collusion	2%	26%



Some 40% of respondents felt highly or moderately vulnerable to corruption and bribery, another type of fraud that increases in propensity as companies expand geographically into new territories.

Indeed, in the past year, 72% of companies were dissuaded from operating in a particular country or region because of the heightened exposure it would bring to fraud. Latin America (cited by 27% of all respondents) was the region which saw most businesses turn away, but the other perennial region of concern, Africa, was not far behind (22%).

Many executives see moving into new geographic markets as risky business. One in eight (13%) of those who say their company's exposure to fraud has increased claim entry into new, riskier markets is a reason for this. One in five (20%) say a greater level of outsourcing and offshoring have contributed to their increased fraud exposure.

CHART 2
TOP THREE REGIONS COMPANIES ARE AVOIDING DUE TO HEIGHTENED FRAUD EXPOSURE

REGION	PERCENTAGE OF COMPANIES THAT HAVE BEEN DISSUADED FROM OPERATING HERE BECAUSE OF THE HEIGHTENED EXPOSURE IT WOULD BRING TO FRAUD
Latin America	27%
Africa	22%
Central & Eastern Europe	14%

The threat from within is on the rise

The findings reveal the biggest fraud threat to companies comes from within. Of those companies that experienced fraud where the perpetrator was known, four in five (81%) suffered at the hands of at least one insider, up from 72% in the previous survey.

More than one in three victims (36%) experienced fraud at the hands of a member of their own senior or middle management, 45% at the hands of a junior employee, and for 23%, the fraud resulted from the conduct of an agent or intermediary.

Currently, much media attention is focused on external cyber threats to companies, but the findings of the report tell a different story. Of those companies that have fallen victim to information loss, theft or attack over the past 12 months, the most common cause was employee malfeasance, involved in 45% of cases, with vendor/supplier malfeasance involved in 29% of cases. By comparison, only a small minority of cases involved an attack by an external hacker on the company itself (2%) or on a vendor/supplier (7%).

With employees constituting such a high risk, it is not surprising that executives responding to the survey believe that high staff turnover is the main driver of increased exposure to fraud, with one in three (33%) citing it as being a problem. This is more than twice as many who named the next highest driver of vulnerability to fraud, greater outsourcing (16%).

In an environment where insiders are the source of the problem, other employees who observe or become aware of what the fraudsters are doing are the company's strongest defense. In the past year, a whistleblower was at least partially responsible for exposing 41% of cases



CHART 3
TOP FIVE DRIVERS OF INCREASED FRAUD EXPOSURE

DRIVER OF INCREASED FRAUD RISK	PERCENTAGE OF EXECUTIVES WHO BELIEVE THIS HAS INCREASED THEIR COMPANY'S EXPOSURE TO FRAUD OVER THE PAST 12 MONTHS
High staff turnover	33%
Increased outsourcing & offshoring	16%
Entry to new, riskier markets	13%
Complexity of products or services sold	11%
Increased collaboration between firms (e.g., joint ventures, partnerships)	10%

of fraud that were uncovered. Employee-discovered and reported fraud is well ahead of the next two sources of discovery, external (31%) or internal (25%) audits.

The findings show that anti-fraud efforts can have an effect on the threat from within. Of those firms hit by fraud where the perpetrator was known, just 20% of those with management controls in place suffered at the hands of a senior or middle manager compared to 31% of firms without such controls.

CHART 4
TOP THREE METHODS OF EXPOSING FRAUD

METHOD OF DISCOVERY	PERCENTAGE OF UNCOVERED FRAUDS THAT WERE EXPOSED VIA THIS METHOD
Whistleblower	41%
External audit	31%
Internal audit	25%

CHART 5
PERPETRATORS OF KNOWN FRAUDS

GROUP	PERCENTAGE OF FIRMS HIT BY FRAUD WHERE SOMEONE IN THIS GROUP WAS A KEY PERPETRATOR
Junior employees	45%
Vendors/Suppliers	18%
Agents and/or Intermediaries	23%
Senior or middle management	36%
JV partners	8%
Regulators	7%
Customers	5%
Government officials	3%
Other	3%



Conclusion

From widespread corruption allegations in FIFA to laundering Russian mafia money in high-end London real estate, fraud is never far from the headlines. What our report and our day-to-day experience tell us is that despite companies making greater and more sophisticated efforts to combat fraud, it remains a serious business threat that cannot be completely eliminated. The adverse impacts of such incidents cannot be underestimated.

Fraud is virulent, and perpetrators adapt their methods on an ongoing basis. As one barrier is put up, fraudsters will seek and find an alternative weakness to exploit. This type of persistence and stealth is especially evident in the creative ways digital networks are constantly being attacked and often penetrated.

In the face of such motivated adversaries, businesses must implement procedures that can help them identify, mitigate and manage fraud risks. There is no absolute or perfect solution, and the techniques employed by fraudsters evolve and are ever-changing. As a result, energy and effort has to be focused not only on prevention, but also on response in the event that such fraudulent efforts are able to circumvent processes and other preventive measures. Being positioned to implement a rapid and decisive response is equally as critical to mitigating such risks. Fraud is not going away and continues to be on the rise, but the well-prepared business can do much to stay one step ahead and be positioned to eliminate or mitigate it.

