BUSINESS FRAUD WATCH

A BASELINE OF FRAUD AND CYBERCRIME RESEARCH IN 2022

MONDAY 6 JUNE 2022

INTRODUCTION

This is the first in a series of six-weekly updates for businesses (especially SMEs) on the current frauds that might affect them. In this update we set out our current understanding of fraud and cybercrime affecting businesses based on recent research undertaken by others.

Future updates will be based on information shared by members our new Business Fraud Watch network which has been set up to support and protect UK businesses (especially SMEs).

Updates will be issued after each meeting to help warn businesses about the risks they may face. We encourage all businesses – and everyone who works with them or otherwise supports them – to use and share these updates.

OUR RESEARCH

We commissioned independent market research firm Savanta to survey 1,009 businesses (of whom 754 were SMEs) in April. We found:

- Fraud is the most disruptive crime faced by SMEs. It is more disruptive than cybercrime, theft, anti-social behaviour, criminal damage, burglary, assault or robbery. For all businesses, cybercrime is the most disruptive crime faced, followed by fraud.
- Larger businesses were more likely to suffer crime in the last two years than SMEs. 46% of all businesses (and 37% of SMEs) had suffered a crime in the last two years.
- For all businesses, a lack of understanding about how fraud could affect business was the biggest barrier to tackling fraud. Followed by the cost of taking action.
- Businesses were asked: What do you think is the single biggest barrier to businesses prioritising tackling fraud, including online fraud?

	SMEs	ALL businesses
Lack of understanding how fraud could affect the business	21%	20%
Cost of taking action	20%	19%
Reimbursed by banks	12%	12%
Prioritise other crimes over fraud	11%	12%
Lack of time	10%	11%
Lack of staff resources	9%	9%
Other	1%	1%
Don't know	16%	15%

- All businesses are twice as likely than not to view fraud as a major risk to growing their business in the next two years. 48% of all businesses (and 44% of small businesses) (agreed or strongly agreed with the statement that 'fraud is a major risk to growing our business in the next two years'. 23% disagreed (20% of small businesses).

OCCUPATIONAL FRAUD 2022: A REPORT TO THE NATIONS

The Association of Certified Fraud Examiners (ACFE) surveys its members about frauds that are committed by individuals against the organisations that employ them. It found:

- Employees play a key role in detecting insider fraud. 42% of frauds were detected by tips. More than half of all tips came from employees. It takes a typical insider fraud 12 months to be detected.
- Collaboration between perpetrators is on the rise. 58% of insider frauds involved collaboration between 2 or more perpetrators (compared with 42% 10 years ago).
- Longer term employees who commit fraud steal almost 3 times as much as more recent employees. They also display common warning signs more consistently. These include living beyond means, usually close association with supplier or customer, unwillingness to share duties, bullying or intimation, irritability/suspiciousness/ defensiveness and recent divorce or family problems.
- Basic anti-fraud controls that are consistently applied are key to effective fraud prevention. 29% of frauds occurred due to a lack of internal controls; 20% were due to the override of existing controls. 53% of SMEs had the most common anti-fraud controls vs. 90% of larger businesses. Anti-fraud controls = lower fraud losses + quicker detection.
- SMEs generally have fewer anti-fraud controls than larger businesses. The average financial loss to an SME from insider fraud is nearly 9% higher than against a larger business. Misappropriation of non-cash assets was half as likely in SMEs. Corruption as involved in only 24% of SME cases.

More information: Visit the ACFE website

GLOBAL ECONOMIC CRIME SURVEY 2022

The results of PwC's survey are based on responses from nearly 1,300 organisations across 53 countries. It found:

- The external fraud threat to businesses is increasing. Cybercrime is perceived to be the biggest threat, followed by customer fraud and asset misappropriation. 43% of the most disruptive or serious frauds were committed by an external perpetrator.
- Two-thirds of businesses that experienced fraud discovered their most disruptive incident through fundamental controls.
- Nearly two-thirds of technology, media and telecommunications companies experienced some form of fraud – the highest of any industry.
- Digital platform and supply chain related fraud risks are increasing. 4 in 10 businesses that had suffered a fraud in the last two years had experienced some form of fraud related to the digital platforms they rely on – often know-your-customer breaches, disinformation and money laundering.
- Few businesses say they are aware of the risks within their own supply chain. 1 in 8 businesses experienced new incidents of supply chain fraud as a result of COVID-19 related disruption.

More information: Visit the PWC website

CYBER SECURITY BREACHES SURVEY 2022

The Department for Digital, Culture, Media & Sport's annual study explores how businesses, charities and educational institutions approach cyber security and react to cyber-attacks. It found:

- 39% of UK businesses identified a cyber-attack in the last year. Of these, 31% were attacked at least once a week. Phishing attempts (83%) were most common; 21% were more sophisticated attacks such as denial-of-service, malware and ransomware. The average cost to medium and large businesses was £19,400 per case.
- 49% of businesses have acted on at least 5 of the '10 steps to cyber security' guide recommended by government. 58% of SMEs outsource their IT and cyber security.
- Some businesses face increased risks because they use unsupported software and bring-your-own-devices by staff. 46% of micro, 42% of small and 43% of medium-sized businesses now have staff using their own devices to carry out work-related activities. 16% of micro, 20% of small and 25% of medium-sized businesses have older, unsupported, versions of windows installed.
- Challenges remain on cyber security decision-making, especially for SMEs. Smaller organisations were generally found to take little pro-active action on cyber security, driven by a lack of internal knowledge, competing priorities for budgets, and a fear of the technicalities of cyber security.

More information: Visit the DCMS website