UNITED KINGDOM REPORT CARD

Top responses given by survey respondents.

Fraud

Percentage of respondents affected by fraud in the past 12 months.

▲ 16% points above 2015

▲ 8% points above global average of 82%

			Global avg.
MOST COMMON TYPES OF FRAUD	Theft of physical assets or stock	41%	29%
	Misappropriation of company funds	37%	18%
	Information theft, loss, or attack *(e.g., data theft)*	24%	24%
	Market collusion *(e.g., price fixing)*	24%	17%
MOST COMMON PERPETRATORS	Junior employees of our own company	41%	39%
	Senior or middle management employees of our own companys	32%	30%
	Ex-employees	30%	27%
	Freelance/temporary employees	27%	27%
	Agents and/or intermediaries *(i.e., a third party working on behalf of your company)*	27%	27%
	Customers	27%	19%
MOST COMMON ANTI-FRAUD MEASURES	Information *(IT security, technical countermeasures)*	84%	82%
	Management *(management controls, incentives, external supervision such as audit committee)*	80%	74%
	IP *(intellectual property risk assessment and trademark monitoring program)*	76%	75%
MOST COMMON MEANS OF DISCOVERY	By a whistle-blower at our company	50%	44%

Cyber Security

Percentage of respondents that experienced a cyber incident in the past 12 months.

▲ 7% points above global average of 85%

			Global avg.
MOST COMMON TYPES OF CYBER INCIDENT	Virus/worm infestation	33%	33%
	Insider theft of customer or employee data	27%	19%
	Data breach resulting in loss of customer or employee data	22%	23%
	Data deletion or loss due to system issues	22%	24%
MOST COMMON PERPETRATORS	Ex-employees	29%	20%
MOST COMMON TARGET	Customer records	42%	51%
	Trade secrets/R&D/IP	42%	40%
	Company/employee identity	40%	36%
MOST COMMON PARTY TO CONTACT WHEN A CYBER INCIDENT OCCURRED	IT service vendor	33%	27%

Security

Percentage of respondents that experienced a security incident in the past 12 months.

▲ 14% points above global average of 68%

			Global avg.
MOST COMMON TYPES OF SECURITY INCIDENTS	Theft or loss of IP	51%	38%
	Geographic and political risk *(i.e., operating in areas of conflict)*	39%	22%
	Workplace violence	29%	23%
MOST COMMON PERPETRATORS	Ex-employees	28%	23%
RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY VULNERABLE TO THE FOLLOWING SECURITY RISKS	Workplace violence	31%	27%
	Theft or loss of IP	24%	19%
	Environmental risk *(including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.)*	24%	20%
	Geographic and political risk *(i.e., operating in areas of conflict)*	24%	12%
	Terrorism, including domestic and international events	24%	18%