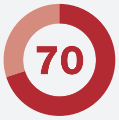
CONSTRUCTION, ENGINEERING, AND INFRASTRUCTURE

Top responses given by survey respondents.

Fraud



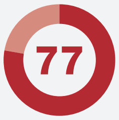
Percentage of respondents affected by fraud in the past 12 months.

▼ 5% points below 2015

▼ 12% points below global average of 82%

			Global avg.
MOST COMMON TYPES OF FRAUD	Vendor, supplier, or procurement fraud	**28%**	26%
	Internal financial fraud *(manipulation of company results)*	**21%**	20%
	Corruption and bribery	**19%**	15%
	Misappropriation of company funds	**19%**	18%
	Theft of physical assets or stock	**19%**	29%
MOST COMMON PERPETRATORS	Junior employees	**45%**	39%
	Ex-employees	**33%**	27%
	Senior or middle management employees	**30%**	30%
	Freelance/temporary employees	**30%**	27%
	Vendors/suppliers	**30%**	26%
MOST COMMON ANTI-FRAUD MEASURES *Percentage of respondents who have implemented the anti-fraud measure.*	Staff *(training, whistle-blower hotline),*	**81%**	76%
	Staff *(background screening)*	**79%**	74%
	Partners, clients, and vendors *(due diligence)*	**79%**	77%
	Information *(IT security, technical countermeasures)*	**79%**	82%
	Risk *(risk officer and risk management system)*	**79%**	78%
MOST COMMON MEANS OF DISCOVERY	Through an internal audit	**38%**	39%

Cyber Security

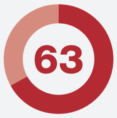


Percentage of respondents that experienced a cyber incident in the past 12 months.

▼ 8% points below global average of 85%

			Global avg.
MOST COMMON TYPES OF CYBER INCIDENT	Virus/worm infestation	**35%**	33%
	Email-based phishing attack	**30%**	26%
	Data deletion or loss due to system issues	**30%**	24%
MOST COMMON PERPETRATORS	Ex-Employees	**20%**	20%
MOST COMMON TARGET	Customer records	**59%**	51%
	Employee records	**45%**	40%
	Physical assets/money	**43%**	38%

Security



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

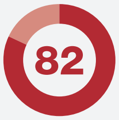
▼ 5% points below global average of 68%

			Global avg.
MOST COMMON TYPES OF SECURITY INCIDENTS	Environmental risk	**33%**	27%
	Theft or loss of IP	**32%**	38%
	Geographic and political risk	**23%**	22%
	Workplace violence	**23%**	23%
MOST COMMON PERPETRATORS	Ex-Employees	**25%**	23%
RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY VULNERABLE TO THE FOLLOWING SECURITY RISKS	Theft or loss of intellectual property	**18%**	19%
	Environmental risk	**18%**	20%
	Workplace violence	**12%**	27%

CONSUMER GOODS

Top responses given by survey respondents.

Fraud



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

▲ 10% points above 2015

= Equal to global average of 82%

			Global avg.
MOST COMMON TYPES OF FRAUD	Information theft, loss, or attack *(e.g., data theft)*	**32%**	24%
	Theft of physical assets or stock	**28%**	29%
	Vendor, supplier, or procurement fraud	**28%**	26%
MOST COMMON PERPETRATORS	Agents and/or intermediaries	**43%**	27%
	Junior employees	**37%**	39%
	Vendors/suppliers	**35%**	26%
	Joint venture partners	**31%**	23%
	Senior or middle management employees	**24%**	30%
MOST COMMON ANTI-FRAUD MEASURES *Percentage of respondents who have implemented the anti-fraud measure.*	Information *(IT security, technical countermeasures)*	**77%**	82%
	Assets *(physical security systems, stock inventories, tagging, asset register)*	**77%**	79%
	Board of director engagement in cyber security policies and procedures	**73%**	75%
MOST COMMON MEANS OF DISCOVERY	By a whistle-blower at our company	**53%**	44%

Cyber Security

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

▼ 2% points below global average of 85%

			Global avg.
MOST COMMON TYPES OF CYBER INCIDENT	Email-based phishing attack	**28%**	26%
	Data breach resulting in loss of customer or employee data	**27%**	23%
	Virus/worm infestation	**27%**	33%
MOST COMMON PERPETRATORS	Ex-employees	**28%**	20%
MOST COMMON TARGET	Customer records	**62%**	51%
	Trade secrets/R&D/IP	**54%**	40%
	Company/employee identity	**30%**	36%

Security

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

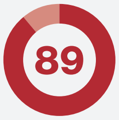
▲ 7% points above global average of 68%

			Global avg.
MOST COMMON TYPES OF SECURITY INCIDENTS	Theft or loss of IP	**27%**	38%
	Environmental risk	**27%**	27%
	Terrorism	**20%**	15%
	Geographic and political risk	**20%**	22%
MOST COMMON PERPETRATORS	Ex-employees	**31%**	23%
RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY VULNERABLE TO THE FOLLOWING SECURITY RISKS	Theft or loss of IP	**22%**	19%
	Workplace violence	**20%**	27%
	Environmental risk	**18%**	20%

FINANCIAL SERVICES REPORT CARD

Top responses given by survey respondents.

Fraud



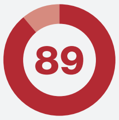
Percentage of respondents affected by fraud in the past 12 months.

▲ 19% points above 2015

▲ 7% points above global average of 82%

			Global avg.
MOST COMMON TYPES OF FRAUD	Theft of physical assets or stock	39%	29%
	Vendor, supplier, or procurement fraud	32%	26%
	IP theft *(e.g., of trade secrets, piracy, or counterfeiting)*	27%	16%
MOST COMMON PERPETRATORS	Junior employees	38%	39%
	Ex-employees	34%	27%
	Senior or middle management employees	32%	30%
	Vendors/suppliers	24%	26%
	Freelance/temporary employees	22%	27%
MOST COMMON ANTI-FRAUD MEASURES *Percentage of respondents who have implemented the anti-fraud measure.*	Risk *(risk officer and risk management system)*	88%	78%
	Information *(IT security, technical countermeasures)*	84%	82%
	IP *(IP risk assessment and trademark monitoring program)*	84%	75%
MOST COMMON MEANS OF DISCOVERY	Through an external audit	40%	36%

Cyber Security

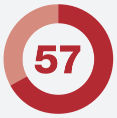


Percentage of respondents that experienced a cyber incident in the past 12 months.

▲ 4% points above global average of 85%

			Global avg.
MOST COMMON TYPES OF CYBER INCIDENT	Data deletion or loss due to system issues	30%	24%
	Email-based phishing attack	27%	26%
	Virus/worm infestation	27%	33%
MOST COMMON PERPETRATORS	Ex-employees	28%	20%
MOST COMMON TARGET	Customer records	42%	51%
	Trade secrets/R&D/IP	38%	40%
	Company/employee identity	38%	36%

Security



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

▼ 11% points below global average of 68%

			Global avg.
MOST COMMON TYPES OF SECURITY INCIDENTS	Theft or loss of IP	34%	38%
	Geographic and political risk	20%	22%
	Workplace violence	16%	23%
MOST COMMON PERPETRATORS	Ex-employees	31%	23%
RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY VULNERABLE TO THE FOLLOWING SECURITY RISKS	Terrorism	21%	18%
	Workplace violence	20%	27%
	Theft or loss of IP	18%	19%

HEALTHCARE, PHARMACEUTICALS, AND BIOTECHNOLOGY

Top responses given by survey respondents.

Fraud

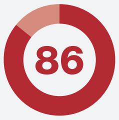
Percentage of respondents affected by fraud in the past 12 months.

▲ 11% points above 2015

▼ 2% points below global average of 82%

			Global avg.
MOST COMMON TYPES OF FRAUD	Vendor, supplier, or procurement fraud	**37%**	26%
	Theft of physical assets or stock	**31%**	29%
	Misappropriation of company funds	**27%**	18%
MOST COMMON PERPETRATORS	Junior employees	**44%**	39%
	Agents and/or intermediaries	**37%**	27%
	Senior or middle management employees	**34%**	30%
	Ex-employees	**29%**	27%
	Joint venture partners	**27%**	23%
MOST COMMON ANTI-FRAUD MEASURES *Percentage of respondents who have implemented the anti-fraud measure.*	Financial *(financial controls, fraud detection, internal audit, external audit, anti-money laundering policies)*	**94%**	77%
	Information *(IT security, technical countermeasures)*	**92%**	82%
	Management *(management controls, incentives, external supervision such as audit committee)*	**92%**	74%
	Risk *(risk officer and risk management system)*	**92%**	78%
MOST COMMON MEANS OF DISCOVERY	By a whistle-blower at our company	**63%**	44%

Cyber Security

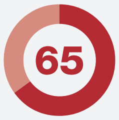


Percentage of respondents that experienced a cyber incident in the past 12 months.

▲ 1% point above global average of 85%

			Global avg.
MOST COMMON TYPES OF CYBER INCIDENT	Virus/worm infestation	**45%**	33%
	Email-based phishing attack	**35%**	26%
	Data breach resulting in loss of customer or employee data	**29%**	23%
	Data deletion or corruption by malware or system issue	**29%**	22%
MOST COMMON PERPETRATORS	Ex-employees	**20%**	20%
MOST COMMON TARGET	Customer records	**48%**	51%
	Employee records	**48%**	40%
	Company/employee identity	**45%**	36%

Security



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

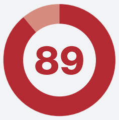
▼ 3% points below global average of 68%

			Global avg.
MOST COMMON TYPES OF SECURITY INCIDENTS	Environmental risk	**35%**	27%
	Theft or loss of intellectual property	**31%**	38%
	Geographic and political risk	**27%**	22%
MOST COMMON PERPETRATORS	Freelance/temporary employees	**15%**	16%
RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY VULNERABLE TO THE FOLLOWING SECURITY RISKS	Workplace violence	**35%**	27%
	Terrorism	**25%**	18%
	Theft or loss of IP	**20%**	19%
	Environmental risk	**20%**	20%

MANUFACTURING

Top responses given by survey respondents.

Fraud



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

▲ 7% points above higher than 2015

▲ 7% points above global average of 82%

			Global avg.
MOST COMMON TYPES OF FRAUD	Information theft, loss, or attack *(e.g., data theft)*	30%	24%
	Regulatory or compliance breach	30%	21%
	IP theft *(e.g., of trade secrets, piracy or counterfeiting)*	26%	16%
MOST COMMON PERPETRATORS	Junior employees	39%	39%
	Freelance/temporary employees	37%	27%
	Senior or middle management employees	33%	30%
	Ex-employees	33%	27%
	Vendors/suppliers	33%	26%
MOST COMMON ANTI-FRAUD MEASURES *Percentage of respondents who have implemented the anti-fraud measure.*	Management *(management controls, incentives, external supervision such as audit committee)*	88%	74%
	Information *(IT security, technical countermeasures)*	86%	82%
	Staff *(training, whistle-blower hotline)*	79%	74%
MOST COMMON MEANS OF DISCOVERY	Through an internal audit	51%	39%

Cyber Security

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

▲ 6% points above global average of 85%

			Global avg.
MOST COMMON TYPES OF CYBER INCIDENT	Virus/worm infestation	39%	33%
	Data breach resulting in loss of IP/trade secrets/R&D	35%	19%
	Email-based phishing attack	35%	26%
MOST COMMON PERPETRATORS	Agents and/or intermediaries	23%	13%
MOST COMMON TARGET	Customer records	63%	51%
	Trade secrets/R&D/IP	52%	40%
	Employee records	44%	40%

Security

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

▲ 13% points above global average of 68%

			Global avg.
MOST COMMON TYPES OF SECURITY INCIDENTS	Theft or loss of IP	56%	38%
	Environmental risk	28%	27%
	Workplace violence	26%	23%
MOST COMMON PERPETRATORS	Competitors	24%	12%
RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY VULNERABLE TO THE FOLLOWING SECURITY RISKS	Environmental risk	28%	20%
	Workplace violence	21%	27%
	Theft or loss of IP	21%	19%

NATURAL RESOURCES

Top responses given by survey respondents.

Fraud

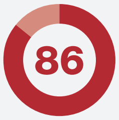
Percentage of respondents affected by fraud in the past 12 months.

▲ 3% points above 2015

▼ 2% points below global average of 82%

			Global avg.
MOST COMMON TYPES OF FRAUD	Vendor, supplier, or procurement fraud	30%	26%
	Money laundering	30%	15%
	Management conflict of interest	28%	21%
MOST COMMON PERPETRATORS	Freelance/temporary employees	35%	27%
	Junior employees	30%	39%
	Ex-employees	30%	27%
	Joint venture partners	30%	23%
	Senior or middle management employees	28%	30%
	Regulators	28%	14%
MOST COMMON ANTI-FRAUD MEASURES *Percentage of respondents who have implemented the anti-fraud measure.*	Information *(IT security, technical countermeasures)*	80%	82%
	IP *(IP risk assessment and trademark monitoring program)*	80%	75%
	Financial *(financial controls, fraud detection, internal audit, external audit, anti-money laundering policies)*	78%	77%
	Partners, clients, and vendors *(due diligence)*	78%	77%
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.

▲ 1% point above global average of 85%

			Global avg.
MOST COMMON TYPES OF CYBER INCIDENT	Virus/worm infestation	36%	33%
	Lost equipment with sensitive data	30%	17%
	Data breach resulting in loss of customer or employee data	24%	23%
	Data breach resulting in loss of IP/trade secrets/R&D	24%	17%
	Data deletion by malicious insider	24%	19%
MOST COMMON PERPETRATORS	Ex-employees	19%	20%
MOST COMMON TARGET	Employee records	58%	40%
	Customer records	53%	51%
	Physical assets/money	47%	38%

Security

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

▲ 2% points above global average of 68%

			Global avg.
MOST COMMON TYPES OF SECURITY INCIDENTS	Theft or loss of IP	40%	38%
	Environmental risk	38%	27%
	Workplace violence	36%	23%
MOST COMMON PERPETRATORS	Permanent employees of our own company	26%	17%
RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY VULNERABLE TO THE FOLLOWING SECURITY RISKS	Workplace violence	36%	27%
	Environmental risk	26%	20%
	Theft or loss of intellectual property	24%	19%

PROFESSIONAL SERVICES

Top responses given by survey respondents.

Fraud

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

▲ 12% points above 2015

▲ 2% points above global average of 82%

			Global avg.
MOST COMMON TYPES OF FRAUD	Management conflict of interest	**29%**	21%
	Theft of physical assets or stock	**29%**	29%
	Information theft, loss, or attack *(background screening)*	**20%**	24%
MOST COMMON PERPETRATORS	Junior employees	**35%**	39%
	Freelance/temporary employees	**28%**	27%
	Ex-employees	**26%**	27%
	Senior or middle management employees	**23%**	30%
	Customers	**21%**	19%
MOST COMMON ANTI-FRAUD MEASURES *Percentage of respondents who have implemented the anti-fraud measure.*	Partners, clients, and vendors *(due diligence)*	**82%**	77%
	Risk *(risk officer and risk management system)*	**80%**	78%
	Assets *(physical security systems, stock inventories, tagging, asset register)*	**78%**	79%
MOST COMMON MEANS OF DISCOVERY	By a whistle-blower at our company	**42%**	44%

Cyber Security

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

▼ 1% point below global average of 85%

			Global avg.
MOST COMMON TYPES OF CYBER INCIDENT	Virus/worm infestation	**35%**	33%
	Denial of service attack	**20%**	14%
	Data deletion or corruption by malware or system issue	**20%**	22%
MOST COMMON PERPETRATORS	Ex-Employees	**23%**	20%
MOST COMMON TARGET	Customer records	**53%**	51%
	Trade secrets/R&D/IP	**30%**	40%
	Company/employee identity	**28%**	36%
	Physical assets/money	**28%**	38%

Security

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

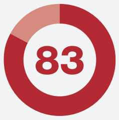
▼ 5% points below global average of 68%

			Global avg.
MOST COMMON TYPES OF SECURITY INCIDENTS	Theft or loss of IP	**35%**	38%
	Environmental risk	**22%**	27%
	Workplace violence	**20%**	23%
MOST COMMON PERPETRATORS	Ex-Employees	**38%**	23%
RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY VULNERABLE TO THE FOLLOWING SECURITY RISKS	Workplace violence	**27%**	27%
	Terrorism	**14%**	18%
	Theft or loss of IP	**10%**	19%
	Environmental risk	**10%**	20%

RETAIL, WHOLESALE, AND DISTRIBUTION

Top responses given by survey respondents.

Fraud



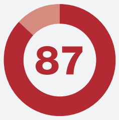
Percentage of respondents affected by fraud in the past 12 months.

▲ 4% points above 2015

▲ 1% point above global average of 82%

			Global avg.
MOST COMMON TYPES OF FRAUD	Theft of physical assets or stock	33%	29%
	Misappropriation of company funds	25%	18%
	Information theft, loss, or attack *(e.g., data theft),*	17%	24%
	Vendor, supplier, or procurement fraud	17%	26%
MOST COMMON PERPETRATORS	Junior employees	37%	39%
	Senior or middle management employees	33%	30%
	Vendors/suppliers	33%	26%
	Agents and/or intermediaries	26%	27%
	Joint venture partners	26%	23%
	Customers	26%	19%
MOST COMMON ANTI-FRAUD MEASURES *Percentage of respondents who have implemented the anti-fraud measure.*	Assets *(physical security systems, stock inventories, tagging, asset register)*	85%	79%
	Financial *(financial controls, fraud detection, internal audit, external audit, anti-money laundering policies)*	83%	77%
	Information *(IT security, technical countermeasures)*	83%	82%
MOST COMMON MEANS OF DISCOVERY	By a whistle-blower at our company	42%	44%

Cyber Security



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

▲ 2% points above global average of 85%

			Global avg.
MOST COMMON TYPES OF CYBER INCIDENT	Email-based phishing attack	25%	26%
	Insider theft of customer or employee data	21%	19%
	Data breach resulting in loss of customer or employee data	19%	23%
	Data breach resulting in loss of IP/trade secrets/R&D	19%	17%
	Denial of service attack	19%	14%
MOST COMMON PERPETRATORS	Freelance/temporary employees	13%	14%
	Ex-employees	13%	20%
	Joint venture partners	13%	6%
	Accidental placement of sensitive data that was indexed by a search engine *(e.g., Google)*	13%	10%
MOST COMMON TARGET	Customer records	44%	51%
	Employee records	40%	40%
	Physical assets/money	36%	38%

Security

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

▲ 11% points above global average of 68%

			Global avg.
MOST COMMON TYPES OF SECURITY INCIDENTS	Theft or loss of IP	38%	38%
	Terrorism	19%	15%
	Geographic and political risk	19%	22%
MOST COMMON PERPETRATORS	Freelance/temporary employees	22%	16%
RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY VULNERABLE TO THE FOLLOWING SECURITY RISKS	Terrorism	31%	18%
	Workplace violence	29%	27%
	Geographic and political risk	19%	12%

TECHNOLOGY, MEDIA, AND TELECOMS

Top responses given by survey respondents.

Fraud

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

= equal to 2015

▼ 3% points below global average of 82%

			Global avg.
MOST COMMON TYPES OF FRAUD	Theft of physical assets or stock	35%	29%
	Information theft, loss, or attack	30%	24%
	Management conflict of interest	25%	21%
MOST COMMON PERPETRATORS	Junior employees	42%	39%
	Senior or middle management employees	36%	30%
	Ex-employees	27%	27%
	Freelance/temporary employees	22%	27%
	Vendors/suppliers	22%	26%
	Regulators	22%	14%
MOST COMMON ANTI-FRAUD MEASURES *Percentage of respondents who have implemented the anti-fraud measure.*	Assets *(physical security systems, stock inventories, tagging, asset register)*	82%	79%
	Financial *(financial controls, internal/external audit, anti-money laundering policies)*	79%	77%
	Partners, clients, and vendors *(due diligence)*	79%	77%
	Risk *(risk officer and risk management system)*	79%	78%
MOST COMMON MEANS OF DISCOVERY	Through an internal audit	40%	39%

Cyber Security

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

▼ 8% points below global average of 85%

			Global avg.
MOST COMMON TYPES OF CYBER INCIDENT	Virus/worm infestation	37%	33%
	Email-based phishing attack	32%	26%
	Data deletion or loss due to system issues	23%	24%
MOST COMMON PERPETRATORS	Freelance/temporary employees	23%	14%
MOST COMMON TARGET	Physical assets/money	48%	38%
	Trade secrets/R&D/IP	43%	40%
	Company/employee identity	43%	36%

Security

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

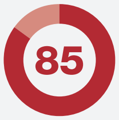
▲ 4% points above global average of 68%

			Global avg.
MOST COMMON TYPES OF SECURITY INCIDENTS	Theft or loss of IP	46%	38%
	Environmental risk	33%	27%
	Geographic and political risk	26%	22%
MOST COMMON PERPETRATORS	Freelance/temporary employees	27%	16%
RESPONDENTS COMPANIES ARE MOST LIKELY TO FEEL HIGHLY VULNERABLE TO THE FOLLOWING SECURITY RISKS	Workplace violence	28%	27%
	Terrorism	21%	18%
	Environmental risk	18%	20%

TRANSPORTATION, LEISURE, AND TOURISM

Top responses given by survey respondents.

Fraud



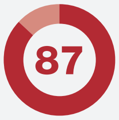
Percentage of respondents affected by fraud in the past 12 months.

▲ 10% points above 2015

▲ 3% points above global average of 82%

			Global avg.
MOST COMMON TYPES OF FRAUD	Theft of physical assets or stock	33%	29%
	Vendor, supplier, or procurement fraud	30%	26%
	Regulatory or compliance breach	26%	21%
MOST COMMON PERPETRATORS	Junior employees	39%	39%
	Agents and/or intermediaries	35%	27%
	Freelance/temporary employees	30%	27%
	Senior or middle management employees	26%	30%
	Joint venture partners	22%	23%
MOST COMMON ANTI-FRAUD MEASURES *Percentage of respondents who have implemented the anti-fraud measure.*	Information *(IT security, technical countermeasures)*	89%	82%
	Assets *(physical security systems, stock inventories, tagging, asset register)*	87%	79%
	Board of director engagement in cyber security policies and proceduress	85%	75%
	Staff *(background screening)*	85%	74%
	Risk *(risk officer and risk management system)*	78%	78%
MOST COMMON MEANS OF DISCOVERY	By a whistle-blower at our company	46%	44%

Cyber Security



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

▲ 2% points above global average of 85%

			Global avg.
MOST COMMON TYPES OF CYBER INCIDENT	Virus/worm infestation	37%	33%
	Alteration or change of customer data	31%	16%
	Data deletion or loss due to system issues	30%	24%
MOST COMMON PERPETRATORS	Ex-employees	19%	20%
MOST COMMON TARGET	Customer records	51%	51%
	Physical assets/money	51%	38%
	Employee records	45%	40%
	Trade secrets/R&D/IP	45%	40%

Security

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

▲ 2% points above global average of 68%

			Global avg.
MOST COMMON TYPES OF SECURITY INCIDENTS	Theft or loss of IP	43%	38%
	Workplace violence	30%	23%
	Environmental risk	26%	27%
MOST COMMON PERPETRATORS	Permanent employees of our own company	24%	17%
	Ex-employees	24%	23%
RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY VULNERABLE TO THE FOLLOWING SECURITY RISKS	Workplace violence	41%	27%
	Environmental risk	35%	20%
	Theft or loss of IP	31%	19%