CHINA REPORT CARD

Top responses given by survey respondents.

Fraud

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

▲ **13%** points above 2015
▲ **4%** points above global average of 82%

Global avg.

MOST COMMON TYPES OF FRAUD			
Regulatory or compliance breach	**41%**	21%
Vendor, supplier, or procurement fraud	**37%**	26%
Theft of physical assets or stock	**25%**	29%
Information theft, loss, or attack *(e.g., data theft)*	**25%**	24%
Corruption and bribery	**25%**	15%
Market collusion *(e.g., price fixing)*	**25%**	17%
Misappropriation of company funds	**25%**	18%

MOST COMMON PERPETRATORS		
Joint venture partners *(i.e., a partner who provides manufacturing or other business function, or a franchisee)*	**52%**	23%
Junior employees of our own company	**48%**	39%
Agents and/or intermediaries *(i.e., a third party working on behalf of your company)*	**43%**	27%
Vendors/suppliers *(i.e., a provider of technology or services to your company)*	**36%**	26%
Senior or middle management employees of our own company	**34%**	30%

MOST COMMON ANTI-FRAUD MEASURES *Percentage of respondents who have implemented the anti-fraud measure.*		
Partners, clients, and vendors *(due diligence)*	**90%**	77%
Assets *(physical security systems, stock inventories, tagging, asset register)*	**86%**	79%
Board of director engagement in cyber security policies and procedures	**86%**	75%

MOST COMMON MEANS OF DISCOVERY		
By a whistle-blower at our company	**55%**	44%
Through an external audit	**55%**	36%

Cyber Security

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

▲ **1%** point above global average of 85%

Global avg.

MOST COMMON TYPES OF CYBER INCIDENT		
Email-based phishing attack	**41%**	26%
Virus/worm infestation	**39%**	33%
Data deletion or corruption by malware or system issue	**39%**	22%

MOST COMMON PERPETRATORS		
Freelance/temporary employees	**25%**	14%

MOST COMMON TARGET		
Customer records	**82%**	51%
Trade secrets/R&D/IP	**59%**	40%
Employee records	**41%**	40%
Company/employee identity	**41%**	36%

MOST COMMON PARTY TO CONTACT WHEN A CYBER INCIDENT OCCURRED		
IT service vendor	**34%**	27%

Security

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

▲ **7%** points above global average of 68%

Global avg.

MOST COMMON TYPES OF SECURITY INCIDENTS		
Environmental risk *(including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.)*	**45%**	27%
Theft or loss of IP	**41%**	38%
Geographic and political risk *(i.e., operating in areas of conflict)*	**25%**	22%

MOST COMMON PERPETRATORS		
Competitors	**21%**	12%

RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY VULNERABLE TO THE FOLLOWING SECURITY RISKS		
Workplace violence	**33%**	27%
Environmental risk *(including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.)*	**31%**	20%
Terrorism, including domestic and international events	**31%**	18%