CANADA REPORT CARD

Top responses given by survey respondents.

Fraud

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

▲ 23% points above 2015

▲ 6% points above global average of 82%

			Global avg.
MOST COMMON TYPES OF FRAUD	Theft of physical assets or stock	34%	29%
	Information theft, loss, or attack *(e.g., data theft)*	32%	24%
	Regulatory or compliance breach	32%	21%
	Vendor, supplier, or procurement fraud	32%	26%
	Misappropriation of company funds	32%	18%
MOST COMMON PERPETRATORS	Senior or middle management employees of our own company	47%	30%
	Junior employees of our own company	39%	39%
	Freelance/temporary employees	36%	27%
	Ex-employees	36%	27%
	Agents and/or intermediaries *(i.e., a third party working on behalf of your company)*	36%	27%
MOST COMMON ANTI-FRAUD MEASURES *Percentage of respondents who have implemented the anti-fraud measure.*	Risk *(risk officer and risk management system)*	90%	78%
	Management *(management controls, incentives, external supervision such as audit committee)*	88%	74%
	Information *(IT security, technical countermeasures)*	86%	82%
	Assets *(physical security systems, stock inventories, tagging, asset register)*	86%	79%
	Partners, clients, and vendors *(due diligence)*	85%	77%
MOST COMMON MEANS OF DISCOVERY	By a whistle-blower at our company	44%	44%

Cyber Security

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

= equal to global average of 85%

			Global avg.
MOST COMMON TYPES OF CYBER INCIDENT	Virus/worm attack	41%	33%
	Lost equipment with sensitive data	39%	17%
	Data deletion or corruption by malware or system issue	34%	22%
	Data breach resulting in loss of IP/trade secrets/R&D	34%	19%
MOST COMMON PERPETRATORS	Permanent employees of our own company	20%	10%
MOST COMMON TARGET	Customer records	57%	51%
	Physical assets/money	57%	38%
	Trade secrets/R&D/IP	51%	40%
MOST COMMON PARTY TO CONTACT WHEN A CYBER INCIDENT OCCURRED	Incident response firm	20%	14%
	IT service vendor	20%	27%

Security

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

▲ 10% points above global average of 68%

			Global avg.
MOST COMMON TYPES OF SECURITY INCIDENTS	Theft or loss of IP	49%	38%
	Environmental risk *(including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.)*	46%	27%
	Geographic and political risk *(i.e., operating in areas of conflict)*	27%	22%
MOST COMMON PERPETRATORS	Ex-employees	28%	23%
RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY VULNERABLE TO THE FOLLOWING SECURITY RISKS	Workplace violence	32%	27%
	Environmental risk *(including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.)*	29%	20%
	Terrorism, including domestic and international events	24%	18%

UNITED STATES REPORT CARD

Top responses given by survey respondents.

Fraud

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

▲ 5% points above 2015

▼ 2% points below global average of 82%

			Global avg.
MOST COMMON TYPES OF FRAUD	IP theft *(e.g. of trade secrets)*, piracy, or counterfeiting	27%	16%
	Information theft, loss, or attack *(e.g., data theft)*	24%	24%
	Management conflict of interest	24%	21%
MOST COMMON PERPETRATORS	Junior employees of our own company	36%	39%
	Senior or middle management employees of our own companys	32%	30%
	Ex-employees	30%	27%
	Vendors/suppliers *(i.e., a provider of technology or services to your company)*	21%	26%
	Freelance/temporary employees	17%	27%
	Customers	17%	19%
MOST COMMON ANTI-FRAUD MEASURES	Information *(IT security, technical countermeasures)*	91%	82%
	Financial *(financial controls, fraud detection, internal audit, external audit, anti-money laundering policies)*	86%	77%
	Assets *(physical security systems, stock inventories, tagging, asset register)*	85%	79%
MOST COMMON MEANS OF DISCOVERY	Through an internal audit	49%	39%

Cyber Security

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

▲ 3% points above global average of 85%

			Global avg.
MOST COMMON TYPES OF CYBER INCIDENT	Virus/worm infestation	42%	33%
	Data deletion or loss due to system issues	26%	24%
	Email-based phishing attack	21%	26%
MOST COMMON PERPETRATORS	Ex-employees	19%	20%
MOST COMMON TARGET	Customer records	57%	51%
	Trade secrets/R&D/IP	38%	40%
	Company/employee identity	38%	36%
MOST COMMON PARTY TO CONTACT WHEN A CYBER INCIDENT OCCURRED	IT service vendor	43%	27%

Security

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

▼ 10% points below global average of 68%

			Global avg.
MOST COMMON TYPES OF SECURITY INCIDENTS	Theft or loss of IP	30%	38%
	Environmental risk *(including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.)*	21%	27%
	Workplace violence	15%	23%
MOST COMMON PERPETRATORS	Competitors	21%	12%
	Random perpetrator	21%	10%
RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY VULNERABLE TO THE FOLLOWING SECURITY RISKS	Workplace violence	18%	27%
	Theft or loss of IP	12%	19%
	Environmental risk *(including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.)*	9%	20%

MIDDLE EAST REPORT CARD

Top responses given by survey respondents.

Fraud

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

▲ 26% points above 2015

▲ 6% points above global average of 82%

			Global avg.
MOST COMMON TYPES OF FRAUD	Internal financial fraud *(manipulation of company results)*	30%	20%
	Theft of physical assets or stock	26%	29%
	Information theft, loss, or attack *(e.g., data theft)*	24%	24%
MOST COMMON PERPETRATORS	Senior or middle management employees of our own company	36%	30%
	Junior employees of our own company	34%	39%
	Joint venture partners *(i.e., a partner who provides manufacturing or other business function, or a franchisee)*	30%	23%
	Agents and/or intermediaries *(i.e., a third party working on behalf of your company)*	27%	27%
	Vendors/suppliers *(i.e., a provider of technology or services to your company)*	23%	26%
MOST COMMON ANTI-FRAUD MEASURES	Information *(IT security, technical countermeasures)*	80%	82%
	Staff *(training, whistle-blower hotline)*	70%	76%
	Staff *(background screening)*	68%	74%
	Risk *(risk officer and risk management system)*	68%	78%
MOST COMMON MEANS OF DISCOVERY	By a whistle-blower at our company	50%	44%

Cyber Security

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

▲ 5% points above global average of 85%

			Global avg.
MOST COMMON TYPES OF CYBER INCIDENT	Virus/worm infestation	30%	33%
	Data deletion or loss due to system issues	30%	24%
	Lost equipment with sensitive data	28%	17%
	Email-based phishing attack	28%	26%
MOST COMMON PERPETRATORS	Accidental placement of sensitive data that was indexed by a search engine *(e.g., Google)*	22%	10%
MOST COMMON TARGET	Physical assets/money	47%	38%
	Trade secrets/R&D/IP	42%	40%
	Customer records	38%	51%
MOST COMMON PARTY TO CONTACT WHEN A CYBER INCIDENT OCCURRED	IT service vendor	24%	27%

Security

82 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	38%	38%
	Workplace violence	32%	23%
	Geographic and political risk *(i.e., operating in areas of conflict)*	32%	22%
MOST COMMON PERPETRATORS	Permanent employees of our own company	24%	17%
RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY VULNERABLE TO THE FOLLOWING SECURITY RISKS	Workplace violence	28%	27%
	Environmental risk *(including damage caused by natural disasters such as floods)*	24%	20%
	Theft or loss of IP	22%	19%

ITALY REPORT CARD

Top responses given by survey respondents.

Fraud

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

▲ 3% points above 2015

▼ 5% points below global average of 82%

			Global avg.
MOST COMMON TYPES OF FRAUD	Theft of Physical Assets or Stock	34%	29%
	Information theft, loss or attack *(e.g., data theft)*	26%	24%
	Regulatory or compliance breach	26%	21%
MOST COMMON PERPETRATORS	Junior employees of our own company	50%	39%
	Ex-employees	36%	27%
	Vendors/suppliers *(i.e., a provider of technology or services to your company)*	33%	26%
	Senior or middle management employees of our own company	31%	30%
	Customers	22%	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)*	83%	79%
	Board of director engagement in cyber security policies and procedures	72%	75%
	Partners, clients, and vendors *(due diligence)*	70%	77%
	IP *(intellectual property risk assessment and trademark monitoring program)*	68%	75%
MOST COMMON MEANS OF DISCOVERY	By a whistle-blower at our company	53%	44%

Cyber Security

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

▼ 6% points below global average of 85%

			Global avg.
MOST COMMON TYPES OF CYBER INCIDENT	Data deletion by malicious insider	30%	19%
	Email-based phishing attack	21%	26%
	Virus/worm infestation	21%	33%
MOST COMMON PERPETRATORS	Ex-employees	24%	20%
MOST COMMON TARGET	Physical assets/money	38%	38%
	Customer records	35%	51%
	Trade secrets/R&D/IP	35%	40%
MOST COMMON PARTY TO CONTACT WHEN A CYBER INCIDENT OCCURRED	Webhosting/website provider	16%	9%

Security

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

= equal to global average of 68%

			Global avg.
MOST COMMON TYPES OF SECURITY INCIDENTS	Theft or loss of intellectual property	43%	38%
	Environmental risk *(including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.)*	21%	27%
	Workplace violence	13%	23%
MOST COMMON PERPETRATORS	Ex-employees	31%	23%
RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY VULNERABLE TO THE FOLLOWING SECURITY RISKS	Workplace violence	17%	27%
	Theft or loss of intellectual property	13%	19%
	Terrorism *(including domestic and international events)*	9%	18%

RUSSIA REPORT CARD

Top responses given by survey respondents.

Fraud

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

▲ 9% points above 2015

= equal to global average of 82%

			Global avg.
MOST COMMON TYPES OF FRAUD	Theft of physical assets or stock	38%	29%
	Information theft, loss, or attack	33%	24%
	Vendor, supplier, or procurement fraud	26%	26%
MOST COMMON PERPETRATORS	Junior employees of our own company	31%	39%
	Freelance/temporary employees	28%	27%
	Senior or middle management employees of our own company	22%	30%
	Ex-employees	22%	27%
	Vendors/suppliers *(i.e., a provider of technology or services to your company)*	19%	26%
	Customers	19%	19%
	Agents and/or intermediaries *(i.e., a third party working on behalf of your company)*	19%	27%
MOST COMMON ANTI-FRAUD MEASURES	Information *(IT security, technical countermeasures)*	90%	82%
	Management *(management controls, incentives, external supervision such as audit committee)*	79%	74%
	Board of director engagement in cyber security policies and procedures	77%	75%
	Risk *(risk officer and risk management system)*	77%	78%
MOST COMMON MEANS OF DISCOVERY	By a whistle-blower at our company	41%	44%

Cyber Security

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

▼ 3% points below global average of 85%

			Global avg.
MOST COMMON TYPES OF CYBER INCIDENT	Email-based phishing attack	33%	26%
	Data deletion or corruption by malware or system issue	26%	22%
	Insider theft of IP/trade secrets/R&D	18%	17%
	Lost equipment with sensitive data	18%	17%
	Denial of service attack	18%	14%
	Virus/worm infestation	18%	33%
MOST COMMON PERPETRATORS	Ex-employees	28%	20%
MOST COMMON TARGET	Customer records	56%	51%
	Employee records	34%	40%
	Physical assets/money	28%	38%
MOST COMMON PARTY TO CONTACT WHEN A CYBER INCIDENT OCCURRED	IT service vendor	31%	27%

Security

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

▼ 9% points below global average of 68%

			Global avg.
MOST COMMON TYPES OF SECURITY INCIDENTS	Theft or loss of IP	38%	38%
	Geographic and political risk *(i.e., operating in areas of conflict)*	21%	22%
	Workplace violence	18%	23%
MOST COMMON PERPETRATORS	Ex-employees	35%	23%
RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY VULNERABLE TO THE FOLLOWING SECURITY RISKS	Workplace violence	18%	27%
	Environmental risk *(including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.)*	8%	20%
	Theft or loss of IP	8%	19%
	Geographic and political risk	8%	12%

SUB-SAHARAN AFRICA REPORT CARD

Top responses given by survey respondents.

Fraud

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

▲ 5% points above 2015

▲ 7% points above global average of 82%

			Global avg.
MOST COMMON TYPES OF FRAUD	Internal financial fraud *(manipulation of company results)*	**31%**	20%
	Information theft, loss, or attack *(e.g., data theft)*	**30%**	24%
	Theft of physical assets or stock	**26%**	29%
MOST COMMON PERPETRATORS	Junior employees of our own company	**33%**	39%
	Freelance/temporary employees	**27%**	27%
	Agents and/or intermediaries *(i.e., a third party working on behalf of your company)*	**25%**	27%
	Senior or middle management employees of our own company	**23%**	30%
	Regulators	**23%**	14%
MOST COMMON ANTI-FRAUD MEASURES *Percentage of respondents who have implemented the anti-fraud measure.*	Board of director engagement in cyber security policies and procedures	**76%**	75%
	Staff *(background screening)*	**70%**	74%
	Information *(IT security, technical countermeasures)*	**70%**	82%
	Partners, clients, and vendors *(due diligence)*	**70%**	77%
MOST COMMON MEANS OF DISCOVERY	Through an internal audit	**60%**	39%

Cyber Security

91 — 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	Data deletion or loss due to system issues	**35%**	24%
	Virus/worm infestation	**31%**	33%
	Wire transfer fraud	**26%**	14%
	Email-based phishing attack	**26%**	26%
MOST COMMON PERPETRATORS	Ex-employees	**22%**	20%
MOST COMMON TARGET	Customer records	**49%**	51%
	Employee records	**47%**	40%
	Trade secrets	**47%**	40%
MOST COMMON PARTY TO CONTACT WHEN A CYBER INCIDENT OCCURRED	IT service vendor	**22%**	27%

Security

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

▲ 6% points above global average of 68%

			Global avg.
MOST COMMON TYPES OF SECURITY INCIDENTS	Theft or loss of IP	**43%**	38%
	Workplace violence	**26%**	23%
	Geographic and political risk *(i.e., operating in areas of conflict)*	**19%**	22%
MOST COMMON PERPETRATORS	Ex-employees	**28%**	23%
RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY VULNERABLE TO THE FOLLOWING SECURITY RISKS	Theft or loss of IP	**28%**	19%
	Workplace violence	**19%**	27%
	Environmental risk *(including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.)*	**17%**	20%

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%

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%

INDIA REPORT CARD

Top responses given by survey respondents.

Fraud

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

▼ 12% points below 2015

▼ 14% points below global average of 82%

			Global avg.
MOST COMMON TYPES OF FRAUD	Theft of physical assets or stock	28%	29%
	Management conflict of interest	27%	21%
	Corruption and bribery	27%	15%
	Vendor, supplier, or procurement fraud	27%	26%
	Market collusion *(e.g., price fixing)*	27%	17%
	Internal financial fraud *(manipulation of company results)*	25%	20%
MOST COMMON PERPETRATORS	Junior employees of our own company	61%	39%
	Agents and/or intermediaries *(i.e., a third party working on behalf of your company)*	49%	27%
	Freelance/temporary employees	41%	27%
	Senior or middle management employees of our own company	37%	30%
	Joint venture partners *(i.e., a partner who provides manufacturing or other business function, or a franchisee)*	37%	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)*	87%	77%
	Partners, clients, and vendors *(due diligence)*	87%	77%
	Information *(IT security, technical countermeasures)*	85%	82%
	Staff *(background screening)*	85%	74%
MOST COMMON MEANS OF DISCOVERY	By a whistle-blower at our company	66%	44%

Cyber Security

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

▼ 12% points below global average of 85%

			Global avg.
MOST COMMON TYPES OF CYBER INCIDENT	Data deletion or corruption by malware or system issue	28%	22%
	Data deletion by malicious insider	27%	19%
	Virus/worm infestation	23%	33%
	Denial of service attack	23%	14%
MOST COMMON PERPETRATORS	Accidental placement of sensitive data that was indexed by a search engine *(e.g., Google)*	25%	10%
MOST COMMON TARGET	Employee records	59%	40%
	Trade secrets/R&D/IP	48%	40%
	Customer records	45%	51%
	Physical assets/money	45%	38%
MOST COMMON PARTY TO CONTACT WHEN A CYBER INCIDENT OCCURRED	IT service vendor	34%	27%

Security

72 — 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	Environmental risk *(including damage caused by natural disasters such as hurricanes,tornadoes, floods, earthquakes, etc.)*	40%	27%
	Workplace violence	37%	23%
	Theft or loss of IP	35%	38%
	Geographic and political risk *(i.e., operating in areas of conflict)*	35%	22%
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	52%	27%
	Terrorism, including domestic and international events	45%	18%
	Environmental risk *(including damage caused by natural disasters such as hurricanes,tornadoes, floods, earthquakes, etc.)*	37%	20%

BRAZIL REPORT CARD

Top responses given by survey respondents.

Fraud

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

▼ 9% points below 2015

▼ 14% points below global average of 82%

			Global avg.
MOST COMMON TYPES OF FRAUD	Theft of physical assets or stock	24%	29%
	Information theft, loss or attack *(e.g., data theft)*	21%	24%
	Vendor, supplier or procurement fraud	21%	26%
MOST COMMON PERPETRATORS	Ex-employees	43%	27%
	Freelance/temporary employees	26%	27%
	Junior employees of our own company	22%	39%
	Vendors/suppliers *(i.e., a provider of technology or services to your company)*	17%	26%
	Agents and/or intermediaries *(i.e., a 3rd party working on behalf of your company)*	17%	27%
	Joint venture partners *(i.e., a partner who provides manufacturing or other business function, or a franchisee)*	17%	23%
	Customers	17%	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)*	88%	79%
	Information *(IT security, technical countermeasures)*	88%	82%
	Management *(management controls, incentives, external supervision such as audit committee)*	85%	74%
MOST COMMON MEANS OF DISCOVERY	Through an internal audit	43%	36%

Cyber Security

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

▼ 9% points below global average of 85%

			Global avg.
MOST COMMON TYPES OF CYBER INCIDENT	Virus/ worm infestation	41%	33%
	Data breach resulting in loss of customer or employee data	29%	23%
	Data deletion or loss due to system issues	21%	24%
MOST COMMON PERPETRATORS	Ex-employees	38%	20%
MOST COMMON TARGET	Customer records	46%	51%
	Employee records	42%	40%
	Company/employee identity	42%	36%
MOST COMMON PARTY TO CONTACT WHEN A CYBER INCIDENT OCCURRED	Webhosting/website provider	23%	9%

Security

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

▼ 15% points below global average of 68%

			Global avg.
MOST COMMON TYPES OF SECURITY INCIDENTS	Theft or loss of IP	32%	38%
	Environmental risk *(including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.)*	18%	27%
	Geographic and political risk *(i.e., operating in areas of conflict)*	12%	22%
MOST COMMON PERPETRATORS	Ex-employees	39%	23%
RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY VULNERABLE TO THE FOLLOWING SECURITY RISKS	Theft or loss of IP	21%	19%
	Workplace violence	18%	27%
	Geographic and political risk *(i.e., operating in areas of conflict)*	15%	12%
	Environmental risk *(including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.)*	15%	20%

COLOMBIA REPORT CARD

Top responses given by survey respondents.

Fraud

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

▲ 12% points above 2015

▲ 13% points above global average of 82%

			Global avg.
MOST COMMON TYPES OF FRAUD	Management conflict of interest	**43%**	21%
	Vendor, supplier, or procurement fraud	**43%**	26%
	Theft of physical assets or stock	**38%**	29%
MOST COMMON PERPETRATORS	Ex-employees	**35%**	27%
	Freelance/temporary employees	**35%**	27%
	Vendors/suppliers *(i.e., a provider of technology or services to your company)*	**35%**	26%
	Senior or middle management employees of our own company	**20%**	30%
	Junior employees of our own company	**20%**	39%
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)*	**95%**	77%
	Assets *(physical security systems, stock inventories, tagging, asset register)*	**95%**	79%
	Staff *(background screening)*	**95%**	74%
MOST COMMON MEANS OF DISCOVERY	Through an internal audit	**50%**	39%

Cyber Security

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

▲ 10% points above global average of 85%

			Global avg.
MOST COMMON TYPES OF CYBER INCIDENT	Virus/worm infestation	**52%**	33%
	Email-based phishing attack	**38%**	26%
	Data deletion or loss due to system issues	**29%**	24%
MOST COMMON PERPETRATORS	Ex-employees	**25%**	20%
MOST COMMON TARGET	Customer records	**50%**	51%
	Physical assets/money	**45%**	38%
	Employee records	**40%**	40%
MOST COMMON PARTY TO CONTACT WHEN A CYBER INCIDENT OCCURRED	Incident response firm	**15%**	14%
	Insurance portal	**15%**	5%
	Webhosting/website provider	**15%**	9%

Security

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

▼ 6% points below global average of 68%

			Global avg.
MOST COMMON TYPES OF SECURITY INCIDENTS	Workplace violence	**24%**	23%
	Theft or loss of intellectual IP	**24%**	38%
	Terrorism, including domestic and international events	**19%**	15%
MOST COMMON PERPETRATORS	Freelance/temporary employees	**38%**	16%
RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY VULNERABLE TO THE FOLLOWING SECURITY RISKS	Terrorism, including domestic and international events	**19%**	18%
	Workplace violence	**19%**	27%
	Environmental risk *(including damage caused by natural disasters such as hurricanes,tornadoes, floods, earthquakes, etc.)*	**14%**	20%

MEXICO REPORT CARD

Top responses given by survey respondents.

Fraud

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

▲ 2% points above 2015

= equal to global average of 82%

			Global avg.
MOST COMMON TYPES OF FRAUD	Vendor, supplier, or procurement fraud	52%	26%
	Theft of physical assets or stock	30%	29%
	Corruption and bribery	18%	15%
MOST COMMON PERPETRATORS	Ex-employees	33%	27%
	Junior employees of our own company	30%	39%
	Freelance/temporary employees	30%	27%
	Vendors/suppliers *(i.e., a provider of technology or services to your company)*	30%	26%
	Agents and/or intermediaries *(i.e., a third party working on behalf of your company)*	26%	27%
MOST COMMON ANTI-FRAUD MEASURES	Partners, clients, and vendors *(due diligence)*	82%	77%
	Financial *(financial controls, fraud detection, internal audit, external audit, anti-money laundering policies)*	82%	77%
	Risk *(risk officer and risk management system)*	81%	78%
MOST COMMON MEANS OF DISCOVERY	Through an internal audit	44%	39%

Cyber Security

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

▼ 3% points below global average of 85%

			Global avg.
MOST COMMON TYPES OF CYBER INCIDENT	Virus/worm infestation	39%	33%
	Email-based phishing attack	33%	26%
	Data deletion or corruption by malware or system issue	33%	22%
MOST COMMON PERPETRATORS	Competitors	22%	6%
MOST COMMON TARGET	Company/employee identity	52%	36%
	Customer records	48%	51%
	Physical assets/money	37%	38%
MOST COMMON PARTY TO CONTACT WHEN A CYBER INCIDENT OCCURRED	Federal law enforcement	30%	8%

Security

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

▼ 20% points below 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.)*	27%	27%
	Theft or loss of IP	24%	38%
	Geographic and political risk *(i.e., operating in areas of conflict)*	21%	22%
MOST COMMON PERPETRATORS	Freelance/temporary employees	31%	16%
	Ex-employees	31%	23%
RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY VULNERABLE TO THE FOLLOWING SECURITY RISKS	Workplace violence	24%	27%
	Terrorism, including domestic and international events	21%	18%
	Theft or loss of IP	18%	19%