CANADA REPORT CARD

		Percentage of respondents		220/	points above	
Fraud	[88]	affected by fraud in the past 12 months.		23% 6%	2015 points above average of 82	
MOST COMMON TYPES OF	Theft of physical a				34%	Global avg.
FRAUD	, ,	loss, or attack (e.g., data theft)			32%	24%
	Regulatory or con				32%	
		or procurement fraud			32%	
		of company funds			32%	18%
MOST COMMON		management employees of our own company			47%	
PERPETRATORS		s of our own company			39%	39%
					36%	
	Freelance/tempor	ary employees			36%	
	Ex-employees		,			
MOOT COMMON ANTI EDAUD		ermediaries (i.e., a third party working on behalf of your comp	pany)		36%	
MOST COMMON ANTI-FRAUD MEASURES		d risk management system)			90%	
Percentage of respondents who have implemented the anti-fraud measure.		nagement controls, incentives, external supervision such as au	ıdit committe	ee)	88%	74%
implemented the anti-fraud measure.	Information (IT sec	curity, technical countermeasures)			86%	
	Assets (physical se	curity systems, stock inventories, tagging, asset register)			86%	79%
	Partners, clients,	and vendors (due diligence)			85%	77%
MOST COMMON MEANS OF DISCOVERY	By a whistle-blow	er at our company			44%	44%
Cyber Security	(85)	Percentage of respondents that experienced a cyber incident in the past 12 months.	=	equal to glob average of 8	oal 5%	Global avg
MOST COMMON TYPES OF	Virus/worm attacl	k			41%	33%
CYBER INCIDENT	Lost equipment w	vith sensitive data			39%	17%
	Data deletion or c	corruption by malware or system issue			34%	22%
	Data breach resul	Iting in loss of IP/trade secrets/R&D			34%	19%
MOST COMMON PERPETRATORS	Permanent emplo	byees of our own company			20%	10%
MOST COMMON TARGET	Customer records	S			57%	51%
	Physical assets/m	noney			57%	38%
	Trade secrets/R&	D/IP			51%	40%
MOST COMMON PARTY TO	Incident response	e firm			20%	14%
CONTACT WHEN A CYBER INCIDENT OCCURRED	IT service vendor				20%	27%
Security	[78]	Percentage of respondents that experienced a security incident in the past 12 months.	•	10%	points above average of 68	
MOST COMMON TYPES OF	[78]	experienced a security incident in the past 12 months.	•	10%	points above average of 68	global 3% Global avg. 38%
	Theft or loss of IP Environmental risk	experienced a security incident in the past 12 months.				Global avg.
MOST COMMON TYPES OF	Theft or loss of IP Environmental risl (including damage co	experienced a security incident in the past 12 months.			49%	Global avg.
MOST COMMON TYPES OF	Theft or loss of IP Environmental risl (including damage co	experienced a security incident in the past 12 months. k aused by natural disasters such as hurricanes, tornadoes, floo			49% 46%	Global avg. 38% 27%
MOST COMMON TYPES OF SECURITY INCIDENTS MOST COMMON	Theft or loss of IP Environmental risl (including damage coordinate) Geographic and p	experienced a security incident in the past 12 months. k aused by natural disasters such as hurricanes, tornadoes, floo political risk (i.e., operating in areas of conflict)			49% 46% 27%	Global avg. 38% 27% 22%
MOST COMMON TYPES OF SECURITY INCIDENTS MOST COMMON PERPETRATORS	Theft or loss of IP Environmental risl (including damage of Geographic and p Ex-employees Workplace violence Environmental risl	experienced a security incident in the past 12 months. k aused by natural disasters such as hurricanes, tornadoes, floo political risk (i.e., operating in areas of conflict)	ds, earthqua	akes, etc.)	49% 46% 27% 28%	Global avg. 38% 27% 22% 23%

UNITED STATES REPORT CARD

INITED STATES REI	0111 021111		Iop responses give	en by survey respo	onde
Fraud	90	Percentage of respondents affected	5 %	points above 2015	
rrauu	80	by fraud in the past 12 months.	2 %	points below gl average of 82%	lobal 6 Globa
MOST COMMON TYPES OF	IP theft (e.g. of trac	de secrets), piracy, or counterfeiting		27%	16
FRAUD	Information theft,	loss, or attack (e.g., data theft)		24%	24
	Management cor			24%	21
MOST COMMON	Junior employees	s of our own company		36%	39
PERPETRATORS		management employees of our own companys		32%	30
	Ex-employees			30%	27
	Vendors/supplier	'S (i.e., a provider of technology or services to your company)		21%	26
	Freelance/tempo	rary employees		17%	27
	Customers			17%	19
MOST COMMON	Information (IT sec	curity, technical countermeasures)		91%	82
ANTI-FRAUD MEASURES		controls, fraud detection, internal audit, external audit, anti-money la	underina policies)	86%	77
		ecurity systems, stock inventories, tagging, asset register)		85%	79
MOST COMMON MEANS OF	Through an interr			49%	39
DISCOVERY	THOUGH ATTINION	rai addit		43 /0	0.
Cyber Security	88	Percentage of respondents that experienced a cyber incident in the past 12 months.	4 3%	points above gl average of 85%	
MOST COMMON TYPES OF	Virus/worm infest	tation		42%	Glob
CYBER INCIDENT		oss due to system issues		26%	24
	Email-based phis	•		21%	26
MOST COMMON PERPETRATORS	Ex-employees	aning attack		19%	20
MOST COMMON TARGET	Customer record	ls.		57%	5
	Trade secrets/R&			38%	40
	Company/employ			38%	36
MOST COMMON PARTY TO CONTACT WHEN A CYBER NCIDENT OCCURRED	IT service vendor			43%	2
Security	58	Percentage of respondents that experienced a security incident in the past 12 months.	1 0%	points below gl average of 68%	Ó
MOST COMMON TYPES OF	Theft or loss of IF			30%	Glob 38
SECURITY INCIDENTS	Environmental ris			21%	27
		caused by natural disasters such as hurricanes, tornadoes, floods, ea	rthquakes, etc.)		
	Workplace violen	ice		15%	2
MOST COMMON	Competitors			21%	13
PERPETRATORS	Random perpetra	ator		21%	10
RESPONDENTS ARE MOST	Workplace violen	nce		18%	2
IKELY TO FEEL HIGHLY	Theft or loss of IF			12%	19
ULNERABLE TO THE OLLOWING SECURITY	Environmental ris			9%	20
RISKS	(including damage C	caused by natural disasters such as hurricanes, tornadoes, floods, ea	r inquakes, etc.)		

MIDDLE EAST REPORT CARD

	Percentage of respondents affected \$\hfrac{1}{26\%}\$	points above 2015		
Fraud	by fraud in the past 12 months.	points above gl average of 82%	ve global 82% Global a	
MOST COMMON TYPES OF	Internal financial fraud (manipulation of company results)	30%	209	
FRAUD	Theft of physical assets or stock	26%	29	
	Information theft, loss, or attack (e.g., data theft)	24%	24	
MOST COMMON	Senior or middle management employees of our own company	36%	30	
PERPETRATORS	Junior employees of our own company	34%	39	
	Joint venture partners (i.e., a partner who provides manufacturing or other business function, or a fran	chisee) 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	Information (IT security, technical countermeasures)	80%	82	
ANTI-FRAUD MEASURES	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	Percentage of respondents that experienced a cyber incident in the past 12 months.	points above gl average of 85%	obal o Globa	
MOST COMMON TYPES OF	Virus/worm infestation	30%	33	
CYBER INCIDENT	Data deletion or loss due to system issues	30%	24'	
	Lost equipment with sensitive data			
	Email-based phishing attack			
	3 · · · · · · · · · · · · · · · · · · ·	28%	26	
	Accidental placement of sensitive data that was indexed by a search engine (e.g., Google)	28%		
PERPETRATORS			10	
PERPETRATORS	Accidental placement of sensitive data that was indexed by a search engine (e.g., Google)	22%	38	
PERPETRATORS	Accidental placement of sensitive data that was indexed by a search engine (e.g., Google) Physical assets/money	22% 47%	10°	
MOST COMMON PERPETRATORS MOST COMMON TARGET MOST COMMON PARTY TO CONTACT WHEN A CYBER INCIDENT OCCURRED	Accidental placement of sensitive data that was indexed by a search engine (e.g., Google) Physical assets/money Trade secrets/R&D/IP	22% 47% 42%	38° 40° 51°	
MOST COMMON TARGET MOST COMMON PARTY TO CONTACT WHEN A CYBER INCIDENT OCCURRED	Accidental placement of sensitive data that was indexed by a search engine (e.g., Google) Physical assets/money Trade secrets/R&D/IP Customer records	22% 47% 42% 38% 24%		
MOST COMMON TARGET MOST COMMON PARTY TO CONTACT WHEN A CYBER INCIDENT OCCURRED Security MOST COMMON TYPES OF	Accidental placement of sensitive data that was indexed by a search engine (e.g., Google) Physical assets/money Trade secrets/R&D/IP Customer records IT service vendor Percentage of respondents that experienced a security incident in	22% 47% 42% 38% 24%	10° 388 40° 51° 27°	
MOST COMMON TARGET MOST COMMON PARTY TO CONTACT WHEN A CYBER INCIDENT OCCURRED Security MOST COMMON TYPES OF	Accidental placement of sensitive data that was indexed by a search engine (e.g., Google) Physical assets/money Trade secrets/R&D/IP Customer records IT service vendor Percentage of respondents that experienced a security incident in the past 12 months.	22% 47% 42% 38% 24%	100 388 400 511 277	
MOST COMMON PARTY TO CONTACT WHEN A CYBER NCIDENT OCCURRED Security MOST COMMON TYPES OF	Accidental placement of sensitive data that was indexed by a search engine (e.g., Google) Physical assets/money Trade secrets/R&D/IP Customer records IT service vendor Percentage of respondents that experienced a security incident in the past 12 months. Theft or loss of IP	22% 47% 42% 38% 24%	100 388 400 511 277 Obball 388 233	
MOST COMMON TARGET MOST COMMON PARTY TO CONTACT WHEN A CYBER INCIDENT OCCURRED Security MOST COMMON TYPES OF SECURITY INCIDENTS	Accidental placement of sensitive data that was indexed by a search engine (e.g., Google) Physical assets/money Trade secrets/R&D/IP Customer records IT service vendor Percentage of respondents that experienced a security incident in the past 12 months. Theft or loss of IP Workplace violence	22% 47% 42% 38% 24% points above glaverage of 68% 38% 32%	100 388 400 511 277	
MOST COMMON TYPES OF SECURITY INCIDENTS MOST COMMON PARTY TO CONTACT WHEN A CYBER INCIDENT OCCURRED MOST COMMON TYPES OF SECURITY INCIDENTS MOST COMMON PERPETRATORS RESPONDENTS ARE MOST	Accidental placement of sensitive data that was indexed by a search engine (e.g., Google) Physical assets/money Trade secrets/R&D/IP Customer records IT service vendor Percentage of respondents that experienced a security incident in the past 12 months. Theft or loss of IP Workplace violence Geographic and political risk (i.e., operating in areas of conflict)	22% 47% 42% 38% 24% points above glaverage of 68% 38% 32% 32%	100 388 400 511 277 obbal 388 233	
MOST COMMON PARTY TO CONTACT WHEN A CYBER	Accidental placement of sensitive data that was indexed by a search engine (e.g., Google) Physical assets/money Trade secrets/R&D/IP Customer records IT service vendor Percentage of respondents that experienced a security incident in the past 12 months. Theft or loss of IP Workplace violence Geographic and political risk (i.e., operating in areas of conflict) Permanent employees of our own company	22% 47% 42% 38% 24% points above glaverage of 68% 32% 32% 24%	100 388 400 511 277 Cobal 388 233 222	

ITALY REPORT CARD

		Percentage of respondents affected	4 3%	points above 2015	
Fraud		by fraud in the past 12 months.	▼ 5%	points below glasterage of 82%	obal Global av
MOST COMMON TYPES OF	Theft of Physical	Assets or Stock		34%	29%
FRAUD	Information theft,	loss or attack (e.g., data theft)		26%	24%
	Regulatory or cor	mpliance breach		26%	21%
MOST COMMON	Junior employees	s of our own company		50%	39%
PERPETRATORS	Ex-employees			36%	27%
	Vendors/suppliers	S (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	Assets (physical se	ecurity systems, stock inventories, tagging, asset register)		83%	79%
ANTI-FRAUD MEASURES Percentage of respondents who	Board of director	engagement in cyber security policies and procedures		72%	75%
have implemented the anti-fraud measure.	Partners, clients,	and vendors (due diligence)		70%	77%
	IP (intellectual prope	erty risk assessment and trademark monitoring program)		68%	75%
MOST COMMON MEANS OF DISCOVERY	By a whistle-blow	ver at our company		53%	44%
Cyber Security	79	Percentage of respondents that experienced a cyber incident in the past 12 months.	▼ 6%	points below glaverage of 85%	obal Global av
MOST COMMON TYPES OF	Data deletion by r	malicious insider		30%	19%
CYBER INCIDENT	Email-based phis	hing attack		21%	26%
	Virus/worm infest	ration		21%	33%
MOST COMMON PERPETRATORS	Ex-employees			24%	20%
MOST COMMON TARGET	Physical assets/n	noney		38%	38%
	Customer records	s		35%	51%
	Trade secrets/R&	D/IP		35%	40%
MOST COMMON PARTY TO CONTACT WHEN A CYBER INCIDENT OCCURRED	Webhosting/web	site 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 av
MOST COMMON TYPES OF	Theft or loss of in	tellectual property		43%	38%
SECURITY INCIDENTS	Environmental ris (including damage c	k aused by natural disasters such as hurricanes, tornadoes, floods, ea	arthquakes, etc.)	21%	27%
	Workplace violen	се		13%	23%
MOST COMMON PERPETRATORS	Ex-employees			31%	23%
RESPONDENTS ARE MOST	Workplace violen	ce		17%	27%
VULNERABLE TO THE	Theft or loss of in	tellectual property		13%	19%
FOLLOWING SECURITY RISKS	Terrorism (including domestic	and international events)		9%	18%

RUSSIA REPORT CARD

Formal	Percentage of respondents affected	4 9%	points above 2015	
Fraud	by fraud in the past 12 months.	=	equal to global average of 82%	Global avg.
MOST COMMON TYPES OF	Theft of physical assets or stock		38%	29%
FRAUD	Information theft, loss, or attack		33%	24%
	Vendor, supplier, or procurement fraud		26%	26%
MOST COMMON	Junior employees of our own company		31%	39%
PERPETRATORS	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	Information (IT security, technical countermeasures)		90%	82%
ANTI-FRAUD MEASURES	Management (management controls, incentives, external supervision such as audit co	ommittee)	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	Percentage of respondents that experienced a cyber incident in the past 12 months.	▼ 3%	points below g average of 85%	obal Global avg.
MOST COMMON TYPES OF	Email-based phishing attack		33%	26%
CYBER INCIDENT	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	Percentage of respondents that experienced a security incident in the past 12 months.	▼ 9%	points below g average of 68%	obal Global avg.
MOST COMMON TYPES OF	Theft or loss of IP		38%	38%
SECURITY INCIDENTS	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	Workplace violence		18%	27%
LIKELY TO FEEL HIGHLY VULNERABLE TO THE FOLLOWING SECURITY	Environmental risk (including damage caused by natural disasters such as hurricanes, tornadoes, floods, ea	arthquakes, etc.)	8%	20%
RISKS	Theft or loss of IP		8%	19%
	Geographic and political risk		8%	12%

SUB-SAHARAN AFRICA REPORT CARD

Eroud	00	Percentage of respondents	★ 5%	points above 2015	
Fraud	89	affected by fraud in the past 12 months.		points above average of 82	global 2% Global a
MOST COMMON TYPES OF	Internal financial	fraud (manipulation of company results)		31%	
FRAUD	Information theft	t, loss, or attack (e.g., data theft)		30%	249
	Theft of physical	l assets or stock		26%	299
MOST COMMON	Junior employee	es of our own company		33%	399
PERPETRATORS	Freelance/tempo	orary employees		27%	279
	Agents and/or in	ntermediaries (i.e., a third party working on behalf of your com	pany)	25%	279
	Senior or middle	e management employees of our own company		23%	309
	Regulators			23%	149
MOST COMMON ANTI-FRAUD	Board of directo	or engagement in cyber security policies and procedure	S	76%	75%
MEASURES Percentage of respondents who have	Staff (background	screening)		70%	749
implemented the anti-fraud measure.	Information (IT se	ecurity, technical countermeasures)		70%	829
	Partners, clients	s, and vendors (due diligence)		70%	779
MOST COMMON MEANS OF DISCOVERY	Through an inter	rnal audit		60%	39%
Cyber Security	91	Percentage of respondents that experienced a cyber incident in the past 12 months.	♠ 6%	points above average of 85	5%
MOST COMMON TYPES OF	Data deletion or	loss due to system issues		35%	Global a
CYBER INCIDENT	Virus/worm infes	station		31%	339
	Wire transfer fra	ud		26%	149
	Email-based phi	ishing attack		26%	269
MOST COMMON PERPETRATORS	Ex-employees			22%	209
MOST COMMON TARGET	Customer record	ds		49%	519
	Employee record	ds		47%	409
	Trade secrets			47%	409
MOST COMMON PARTY TO CONTACT WHEN A CYBER INCIDENT OCCURRED	IT service vendo	or		22%	279
Security	74	Percentage of respondents that experienced a security incident in the past 12 months.	♠ 6%	points above average of 68	3%
MOST COMMON TYPES OF	Theft or loss of I	Р		43%	Global a
SECURITY INCIDENTS	Workplace viole	nce		26%	239
	Geographic and	political risk (i.e., operating in areas of conflict)		19%	229
MOST COMMON PERPETRATORS	Ex-employees			28%	239
RESPONDENTS ARE MOST	Theft or loss of I	Р		28%	199
LIKELY TO FEEL HIGHLY VULNERABLE TO THE	Workplace viole	nce		19%	279
/ULNERABLE TO THE FOLLOWING SECURITY RISKS	Environmental ri	sk caused by natural disasters such as hurricanes, tornadoes, floc	ods. earthquakes. etc.)	17%	20%

UNITED KINGDOM REPORT CARD

		מא		en by survey respo	oridoria
	Percentage of respondents affected		16%	points above 2015	
Fraud	90	by fraud in the past 12 months.		points above gl average of 82%	
MOST COMMON TYPES OF	Theft of physical a	assets or stock		41%	Global av
FRAUD	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		s of our own company		41%	39%
PERPETRATORS	Senior or middle r	management employees of our own companys		32%	30%
	Ex-employees			30%	27%
	Freelance/tempor	rary employees		27%	27%
	Agents and/or into	ermediaries (i.e., a third party working on behalf of your company)		27%	27%
	Customers			27%	19%
MOST COMMON		curity, technical countermeasures)		84%	82%
ANTI-FRAUD MEASURES		nagement controls, incentives, external supervision such as audit co	nmmittee)	80%	74%
	-	erty risk assessment and trademark monitoring program)	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	76%	75%
MOST COMMON MEANS OF				50%	44%
DISCOVERY	by a whistie-blow	er at our company		50%	4470
Cyber Security	92	Percentage of respondents that experienced a cyber incident in the past 12 months.	↑ 7%	points above gl average of 85%	lobal 6
MOST COMMON TYPES OF	Virus/worm infest	ration		33%	Global a
CYBER INCIDENT		stomer or employee data		27%	19%
				22%	23%
		Iting in loss of customer or employee data			24%
MACOT COMMON		oss due to system issues		22%	
MOST COMMON PERPETRATORS	Ex-employees			29%	20%
MOST COMMON TARGET	Customer records	S		42%	51%
	Trade secrets/R&	D/IP		42%	40%
	Company/employ	vee identity		40%	36%
MOST COMMON PARTY TO CONTACT WHEN A CYBER INCIDENT OCCURRED	IT service vendor			33%	27%
Security	82	Percentage of respondents that experienced a security incident in the past 12 months.	▲ 14%	points above gl average of 68%	llobal 6
MOST COMMON TYPES OF	Theft or loss of IP			51%	38%
SECURITY INCIDENTS	Geographic and p	political risk (i.e., operating in areas of conflict)		39%	22%
	Workplace violend	, , , ,		29%	23%
MOST COMMON	Ex-employees			28%	23%
PERPETRATORS					
RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY	Workplace violend			31%	27%
VULNERABLE TO THE	Theft or loss of IP			24%	19%
FOLLOWING SECURITY RISKS	Environmental risl (including damage co	k aused by natural disasters such as hurricanes, tornadoes, floods, ea	arthquakes, etc.)	24%	20%
	Geographic and p	political risk (i.e., operating in areas of conflict)		24%	12%
	Terrorism, including	ng domestic and international events		24%	18%

CHINA REPORT CARD

Fraud		age of respondents I by fraud in the past hs.	▲ 10/ poi	nts above 5 nts above or rage of 82	global % ^{Global} avg.
MOST COMMON TYPES OF	Regulatory or compliance bre	each		41%	21%
FRAUD	Vendor, supplier, or procurem	ent fraud		37%	26%
	Theft of physical assets or sto	ock		25%	29%
	Information theft, loss, or atta	ck (e.g., data theft)		25%	24%
	Corruption and bribery			25%	15%
	Market collusion (e.g., price fixir	ng)		25%	17%
	Misappropriation of company	funds		25%	18%
MOST COMMON	Joint venture partners (i.e., a pa	artner who provides manufacturing or other busin	ness function, or a franchisee)	52%	23%
PERPETRATORS	Junior employees of our own	company		48%	39%
	Agents and/or intermediaries	(i.e., a third party working on behalf of your comp	pany)	43%	27%
	Vendors/suppliers (i.e., a provid	der of technology or services to your company)		36%	26%
	Senior or middle managemen	t employees of our own company		34%	30%
MOST COMMON ANTI-FRAUD	Partners, clients, and vendors	G (due diligence)		90%	77%
MEASURES Percentage of respondents who have	Assets (physical security systems	s, stock inventories, tagging, asset register)		86%	79%
implemented the anti-fraud measure.	Board of director engagemen	t in cyber security policies and procedures	S	86%	75%
MOST COMMON MEANS OF	By a whistle-blower at our co	mpany		55%	44%
DISCOVERY	Through an external audit			55%	36%
Cyber Security MOST COMMON TYPES OF	in the pa	nced a cyber incident ast 12 months.	1% point ave	nt above gl rage of 85°	Global avg.
CYBER INCIDENT	Email-based phishing attack Virus/worm infestation			39%	33%
	Data deletion or corruption by	malwara or evetem issue		39%	22%
MOST COMMON	Freelance/temporary employe	•		25%	14%
PERPETRATORS	r reelance/temporally employe	765		25 /0	14/0
MOST COMMON TARGET	Customer records			82%	51%
	Trade secrets/R&D/IP			59%	40%
	Employee records			41%	40%
	Company/employee identity				
the state of the s				41%	36%
MOST COMMON PARTY TO CONTACT WHEN A CYBER INCIDENT OCCURRED	IT service vendor			41% 34%	36% 27%
CONTACT WHEN A CYBER	Percenta experier	age of respondents that nced a security incident ast 12 months.	♣ 7% poi	34% Ints above orage of 68	27%
CONTACT WHEN A CYBER INCIDENT OCCURRED	Percenta experier in the pa	nced a security incident	1 770 ave	34% Ints above orage of 68	27% global %
Security MOST COMMON TYPES OF	Percenta experier in the pa	nced a security incident ast 12 months.	1 770 ave	34% Ints above orage of 68	27% global % Global avg.
Security MOST COMMON TYPES OF	Percenta experier in the pa	nced a security incident ast 12 months. ral disasters such as hurricanes, tornadoes, floo	1 770 ave	34% Ints above grage of 68	27% global % Global avg. 27%
Security MOST COMMON TYPES OF	Percenta experier in the pa	nced a security incident ast 12 months. ral disasters such as hurricanes, tornadoes, floo	1 770 ave	34% ants above strage of 68' 45% 41%	27% global global avg. 27% 38%
CONTACT WHEN A CYBER INCIDENT OCCURRED Security MOST COMMON TYPES OF SECURITY INCIDENTS MOST COMMON PERPETRATORS RESPONDENTS ARE MOST	Percenta experier in the pase. Environmental risk (including damage caused by natural to risk of IP) Geographic and political risk (including damage)	nced a security incident ast 12 months. ral disasters such as hurricanes, tornadoes, floo	1 770 ave	34% htts above grage of 68 ³ 45% 41% 25%	27% global global avg. 27% 38% 22%
Security MOST COMMON TYPES OF SECURITY INCIDENTS MOST COMMON PERPETRATORS	Percenta experier in the particular in the particular damage caused by natural Theft or loss of IP Geographic and political risk of Competitors Workplace violence Environmental risk	nced a security incident ast 12 months. ral disasters such as hurricanes, tornadoes, floo	ds, earthquakes, etc.)	34% ants above orage of 68 th 45% 41% 25% 21%	27% global avg. 27% 38% 22% 12%

INDIA REPORT CARD

## 14% prints and in the past 12 months. ## 14% prints of physical seasts or stock ## 14% prints of physical		Percentage of respondents	oints below	
MOST COMMON TYPES OF FRAUD The for physical assets or stock Management conflict of interest Compution and briefly Vendor, supplier, or procurement fraud Market collision (s.g., proc heavy) Vendor, supplier, or procurement fraud Market collision (s.g., proc heavy) Vendor, supplier, or procurement fraud Market collision (s.g., proc heavy) Vendor, supplier, or procurement fraud Market collision (s.g., proc heavy) Internal financial infancial fraud pranspulsation of company participation of procurement fraud Market collision (s.g., proc heavy) Julior employees of our own company Agents and/or infarried financy press Senior or middle management employees of our own company Joint venture particips (s.g., a pressure who prevention assurbicturing or other business seniors, or a franchises) MOST COMMON ANTI-FRAUD Financial planearia conflict, fraud detection, reternal audit, and-morrey business seniors, or a franchises) MOST COMMON MEANS OF Discovery Cyber Security Percentage of respondents that experienced infarried fraud practice conflicts, fraud and seniors, reternal audit, and-morrey business seniors, or a franchises) MOST COMMON MEANS OF Discovery Cyber Security Percentage of respondents that experienced a cyber incident in the past 12 months. MOST COMMON TYPES OF CYBER INCIDENT Accidental placement of sensitive data that was indexed by a search engine (e.g., cooper) Employee records Denial of service uttack Accidental placement of sensitive data that was indexed by a search engine (e.g., cooper) Trade accidental placement of sensitive data that was indexed by a search engine (e.g., cooper) Trade accidental placement of sensitive data that was indexed by a search engine (e.g., cooper) Percentage of respondents that experienced a security incident in the past 12 months. Percentage of respondents that experienced a security incident in the past 12 months. Provincial processes of the past 12 months. Percentage of respondents that experienced a security incident in the past 12 mo	Fraud	affected by fraud in the past	oints below o	%
Most Common Means of respondents and history (27% 15 12% 15 12% 15 12% 16 12% 1	MOST COMMON TYPES OF	Theft of physical assets or stock	28%	29%
Vendor, supplier, or procurement fraud Market collusion pag., pres finals Internal financial fraud pressure of common company Internal financial fraud pressure of common company Agents and/or intermediaries (i.e., a twid party working on behalf of your company) Agents and/or intermediaries (i.e., a twid party working on behalf of your company) Agents and/or intermediaries (i.e., a twid party working on behalf of your company) Joint venture partners (i.e., a twid party working on behalf of your company) Joint venture partners (i.e., a partner who provides manufacturing or officer business function, or a franchises) Serior or middle management employees of our own company Joint venture partners (i.e., a partner who provides manufacturing or officer business function, or a franchises) 37% 77 MMOST COMMON ANTI-FRAUD Financial dimexical conducts, and vendors (deedlen, internal audit, external audit, and-increay durindering politices) 47% 77 Financial financial consulting Information (if accords, technical counterwinessures) Staff (background acreaming) By a whistle-blower at our company Cyber Security Percentage of respondents that experienced a cyber inicident in the past 12 months. MOST COMMON TYPES OF OYBER INCIDENT Data deletion by malekare or oystem issue Denial of service attack Accidental placement of sensitive data that was indexed by a search engine (e.g., Coople) Employee records Trade secreta/ISB/IPP Customer records Physical assets/innory If service vendor Trade secreta/ISB/IPP Customer records The formation of the financial	FRAUD	Management conflict of interest	27%	21%
Market collusion (a.g., price florage) Internal financial fraud management company results) Junior employees of our own company Againts and/or internatidates (e.e., a tind party working on behalf of your company) Freelance/temporary employees Sanice or middle management employees of our own company Joint venture partners (e.e., a tind party working on behalf of your company) Joint venture partners (e.e., a tind party working on behalf of your company) Joint venture partners (e.e., a partners who provides management employees of our own company) Joint venture partners (e.e., a partners who provides management audit, anti-money functions or a franchise) MEASURES MACE COMMON ANTI-FRAUD Financial financial controls, finand detection, internal audit, enternal audit, anti-money functioning problems Partners, clients, and vendors (due diligence) Information of executive, inchread controls, finand detection, internal audit, enternal audit, anti-money functioning problems By a whistler-blower at our company Information of executive, inchread controls management By a whistler-blower at our company Percentage of respondents that experienced a cyber incident in the past 12 months. MOST COMMON TYPES OF OYEER INCIDENT Data deletion or corruption by malware or system issue Data deletion or corruption by malware or system issue Data deletion or corruption by malware or system issue Data deletion or corruption by malware or system issue Data deletion or corruption by malware or system issue Data deletion or corruption by malware or system issue Data deletion or corruption by malware or system issue Data deletion or corruption by malware or system issue Data deletion or corruption by malware or system issue Data deletion or corruption by malware or system issue Data deletion or corruption by malware or system issue Data deletion or corruption by malware or system issue Data deletion or corruption by malware or system issue Data deletion or corruption by malware or system issue Data deletion or corru		Corruption and bribery	27%	15%
Internal financial fraud inensities of company results 25% 20 MOST COMMON PERPETRATORS 25% 20 Agents and/or intermediatins & a. a tend party working on behalf of your company) 49% 27 Freelance/temporary employees 41% 22 Senior or middle management employees of our own company 37% 30 MOST COMMON ANTI-FRAUD 50 50 50 50 MOST COMMON ANTI-FRAUD 50 50 50 50 50 MOST COMMON MEANURS 25 50 50 50 Partners, clients, and vendors (timed audit, enternal audit, entirence) (laundering policies) 87% 77 Partners, clients, and vendors (timed audit, enternal audit, enternal audit, enternal enterna		Vendor, supplier, or procurement fraud	27%	269
Junior employees of our own company Agents and/or intermediaries (e.e. a find party working on behalf of your company) Agents and/or intermediaries (e.e. a find party working on behalf of your company) Freelenco/temporary employees Serior or middle management employees of our own company Joint venture partners (e.e. a partner who provides manufacturing or other business function, or a franchisced Joint venture partners (e.e. a partner who provides manufacturing or other business function, or a franchisced Joint venture partners (e.e. a partner who provides manufacturing or other business function, or a franchisced Joint venture partners, clients, and vendors sible diligenced Financial financial centrols, fraud debetion, internal audit, and money function, or a franchisced Information of a social, technical contentrata audit, and money function, or a franchisced Information of a social, technical contentrata audit, and money function, or a franchisced Information of a social, technical contentrataves) Staff (abolground screening) Staff (abolground screening) By a whistle-blower at our company Cyber Security Percentage of respondents that experienced a cyber incident in the past 12 months. Data deletion or corruption by malkinger or system issue Data deletion by mallicious insider Virus/worm infestation Denial of service attack Accidental placement of sensitive data that was indexed by a search engine (e.g., Geograf) Trade secretes/REDIP Contract when A cyber functions Trade secretes/REDIP Contract when A cyber functions Trade secretes/REDIP Contract when A cyber functions in the past 12 months. Environmental risk fencium deasters such as humcanes, fornadous, foods, carthquakes, etc.) Workplace violence Thetro cross of IP Geographic and political risk (e.g., operating in areas of conflict) Fermanent employees of our own company ERBFORDENTS ARE MOST LIGHT with finite temployees of our own company ERBFORDENTS ARE MOST LIGHT with finite temployees of our own company Encloyment Setseurity Workplace		Market collusion (e.g., price fixing)	27%	179
Agents and/or intermediaties (i.e., a third party working on behalf of your company) Frieelance/bemporary employees Serior or middle management employees of our own company Joint venture partners (ii.e., a partner who provides manufacturing or other business function, or a franchisser) Joint venture partners (ii.e., a partner who provides manufacturing or other business function, or a franchisser) Joint venture partners (ii.e., a partner who provides manufacturing or other business function, or a franchisser) Joint venture partners (ii.e., a partner who provides manufacturing or other business function, or a franchisser) Joint venture partners (iii.e., a partner who provides manufacturing or other business function, or a franchisser) Joint venture partners (iii.e., a partner who provides manufacturing or other business function, or a franchisser) Joint venture partners (iii.e., a partners (iii		Internal financial fraud (manipulation of company results)	25%	209
Agents and/or intermediates (i.e., a third party working on behalf of your company) Freelance/temporary employees Senior or middle management employees of our own company Joint wenture partners (i.e., a partner who provides manufacturing or other business function, or a franchissed) Joint wenture partners (i.e., a partner who provides manufacturing or other business function, or a franchissed) Joint wenture partners, (i.e., a partner who provides manufacturing or other business function, or a franchissed) Joint wenture partners, clients, and vendors (i.e. a diagence) Joint wenture partners, clients, and vendors (i.e. a diagence) Joint wenture partners, clients, and vendors (i.e. a diagence) Information (if accurity, feomeral conformassures) Staff (background screening) By a whistle-blower at our company Percentage of respondents that experienced a cyber incident in the past 12 months. MOST COMMON TYPES OF Other Virus/worm infestation Data deletion by malicious insider Virus/worm infestation Daniel of service attack Accidental placement of sensitive data that was indexed by a search engine (ii.g., Google) Security Percentage of respondents that experienced a cyber incident in the past 12 months. Joint Virus/worm infestation Daniel of service attack Accidental placement of sensitive data that was indexed by a search engine (ii.g., Google) Security Percentage of respondents that experienced a security incident in the past 12 months. MOST COMMON PARTY TO CONTACT WHEN A CYBER (ii.e.) Physical assets/money If service vendor Take secrets/R&D/IP Customer records Physical assets/money If service vendor The for loss of IP Geographic and political risk (ii.e., operating in areas of conflict) Security MOST COMMON PERPETRATORS Permanent employees of our own company Permanent employees of our own company Permanent employees of our own company Workplace vicelence The for root is, including domestic and international events Environmental risk Finity of the fermion of the service states and international ev	MOST COMMON	Junior employees of our own company	61%	399
Senior or middle management employees of our own company Joint venture partners (i.e., is partner who provides manufacturing or other business function, or a franchisea) MOST COMMON ANTI-FRAUD MEASURES Precentage of respondents with a law measure mplemented fine sint-fraud measure Partners, clients, and vendors (side disponce) Information (if socurity, technical countermassures) Staff (background screening) Percentage of frespondents that experienced a cyber incident in the past 12 months. Cyber Security Percentage of frespondents that experienced a cyber incident in the past 12 months. Cyber Incident In the past 12 months. Data deletion or corruption by malware or system issue Data deletion by malicious insider Virus/worm infestation Denial of service attack MOST COMMON TYPES OF Virus/worm infestation Denial of service attack MOST COMMON TARGET Employee records Trade secrets/R8D/IP Customer records Trade secrets/R8D/IP Customer records Physical assets/money IT service vendor IT service vendor The condition of the past 12 months. Percentage of respondents that experienced by a search engine (e.g., Googie) 25% 10 MOST COMMON TARGET Employee records Trade secrets/R8D/IP Customer records Trade secrets/R8D/IP Customer records Trade secrets/R8D/IP Customer records Physical assets/money IT service vendor To service vendor	PERPETRATORS	Agents and/or intermediaries (i.e., a third party working on behalf of your company)	49%	279
MOST COMMON ANTI-FRAUD MEASURES Percentage of respondents who never implemented the anti-fraud measure information of security. **Refined actions in the past 12 months.** **Percentage of respondents who never implemented the anti-fraud measure information of security, **Refined controls (treat disperce)** **Indicate the anti-fraud measure information of security, **Refined contrainessurers)** **Staff (packground screening)** **Bay whistle-blower at our company** **Percentage of respondents that experienced a cyber incident in the past 12 months.** **Percentage of respondents that experienced a cyber incident in the past 12 months.** **Percentage of respondents that experienced a cyber incident in the past 12 months.** **MOST COMMON TYPES OF CYBER INCIDENT** **Data deletion or corruption by malware or system issue** **Data deletion by malicious insider** **Virus-worm infestation** **Data deletion by malicious insider** **Virus-worm		Freelance/temporary employees	41%	279
MOST COMMON ANTI-FRAUD Financial (mancial controls, traud detection, internal audit, external audit, anti-money laundering policies) Partners, clients, and vendors (the diligence) Partners, clients (the diligence) Partners, clents (the dilig		Senior or middle management employees of our own company	37%	309
MAST COMMON TARGET Employee records Employee records MOST COMMON TARGET Employee records Employee records Percentage of respondents who was indexed by a search engine (a.g., Goople) Employee records Trade secrets/RRD/IP Customer records Physical assets/money The security Percentage of respondents that experienced a cyber incident in the past 12 months. Percentage of system issue 28% 22 28% 22 28% 22 28% 24 28% 25% 26% 26% 26% 26% 26% 26% 26% 26% 26% 26		Joint venture partners (i.e., a partner who provides manufacturing or other business function, or a franchise	e) 37 %	239
Partners, clients, and vendors due diligence) ### Partners, clients, and vendors due diligence) ### Partners, clients, and vendors due diligence) ### Partners, clients, and vendors due diligence) ### Partners, clients, and vendors due diligence) ### Partners, clients, and vendors due diligence) ### Partners, clients, and vendors due diligence) ### Partners, clients, and vendors due diligence ### Partners, clients, and vendors due diligence) ### Partners, clients, and vendors due diligence ### Partners, and vendors ### Partners, clients, and vendors due diligence ### Partners, clients, and vendors due diligence ### Partners, clients, and vendor due diligence ### Partners, clients, and vendor due diligence ### Partners, and vendor diligence ### Partners, clients, and vendor due due diligence ### Partners, and vendor despect in clients due to receive de de sever in clients ### Partners, clients due concerns, and vendors despers, and vendor despers, and vendor due search engine (e.g., Google) ### Partners, Common Partners, Complete data that was indexed by a search engine (e.g., Google) ### Partners, Google, despers, and and an analysis of the search engine (e.g., Google) ### Partners, Google, despers, and an analysis of the search engine (e.g., Google) ### Partners, Google, despers, and an analysis of the search engine (e.g., Google) ### Partners, Google, despers, and an analysis of the search engine (e.g., Google) ### Partners, Clients #	MOST COMMON ANTI-FRAUD			779
Information (IT security, technical countermeasures) Staff (background screening) By a whistle-blower at our company) Percentage of respondents that experienced a cyber incident in the past 12 months. MOST COMMON TYPES OF CYBER INCIDENT Data deletion for corruption by mailware or system issue Data deletion by malicious insider Virus/worm infestation Denial of service attack Accidental placement of sensitive data that was indexed by a search engine (a.g., Google) Trade secrets/RSDJIP Quistomer records Trade secrets/RSDJIP Quistomer records Physical assets/money Trade secrets/RSDJIP Contract When A Cyber INCIDENT OCOURRED Security Percentage of respondents that experienced a security incident in the past 12 months. Denial of service attack Accidental placement of sensitive data that was indexed by a search engine (a.g., Google) 25% 10 MOST COMMON PARTY TO CONTRACT WHEN A CYBER INCIDENT OCCURRED Percentage of respondents that experienced a security incident in the past 12 months. Denial of service vendor Percentage of respondents that experienced a security incident in the past 12 months. Denial of service vendor Percentage of respondents that experienced a security incident in the past 12 months. Denial of service vendor Percentage of respondents that experienced a security incident in the past 12 months. Denial of service vendor Percentage of respondents that experienced a security incident in the past 12 months. Denial of service vendor Percentage of respondents that experienced a security incident in the past 12 months. Denial of service vendor Percentage of respondents that experienced a security incident in the past 12 months. Denial of service vendor Percentage of respondents that experienced a security incident in the past 12 months. Denial of service vendor Percentage of respondents that experienced a security incident in the past 12 months. Denial of service vendor Percentage of respondents that vendors vendors vendors vendors vendors vendors vendors vendors vendo		Partners, clients, and vendors (due diligence)	87%	779
Cyber Security Percentage of respondents that experienced a cyber incident in the past 12 months. Data deletion to roundly in sider Virus/worm infestation Denial of service attack Accidental placement of sensitive data that was indexed by a search engine (e.g., Google) Perperentage of respondents that experienced a cyber incident in the past 12 months. Data deletion by malicious insider Virus/worm infestation Denial of service attack Accidental placement of sensitive data that was indexed by a search engine (e.g., Google) Employee records Trade secrets/R&D/IP Customer records Physical assets/money Trade secrets/R&D/IP Customer records Trade secrets/R&D/IP Customer records Trade secrets/R&D/IP Customer records Physical assets/money Trade secrets/R&D/IP Customer records			85%	829
## Percentage of respondents that experienced a cyber incident in the past 12 months. ## Percentage of respondents that experienced a cyber incident in the past 12 months. ## Percentage of respondents that experienced a cyber incident in the past 12 months. ## Percentage of respondents that experienced a cyber incident in the past 12 months. ## Percentage of respondents that experienced a cyber incident in the past 12 months. ## Percentage of respondents that experienced a cyber incident in the past 12 months. ## Percentage of respondents in the past 12 months. ## Percentage of respondents in the past 12 months. ## Percentage of respondents in the past 12 months. ## Percentage of respondents in the past 12 months. ## Percentage of respondents that experienced a security incident in the past 12 months. ## Percentage of respondents that experienced a security incident in the past 12 months. ## Percentage of respondents that experienced a security incident in the past 12 months. ## Percentage of respondents that experienced a security incident in the past 12 months. ## Percentage of respondents that experienced a security incident in the past 12 months. ## Percentage of respondents that experienced a security incident in the past 12 months. ## Percentage of respondents that experienced a security incident in the past 12 months. ## Percentage of respondents that experienced a security incident in the past 12 months. ## Percentage of respondents that experienced a security incident in the past 12 months. ## Percentage of respondents that experienced a security incident in the past 12 months. ## Percentage of respondents that experienced a security incident in the past 12 months. ## Percentage of respondents that experienced a security incident in the past 12 months. ## Percentage of respondents that experienced a security incident in the past 12 months. ## Percentage of respondents that experienced a security incident in the past 12 months. ## Percentage of respondents that experienced a sec		Staff (background screening)	85%	749
Percentage of respondents that experienced a cyber incident in the past 12 months. **Description** **Description** **Description** **Description** **Description** **Description** **Data deletion or corruption by malware or system issue Data deletion by malicious insider Virus/worm infestation Denial of service attack **MOST COMMON PERPETRATIONS** **MOST COMMON TARGET** **Employee records** **Trade secrets/R&D/IP** Customer records** Physical assets/money To secrets/R&D/IP** Customer records* Physical assets/money The service vendor **Trade secrets/R&D/IP** Contact when a cyber incident in the past 12 months. **MOST COMMON TYPES OF SECURITY INCIDENTS** **MOST COMMON TYPES OF SECURITY INCIDENTS** **Procentage of respondents that experienced a security incident in the past 12 months. **MOST COMMON TYPES OF SECURITY INCIDENTS** **MOST COMMON				449
Virus/worm infestation Denial of service attack MOST COMMON PERPETRATORS Accidental placement of sensitive data that was indexed by a search engine (e.g., Google) PERPETRATORS MOST COMMON TARGET Employee records Trade secrets/R&D/IP Customer records Physical assets/money IT service vendor Percentage of respondents that experienced a security incident in the past 12 months. Percentage of respondents that experienced a security incident in the past 12 months. MOST COMMON TYPES OF SECURITY INCIDENTS Environmental risk (including damage caused by natural disasters such as hurricanes, tomadoes, floods, earthquakes, etc.) Workplace violence Theft or loss of IP Geographic and political risk (i.e., operating in areas of conflict) Permanent employees of our own company PERPETRATORS RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY VULNERABLE TO THE FOLLOWING SECURITY Forum including domestic and international events Environmental risk Terrorism, including domestic and international events Environmental risk Findronmental risk Terrorism, including domestic and international events Environmental risk Terrorism, including domestic and international events	MOST COMMON TYPES OF CYBER INCIDENT			Global a
Virus/worm infestation Denial of service attack MOST COMMON PERPETRATORS Accidental placement of sensitive data that was indexed by a search engine (e.g., Google) PERPETRATORS MOST COMMON TARGET Employee records Trade secrets/R&D/IP Customer records Physical assets/money IT service vendor Percentage of respondents that experienced a security incident in the past 12 months. Percentage of respondents that experienced a security incident in the past 12 months. MOST COMMON TYPES OF SECURITY INCIDENTS Environmental risk (including damage caused by natural disasters such as hurricanes, tomadoes, floods, earthquakes, etc.) Workplace violence Theft or loss of IP Geographic and political risk (i.e., operating in areas of conflict) Permanent employees of our own company PERPETRATORS RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY VULNERABLE TO THE FOLLOWING SECURITY Forum including domestic and international events Environmental risk Terrorism, including domestic and international events Environmental risk Findronmental risk Terrorism, including domestic and international events Environmental risk Terrorism, including domestic and international events			27%	199
Accidental placement of sensitive data that was indexed by a search engine (e.g., Google) PERPETRATORS MOST COMMON TARGET Employee records Trade secrets/R8D/IP Customer records Physical assets/money IT service vendor Percentage of respondents that experienced a security incident in the past 12 months. Percentage of respondents that experienced a security incident in the past 12 months. Environmental risk (including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.) Workplace violence Theft or loss of IP Geographic and political risk (i.e., operating in areas of conflict) MOST COMMON PRESON (Including damage caused by natural disasters of conflict) MOST COMMON (Including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.) Workplace violence Theft or loss of IP Geographic and political risk (i.e., operating in areas of conflict) MOST COMMON (Including damage caused by natural disasters of conflict) MOST COMMON (Including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.) Workplace violence The following seconds: Workplace violence Terrorism, including domestic and international events Environmental risk Environmental risk Terrorism, including domestic and international events Environmental risk Terrorism, including domestic and international events Environmental risk Terrorism (Including domestic and international events)		Virus/worm infestation	23%	339
MOST COMMON TARGET Employee records Trade secrets/R&D/IP Customer records Physical assets/money MOST COMMON PARTY TO CONTACT WHEN A CYBER INCIDENT OCCURRED Percentage of respondents that experienced a security incident in the past 12 months. Percentage of respondents that experienced a security incident in the past 12 months. Cidental Common TYPES OF SECURITY INCIDENTS Environmental risk (including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.) Workplace violence Theft or loss of IP Geographic and political risk (i.e., operating in areas of conflict) MOST COMMON PERPETRATORS RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY VULNERABLE TO THE FOLLOWING SECURITY Environmental risk Environmental		Denial of service attack	23%	149
Trade secrets/R&D/IP Customer records Physical assets/money IT service vendor Trade secrets/R&D/IP Customer records Physical assets/money IT service vendor IT service vendor Trade secrets/R&D/IP Customer records Physical assets/money IT service vendor IT service vendor Trade secrets/R&D/IP A 5% 51 A 5% 38 Percentage of respondents that experienced a security incident in the past 12 months. Environmental risk (including damage caused by natural disasters such as hurricanes, tomadoes, floods, earthquakes, etc.) Workplace violence Theft or loss of IP Geographic and political risk (i.e., operating in areas of conflict) MOST COMMON PERPETRATORS RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY VULNERABLE TO THE FOLLOWING SECURITY Environmental risk Environ		Accidental placement of sensitive data that was indexed by a search engine (e.g., Google)	25%	109
Customer records Physical assets/money MOST COMMON PARTY TO CONTACT WHEN A CYBER INCIDENT OCCURRED Percentage of respondents that experienced a security incident in the past 12 months. Percentage of respondents that experienced a security incident in the past 12 months. Environmental risk (including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.) Workplace violence Theft or loss of IP Geographic and political risk (i.e., operating in areas of conflict) MOST COMMON PERPETRATORS RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY VULNERABLE TO THE FOLLOWING SECURITY Environmental risk Tervironmental risk Tervironment	MOST COMMON TARGET	Employee records	59%	409
Physical assets/money MOST COMMON PARTY TO CONTACT WHEN A CYBER INCIDENT OCCURRED Percentage of respondents that experienced a security incident in the past 12 months. Percentage of respondents that experienced a security incident in the past 12 months. Environmental risk (including damage caused by natural disasters such as hurricanes,tornadoes, floods, earthquakes, etc.) Workplace violence Theft or loss of IP Geographic and political risk (i.e., operating in areas of conflict) MOST COMMON PERPETRATORS RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY VULNERABLE TO THE FOLLOWING SECURITY Workplace violence Terrorism, including domestic and international events Environmental risk 145% 38 27 40% 27		Trade secrets/R&D/IP	48%	409
MOST COMMON PARTY TO CONTACT WHEN A CYBER INCIDENT OCCURRED Percentage of respondents that experienced a security incident in the past 12 months. Percentage of respondents that experienced a security incident in the past 12 months. Environmental risk (including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.) Workplace violence Theft or loss of IP Geographic and political risk (i.e., operating in areas of conflict) Permanent employees of our own company Workplace violence RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY VULNERABLE TO THE FOLLOWING SECURITY Following SECURITY Terrorism, including domestic and international events Environmental risk Total Common points above global average of 68% 40% 27 40% 2		Customer records	45%	519
Percentage of respondents that experienced a security incident in the past 12 months. Environmental risk (including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.) Workplace violence Theft or loss of IP Geographic and political risk (i.e., operating in areas of conflict) MOST COMMON PERPETRATORS RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY VULNERABLE TO THE FOLLOWING SECURITY Workplace violence Terrorism, including domestic and international events Environmental risk Terrorism, including domestic and international events Environmental risk Terrorism, including domestic and international events Environmental risk Terrorism, including domestic and international events Terrorism, including domestic and international events Environmental risk Terrorism (1200 points above globs average of 68% Terrorism (1200 points) Terrorism (Physical assets/money	45%	389
Experienced a security incident in the past 12 months. MOST COMMON TYPES OF SECURITY INCIDENTS Environmental risk (including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.) Workplace violence Theft or loss of IP Geographic and political risk (i.e., operating in areas of conflict) MOST COMMON PERPETRATORS RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY VULNERABLE TO THE FOLLOWING SECURITY Environmental risk Environmental risk experienced a security incident in the past 12 months. 40% 27 40% 20 40% 27 40% 20 4	MOST COMMON PARTY TO CONTACT WHEN A CYBER INCIDENT OCCURRED	IT service vendor	34%	27%
MOST COMMON TYPES OF SECURITY INCIDENTS Environmental risk (including damage caused by natural disasters such as hurricanes, tornadoes, floods, earthquakes, etc.) Workplace violence Theft or loss of IP Geographic and political risk (i.e., operating in areas of conflict) MOST COMMON PERPETRATORS RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY VULNERABLE TO THE FOLLOWING SECURITY Environmental risk Environmental risk 140% 27 40% 28 37% 28 38 38 38 38 20	Security	72 experienced a security incident $ riangle 4\%$		%
Theft or loss of IP Geographic and political risk (i.e., operating in areas of conflict) MOST COMMON PERPETRATORS Permanent employees of our own company PERPETRATORS Workplace violence Terrorism, including domestic and international events 45% 18 Environmental risk Theft or loss of IP 35% 22 26% 17 27 28 29 20 20 20 20 20 20 21 22 23 24 25 26% 27 27 27 28 29 20 20 20 20 20 20 20 20 20	MOST COMMON TYPES OF SECURITY INCIDENTS		40%	27%
Geographic and political risk (i.e., operating in areas of conflict) MOST COMMON PERPETRATORS RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY VULNERABLE TO THE FOLLOWING SECURITY Geographic and political risk (i.e., operating in areas of conflict) 26% 17 26% 27 27 28 29 29 20 20 20 20 21 21 22 23 24 25% 18 26% 18		Workplace violence	37%	239
MOST COMMON PERPETRATORS RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY VULNERABLE TO THE FOLLOWING SECURITY Permanent employees of our own company Workplace violence 52% 27 Terrorism, including domestic and international events 45% 18 270 280 290 291 292 293 293 294 295 295 297 297 298 298 298 298 298 298		Theft or loss of IP	35%	389
PERPETRATORS RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY VULNERABLE TO THE FOLLOWING SECURITY Workplace violence 52% 27 Terrorism, including domestic and international events 45% 18 200		Geographic and political risk (i.e., operating in areas of conflict)	35%	229
LIKELY TO FEEL HIGHLY VULNERABLE TO THE FOLLOWING SECURITY Terrorism, including domestic and international events 45% 18 20		Permanent employees of our own company	26%	179
VULNERABLE TO THE FOLLOWING SECURITY Environmental risk 18 Ierrorism, including domestic and international events 45% 18 20 21		Workplace violence	52%	279
FOLLOWING SECURITY Environmental risk 20		Terrorism, including domestic and international events	45%	189
RISKS (including damage caused by natural disasters such as hurricanes,tornadoes, floods, earthquakes, etc.)	FOLLOWING SECURITY RISKS		37%	209

BRAZIL REPORT CARD

Fraud		ntage of respondents ed by fraud in the past nths.	▼ 9% ▼ 14%	points below 2015 points below average of 82	global % ^{Global} avg.
MOST COMMON TYPES OF	Theft of physical assets or	stock		24%	29%
FRAUD	Information theft, loss or at	tack (e.g., data theft)		21%	24%
	Vendor, supplier or procure	ment fraud		21%	26%
MOST COMMON	Ex-employees			43%	27%
PERPETRATORS	Freelance/temporary emplo	pyees		26%	27%
	Junior employees of our ow	n company		22%	39%
	Vendors/suppliers (i.e., a pro	vider of technology or services to your company)		17%	26%
	Agents and/or intermediarie	es (i.e., a 3rd party working on behalf of your comp	any)	17%	27%
	Joint venture partners (i.e., a	a partner who provides manufacturing or other busi	iness function, or a francl	nisee) 17%	23%
	Customers			17%	19%
MOST COMMON ANTI-FRAUD	Assets (physical security syste	ms, stock inventories, tagging, asset register)		88%	79%
MEASURES Percentage of respondents who have	Information (IT security, techn	nical countermeasures)		88%	82%
implemented the anti-fraud measure.	Management (management o	controls, incentives, external supervision such as au	ıdit committee)	85%	74%
MOST COMMON MEANS OF DISCOVERY	Through an internal audit			43%	36%
Cyber Security	76 experie	ntage of respondents that enced a cyber incident past 12 months.	→ 9%	points below average of 85	global % Global avg.
MOST COMMON TYPES OF	Virus/ worm infestation			41%	33%
CYBER INCIDENT	Data breach resulting in los	s 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 identit	у		42%	36%
MOST COMMON PARTY TO CONTACT WHEN A CYBER INCIDENT OCCURRED	Webhosting/website provic	ler		23%	9%
Security	53 experie	ntage of respondents that enced a security incident past 12 months.	▼ 15%	points below average of 68	global % Global ava.
MOST COMMON TYPES OF	Theft or loss of IP			32%	38%
SECURITY INCIDENTS	Environmental risk (including damage caused by n	atural disasters such as hurricanes, tornadoes, floc	ods, earthquakes, etc.)	18%	27%
	Geographic and political ris	k (i.e., operating in areas of conflict)		12%	22%
MOST COMMON PERPETRATORS	Ex-employees			39%	23%
RESPONDENTS ARE MOST	Theft or loss of IP			21%	19%
LIKELY TO FEEL HIGHLY VULNERABLE TO THE	Workplace violence			18%	27%
FOLLOWING SECURITY	Geographic and political ris	sk (i.e., operating in areas of conflict)		15%	12%
RISKS	Environmental risk (including damage caused by n	atural disasters such as hurricanes, tornadoes, floc	nds, earthquakes, etc.)	15%	20%

COLOMBIA REPORT CARD

Fraud	Percentage of respondents affected by fraud in the past	★ 12%	points above 2015
Tradu	12 months.	13%	points above global average of 82%
MOST COMMON TYPES OF	Management conflict of interest		43% 21%
FRAUD	Vendor, supplier, or procurement fraud		43% 26%
	Theft of physical assets or stock		38% 29%
MOST COMMON PERPETRATORS	Ex-employees		35% 27%
PENPETRATORS	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	Financial (financial controls, fraud detection, internal audit, external audit, anti-m	oney laundering policies)	95% 77%
Percentage of respondents who have	Assets (physical security systems, stock inventories, tagging, asset register)		95% 79%
implemented the anti-fraud measure.	Staff (background screening)		95% 74%
MOST COMMON MEANS OF DISCOVERY	Through an internal audit		50% 39%
Cyber Security	Percentage of respondents that experienced a cyber incident in the past 12 months.	10%	points above global average of 85%
MOST COMMON TYPES OF	Virus/worm infestation		52% 33%
CYBER INCIDENT	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 response firm		15% 14%
INCIDENT OCCURRED	Insurance portal		15% 5%
	Webhosting/website provider		15% 9%
Security	Percentage of respondents that experienced a security incident in the past 12 months.	▼ 6%	points below global average of 68%
MOST COMMON TYPES OF	Workplace violence		24% 23%
SECURITY INCIDENTS	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	Terrorism, including domestic and international events		19% 18%
LIKELY TO FEEL HIGHLY VULNERABLE TO THE	Workplace violence		19% 27%
FOLLOWING SECURITY RISKS	Environmental risk (including damage caused by natural disasters such as hurricanes,tornadoes, floo	ods, earthquakes, etc.)	14% 20%

MEXICO REPORT CARD

		Percentage of respondents affected	2 %	points above 2015	
Fraud	82	by fraud in the past 12 months.	=	equal to global average of 82%	Global avo
MOST COMMON TYPES OF	Vendor, supplier, o	or procurement fraud		52%	26%
FRAUD	Theft of physical a	assets or stock		30%	29%
	Corruption and bri	ibery		18%	15%
MOST COMMON	Ex-employees			33%	27%
PERPETRATORS	Junior employees	of our own company		30%	39%
	Freelance/tempora	ary employees		30%	27%
	Vendors/suppliers	(i.e., a provider of technology or services to your company)		30%	26%
	Agents and/or inte	ermediaries (i.e., a third party working on behalf of your company)		26%	27%
MOST COMMON	Partners, clients, a	and vendors (due diligence)		82%	77%
ANTI-FRAUD MEASURES	Financial (financial o	controls, fraud detection, internal audit, external audit, anti-money la	aundering policies)	82%	77%
	Risk (risk officer and	l risk management system)		81%	78%
MOST COMMON MEANS OF DISCOVERY	Through an interna	al audit		44%	39%
Cyber Security	82	Percentage of respondents that experienced a cyber incident in the past 12 months.	▼ 3%	points below glo average of 85%	obal Global avg
MOST COMMON TYPES OF	Virus/worm infesta	ation		39%	33%
CYBER INCIDENT	Email-based phish	ning attack		33%	26%
	Data deletion or co	orruption by malware or system issue		33%	22%
MOST COMMON PERPETRATORS	Competitors			22%	6%
MOST COMMON TARGET	Company/employe	ee identity		52%	36%
	Customer records	3		48%	51%
	Physical assets/m	oney		37%	38%
MOST COMMON PARTY TO CONTACT WHEN A CYBER INCIDENT OCCURRED	Federal law enforc	cement		30%	8%
Security	48	Percentage of respondents that experienced a security incident in the past 12 months.	▼ 20%	points below glo average of 68%	obal Global avg
MOST COMMON TYPES OF SECURITY INCIDENTS	Environmental risk	(aused by natural disasters such as hurricanes, tornadoes, floods, ea	arthquakes, etc.)	27%	27%
SECONITY INCIDENTS	Theft or loss of IP			24%	38%
	Geographic and p	political risk (i.e., operating in areas of conflict)		21%	22%
MOST COMMON	Freelance/tempora			31%	16%
PERPETRATORS	Ex-employees			31%	23%
RESPONDENTS ARE MOST	Workplace violence	ce		24%	27%
LIKELY TO FEEL HIGHLY	·	ng domestic and international events		21%	18%
VULNERABLE TO THE FOLLOWING SECURITY	Theft or loss of IP	and international events		18%	19%
RISKS				10 /0	.3,0