CONSTRUCTION, ENGINEERING, AND INFRASTRUCTURE

Froud	Percentage of respondents affected * 5%	points belov 2015	v
Fraud	by fraud in the past 12 months. \downarrow 12%	points belov average of 8	v global 32% _{Global avg.}
MOST COMMON TYPES OF	Vendor, supplier, or procurement fraud	28	
FRAUD	Internal financial fraud (manipulation of company results)	21	% 20%
	Corruption and bribery	19	% 15%
	Misappropriation of company funds	19	% 18%
	Theft of physical assets or stock	19	% 29%
MOST COMMON PERPETRATORS	Junior employees	45	% 39%
	Ex-employees	33	% 27%
	Senior or middle management employees	30	% 30%
	Freelance/temporary employees	30	% 27%
	Vendors/suppliers	30	% 26%
MOST COMMON ANTI-	Staff (training, whistle-blower hotline),	81	% 76%
FRAUD MEASURES Percentage of respondents who	Staff (background screening)	79	% 74%
have implemented the anti-fraud measure.	Partners, clients, and vendors (due diligence)	79	% 77%
	Information (IT security, technical countermeasures)	79	% 82%
	Risk (risk officer and risk management system)	79	% 78%
MOST COMMON MEANS OF DISCOVERY	Through an internal audit	38	% 39%
Cyber Security	Percentage of respondents that experienced a cyber incident in the past 12 months.	points belov average of 8	v global 15% _{Global avg.}
MOST COMMON TYPES OF	Virus/worm infestation	35	% 33%
CYBER INCIDENT	Email-based phishing attack	30	% 26%
	Data deletion or loss due to system issues	30	% 24%
MOST COMMON PERPETRATORS	Ex-Employees	20	% 20%
MOST COMMON TARGET	Customer records	59	% 51%
	Employee records	45	% 40%
	Physical assets/money	43	% 38%
Security	63 Percentage of respondents that experienced a security incident in the past 12 months. ▼ 5%	points belov average of 6	v global 88%
MOST COMMON TYPES OF	Environmental risk	33	Global avg. 27%
SECURITY INCIDENTS	Theft or loss of IP	32	% 38%
	Geographic and political risk	23	% 22%
	Workplace violence	23	% 23%
MOST COMMON PERPETRATORS	Ex-Employees	25	% 23%
RESPONDENTS ARE MOST	Theft or loss of intellectual property	18	% 19%
LIKELY TO FEEL HIGHLY VULNERABLE TO THE	Environmental risk	18	% 20%
FOLLOWING SECURITY RISKS	Workplace violence	12	% 27%

CONSUMER GOODS	Top responses given	by survey respon	ndent
Fraud	82 by fraud in the past 12 months.	points above 2015 Equal to global average of 82%	Global a
MOST COMMON TYPES OF	Information theft, loss, or attack (e.g., data theft)	32%	24%
FRAUD	Theft of physical assets or stock	28%	29%
	Vendor, supplier, or procurement fraud	28%	26%
MOST COMMON	Agents and/or intermediaries	43%	279
PERPETRATORS	Junior employees	37%	39%
	Vendors/suppliers	35%	269
	Joint venture partners	31%	239
	Senior or middle management employees	24%	309
MOST COMMON	Information (IT security, technical countermeasures)	77%	829
ANTI-FRAUD MEASURES	Assets (physical security systems, stock inventories, tagging, asset register)	77%	799
Percentage of respondents who have implemented the anti-fraud	Board of director engagement in cyber security policies and procedures		759
measure. MOST COMMON MEANS OF	By a whistle-blower at our company		449
Cyber Security	 Percentage of respondents that experienced a cyber incident in the past 12 months. 	points below glob average of 85%	bal _{Global}
MOST COMMON TYPES OF	Email-based phishing attack	28%	269
CYBER INCIDENT	Data breach resulting in loss of customer or employee data	27%	239
	Virus/worm infestation	27%	339
MOST COMMON PERPETRATORS	Ex-employees	28%	209
MOST COMMON TARGET	Customer records	62%	519
	Trade secrets/R&D/IP	54%	409
	Company/employee identity	30%	369
Security	Percentage of respondents that experienced a security incident in the past 12 months.	points above glob average of 68%	bal
MOST COMMON TYPES OF	Theft or loss of IP	27%	38%
SECURITY INCIDENTS	Environmental risk	27%	279
	Terrorism	20%	15%
	Geographic and political risk	20%	229
MOST COMMON PERPETRATORS	Ex-employees	31%	239
RESPONDENTS ARE MOST	Theft or loss of IP	22%	199
LIKELY TO FEEL HIGHLY VULNERABLE TO THE	Workplace violence	20%	279
FOLLOWING SECURITY RISKS	Environmental risk	18%	209

FINANCIAL SERVICES REPORT CARD

		011112	Top responses give	sin by survey resp	Jondeni
	Percentage of reapendente offected	19% points above 2015			
Fraud	89	89 Percentage of respondents affected by fraud in the past 12 months.		points above g average of 829	global %
MOST COMMON TYPES OF	Theft of physica	Il assets or stock		39%	Global a
FRAUD	Vendor, supplie	r, or procurement fraud		32%	26%
		ade secrets, piracy, or counterfeiting)		27%	169
MOST COMMON	Junior employee	98		38%	, 39%
PERPETRATORS	Ex-employees			34%	27%
	Senior or middle	e management employees		32%	, 309
	Vendors/supplie			24%	269
		orary employees		22%	279
MOST COMMON		ind risk management system)		88%	, 789
ANTI-FRAUD MEASURES		ecurity, technical countermeasures)		84%	
Percentage of respondents who have implemented the anti-fraud		nent and trademark monitoring program)		84%	
MOST COMMON MEANS OF DISCOVERY	Through an exte	ernal audit		40%	369
Cyber Security	89	Percentage of respondents that experienced a cyber incident in the past 12 months.	♠ 4%	points above g average of 859	global % _{Global}
MOST COMMON TYPES OF	Data deletion or	loss due to system issues		30%	
CYBER INCIDENT	Email-based ph	ishing attack		27%	26%
	Virus/worm infe	station		27%	33
MOST COMMON PERPETRATORS	Ex-employees			28%	20
MOST COMMON TARGET	Customer recor	ds		42%	519
	Trade secrets/R	&D/IP		38%	4 09
	Company/emplo	oyee identity		38%	369
Security	57	Percentage of respondents that experienced a security incident in the past 12 months.	♥ 11%	points below g average of 689	jlobal %
MOST COMMON TYPES OF	Theft or loss of	IP		34%	Global 389
SECURITY INCIDENTS	Geographic and	d political risk		20%	229
	Workplace viole			16%	239
MOST COMMON PERPETRATORS	Ex-employees			31%	
RESPONDENTS ARE MOST	Terrorism			21%	18
RESPONDENTS ARE MOST LIKELY TO FEEL HIGHLY				20%	
	Workplace viole				
LIKELY TO FEEL HIGHLY VULNERABLE TO THE FOLLOWING SECURITY	Workplace viole			18%	

HEALTHCARE, PHARMACEUTICALS, AND BIOTECHNOLOGY

	Percentage of respondents affected 11% points	above
Fraud	by fraud in the past 12 months.	below global ge of 82% _{Global al}
MOST COMMON TYPES OF	Vendor, supplier, or procurement fraud	37% 26%
FRAUD	Theft of physical assets or stock	31% 29%
	Misappropriation of company funds	27% 18%
MOST COMMON	Junior employees	44% 39%
PERPETRATORS	Agents and/or intermediaries	37% 27%
	Senior or middle management employees	34% 30%
	Ex-employees	29% 27%
	Joint venture partners	27% 23%
MOST COMMON	Financial (financial controls, fraud detection, internal audit, external audit, anti-money laundering policies)	94% 77%
ANTI-FRAUD MEASURES Percentage of respondents who	Information (IT security, technical countermeasures)	92% 82%
have implemented the anti-fraud measure.	Management (management controls, incentives, external supervision such as audit committee)	92% 74%
	Risk (risk officer and risk management system)	92% 78%
MOST COMMON MEANS OF DISCOVERY	By a whistle-blower at our company	63% 44%
Cyber Security	Percentage of respondents that experienced a cyber incident in the past 12 months.	above global ge of 85% _{Global a} r
MOST COMMON TYPES OF	Virus/worm infestation	45% 33%
CYBER INCIDENT	Email-based phishing attack	35% 26%
	Data breach resulting in loss of customer or employee data	29% 23%
	Data deletion or corruption by malware or system issue	29% 22%
MOST COMMON PERPETRATORS	Ex-employees	20% 20%
MOST COMMON TARGET	Customer records	48% 51%
	Employee records	48% 40%
	Company/employee identity	45% 36%
Security	 Percentage of respondents that experienced a security incident in the past 12 months. 	below global ge of 68% _{Global a} r
MOST COMMON TYPES OF	Environmental risk	35% 27%
SECURITY INCIDENTS	Theft or loss of intellectual property	31% 38%
	Geographic and political risk	27% 22%
MOST COMMON PERPETRATORS	Freelance/temporary employees	15% 16%
RESPONDENTS ARE MOST	Workplace violence	35% 27%
LIKELY TO FEEL HIGHLY VULNERABLE TO THE	Terrorism	25% 18%
FOLLOWING SECURITY RISKS	Theft or loss of IP	20% 19%
	Environmental risk	20% 20%

IANUFACTURING			Top responses give	ən by survey respo	onden
Fraud		Percentage of respondents affected by fraud in the past 12 months.	▲ 7%▲ 7%	points above hig than 2015 points above glo average of 82%	obal
MOST COMMON TYPES OF	Information theft,	loss, or attack (e.g., data theft)		30%	24%
FRAUD	Regulatory or con	npliance breach		30%	21%
	IP theft (e.g., of trac	de secrets, piracy or counterfeiting)		26%	16%
MOST COMMON	Junior employees	;		39%	39%
PERPETRATORS	Freelance/tempor	rary employees		37%	279
	Senior or middle r	management employees		33%	309
	Ex-employees			33%	279
	Vendors/suppliers	S		33%	269
MOST COMMON	Management (mar	nagement controls, incentives, external supervision such as audi	it committee)	88%	749
ANTI-FRAUD MEASURES Percentage of respondents who	Information (IT sec	urity, technical countermeasures)		86%	829
nave implemented the anti-fraud measure.	Staff (training, whist	tle-blower hotline)		79%	749
MOST COMMON MEANS OF DISCOVERY	Through an intern	al audit		51%	39%
Cyber Security	91	Percentage of respondents that experienced a cyber incident in the past 12 months.	♠ 6%	points above glo average of 85%	obal
MOST COMMON TYPES OF	Virus/worm infest	ation		39%	339
CYBER INCIDENT	Data breach resul	lting in loss of IP/trade secrets/R&D		35%	199
	Email-based phisl	hing attack		35%	269
MOST COMMON PERPETRATORS	Agents and/or inte	ermediaries		23%	139
MOST COMMON TARGET	Customer records	ŝ		63%	519
	Trade secrets/R&I	D/IP		52%	409
	Employee records	S		44%	40%
Security	81	Percentage of respondents that experienced a security incident in the past 12 months.	1 3%	points above glo average of 68%	
MOST COMMON TYPES OF	Theft or loss of IP			56%	Global
SECURITY INCIDENTS	Environmental risk	k		28%	279
	Workplace violend	ce		26%	239
MOST COMMON PERPETRATORS	Competitors			24%	12
RESPONDENTS ARE MOST	Environmental risk	k		28%	209
LIKELY TO FEEL HIGHLY	Workplace violend	ce		21%	279
/ULNERABLE TO THE					

MANITEA CTITOINC

NATURAL RESOURCES

Top responses given by survey respondents.

★ 3% points above 2015

-	Percentage of respondents affected $\mathbf{T} \mathbf{y} \mathbf{y} 0$ 2013	nts above 5			
Fraud	by fraud in the past 12 months.	nts below glo rage of 82%	bal _{Global}		
MOST COMMON TYPES OF	Vendor, supplier, or procurement fraud	30%	269		
FRAUD	Money laundering	30%	15		
	Management conflict of interest	28%	21		
	Freelance/temporary employees	35%	27		
PERPETRATORS	Junior employees	30%	39		
	Ex-employees	30%	27		
	Joint venture partners	30%	23		
	Senior or middle management employees				
	Regulators	28%	14		
NOST COMMON	Information (IT security, technical countermeasures)	80%	82		
ANTI-FRAUD MEASURES Percentage of respondents who	IP (IP risk assessment and trademark monitoring program)	80%	78		
ave implemented the anti-fraud neasure.	Financial (financial controls, fraud detection, internal audit, external audit, anti-money laundering policies)	78%	7		
	Partners, clients, and vendors (due diligence)	78%	7		
MOST COMMON MEANS OF	By a whistle-blower at our company	50%	4		
		nt above glol			
	in the past 12 months.	rage of 85%	Glob		
MOST COMMON TYPES OF	Virus/worm infestation	rage of 85%	Glob 33		
MOST COMMON TYPES OF	Virus/worm infestation Lost equipment with sensitive data	rage of 85% 36% 30%	Glob 33		
MOST COMMON TYPES OF	Virus/worm infestation Lost equipment with sensitive data Data breach resulting in loss of customer or employee data	36% 30% 24%	Glob 3 1 2		
MOST COMMON TYPES OF	Virus/worm infestation Lost equipment with sensitive data Data breach resulting in loss of IP/trade secrets/R&D	36% 30% 24% 24%	Glot 3 1 2 1		
MOST COMMON TYPES OF CYBER INCIDENT MOST COMMON	Virus/worm infestation Lost equipment with sensitive data Data breach resulting in loss of customer or employee data	36% 30% 24%	Globb 33 17 23 17 17 19		
MOST COMMON TYPES OF CYBER INCIDENT MOST COMMON PERPETRATORS	Virus/worm infestation aver Lost equipment with sensitive data aver Data breach resulting in loss of customer or employee data aver Data breach resulting in loss of IP/trade secrets/R&D aver Data deletion by malicious insider aver Ex-employees aver	 36% 30% 24% 24% 24% 19% 	Glob 3: 11 2: 11 11 2: 2: 2:		
MOST COMMON TYPES OF CYBER INCIDENT MOST COMMON PERPETRATORS	Virus/worm infestation Lost equipment with sensitive data Data breach resulting in loss of customer or employee data Data breach resulting in loss of IP/trade secrets/R&D Data deletion by malicious insider Ex-employees Employee records	 36% 30% 24% 24% 24% 19% 58% 	Glob 3 1 1 1 1 1 2 1 1 2 1 2 1 1 1 1 1 2 1 1		
Cyber Security MOST COMMON TYPES OF CYBER INCIDENT MOST COMMON PERPETRATORS MOST COMMON TARGET	Virus/worm infestation aver Lost equipment with sensitive data ata breach resulting in loss of customer or employee data Data breach resulting in loss of IP/trade secrets/R&D ata breach resulting in loss of IP/trade secrets/R&D Data deletion by malicious insider ata employees Employee records ata breach resulting in loss of IP/trade secrets/R&D	rage of 85% 36% 30% 24% 24% 24% 19% 58% 53%	Glot 3 1 1 2 1 1 1 2 1 2 1 2 1 2 1 2 1 2 1 2		
MOST COMMON TYPES OF CYBER INCIDENT MOST COMMON PERPETRATORS MOST COMMON TARGET	Virus/worm infestation Lost equipment with sensitive data Data breach resulting in loss of customer or employee data Data breach resulting in loss of IP/trade secrets/R&D Data deletion by malicious insider Ex-employees Employee records Customer records Physical assets/money Percentage of respondents that experienced a conjunction of the formation of t	 36% 30% 24% 24% 24% 19% 58% 	Globb 33 17 22 17 17 20 17 20 40 5 38		
MOST COMMON TYPES OF CYBER INCIDENT MOST COMMON PERPETRATORS MOST COMMON TARGET Security MOST COMMON TYPES OF	Virus/worm infestation Lost equipment with sensitive data Data breach resulting in loss of customer or employee data Data breach resulting in loss of IP/trade secrets/R&D Data deletion by malicious insider Ex-employees Employee records Customer records Physical assets/money Percentage of respondents that experienced a security incident in $4 \ 2\%$ prime	age of 85% 36% 30% 24% 24% 19% 58% 53% 47%	Globb 33 11 22 11 12 20 5 5 5 38 38 38 00 ball Glob		
MOST COMMON TYPES OF CYBER INCIDENT MOST COMMON PERPETRATORS MOST COMMON TARGET Security MOST COMMON TYPES OF	Virus/worm infestation Lost equipment with sensitive data Data breach resulting in loss of customer or employee data Data breach resulting in loss of IP/trade secrets/R&D Data deletion by malicious insider Ex-employees Employee records Customer records Physical assets/money Percentage of respondents that experienced a security incident in the past 12 months.	rage of 85% 36% 30% 24% 24% 24% 19% 58% 53% 47%	Globbal Globbal Globbal		
MOST COMMON TYPES OF CYBER INCIDENT MOST COMMON PERPETRATORS MOST COMMON TARGET Security MOST COMMON TYPES OF	Virus/worm infestation Lost equipment with sensitive data Data breach resulting in loss of customer or employee data Data breach resulting in loss of lP/trade secrets/R&D Data deletion by malicious insider Ex-employees Employee records Customer records Physical assets/money Percentage of respondents that experienced a security incident in the past 12 months.	rage of 85% 36% 30% 24% 24% 24% 19% 53% 53% 47%	Glot 3 1 1 1 1 2 4 5 3 5 5 3 5 5 6 1 1 1 1 1 1 1 1 1 1 1 1 1		
MOST COMMON TYPES OF TYBER INCIDENT	Virus/worm infestation aver Lost equipment with sensitive data ata Data breach resulting in loss of customer or employee data ata Data breach resulting in loss of IP/trade secrets/R&D ata Data deletion by malicious insider ata Ex-employees ata Employee records ata sets/money Image: Comparison of the past 12 months. ata 22% Private of the past 12 months. ata 22% Image: Comparison of the past 12 months. ata 22% Image: Comparison of the past 12 months. ata 22% Customer records ata 22% Image: Comparison of the past 12 months. ata 22%	rage of 85% 30% 24% 24% 24% 19% 58% 53% 47% 47%	Glob 3: 11 2: 11 2: 4: 5: 3: 3: 5: 3: 5: 3: 5: 3: 2: 2: 2: 2: 2: 2: 2: 2: 2: 2		
AOST COMMON TYPES OF CYBER INCIDENT AOST COMMON PERPETRATORS AOST COMMON TARGET Security MOST COMMON TYPES OF SECURITY INCIDENTS AOST COMMON PERPETRATORS RESPONDENTS ARE MOST	Virus/worm infestation Lost equipment with sensitive data Data breach resulting in loss of customer or employee data Data breach resulting in loss of IP/trade secrets/R&D Data deletion by malicious insider Ex-employees Employee records Customer records Physical assets/money Percentage of respondents that experienced a security incident in the past 12 months. Theft or loss of IP Environmental risk Workplace violence	rage of 85% 36% 30% 24% 24% 19% 58% 53% 47% hts above gla 18% 38% 36%	Globb 3: 11 2: 11 2: 11 2: 2: 3: 3: 3: 3: 3: 2: 2: 2: 2: 11		
MOST COMMON TYPES OF CYBER INCIDENT MOST COMMON PERPETRATORS	Virus/worm infestation Lost equipment with sensitive data Data breach resulting in loss of customer or employee data Data breach resulting in loss of IP/trade secrets/R&D Data deletion by malicious insider Ex-employees Employee records Customer records Physical assets/money Percentage of respondents that experienced a security incident in the past 12 months. Theft or loss of IP Environmental risk Workplace violence Permanent employees of our own company	rage of 85% 36% 30% 24% 24% 24% 19% 58% 53% 47% 47% 47% 40% 38% 36% 26%	Glob 33 11 22 11 12 20 40 5		

Top responses given by survey respondents

PROFESSIONAL SERVICES

▲ 12% points above 2015 Percentage of respondents affected Fraud points above global average of 82% by fraud in the past 12 months. 2% Global avo MOST COMMON TYPES OF 21% Management conflict of interest 29% FRAUD 29% 29% Theft of physical assets or stock Information theft, loss, or attack (background screening) 20% 24% MOST COMMON 35% 39% Junior employees PERPETRATORS 27% Freelance/temporary employees 28% 26% 27% Ex-employees Senior or middle management employees 23% 30% 19% Customers 21% MOST COMMON Partners, clients, and vendors (due diligence) 82% 77% ANTI-FRAUD MEASURES 78% Percentage of respondents who have implemented the anti-fraud Risk (risk officer and risk management system) 80% Assets (physical security systems, stock inventories, tagging, asset register) 79% 78% MOST COMMON MEANS OF By a whistle-blower at our company 42% 44% DISCOVERY Percentage of respondents that point below global average of 85% 1% **Cyber Security** experienced a cyber incident in the past 12 months. Global avo Virus/worm infestation 35% 33% 14% Denial of service attack 20% 22% Data deletion or corruption by malware or system issue 20% MOST COMMON Ex-Employees 23% 20% PERPETRATORS Customer records 51% 53% Trade secrets/R&D/IP 30% 40% 28% 36% Company/employee identity Physical assets/money 28% 38% Percentage of respondents that points below global average of 68% **Security** 5% experienced a security incident in the past 12 months. MOST COMMON TYPES OF Theft or loss of IP 35% 38% SECURITY INCIDENTS Environmental risk 22% 27% Workplace violence 23% 20% MOST COMMON Ex-Employees 38% 23% PERPETRATORS **RESPONDENTS ARE MOST** Workplace violence 27% 27% LIKELY TO FEEL HIGHLY 18% Terrorism 14% VULNERABLE TO THE FOLLOWING SECURITY Theft or loss of IP 10% 19% Environmental risk 10% 20%

RETAIL, WHOLESALE, AND DISTRIBUTION

Top responses given by survey respondents points above 2015 **4%** Percentage of respondents affected point above global average of 82% by fraud in the past 12 months. 1% Global avo MOST COMMON TYPES OF 29% Theft of physical assets or stock 33% Misappropriation of company funds 25% 18% Information theft, loss, or attack (e.g., data theft), 17% 24% Vendor, supplier, or procurement fraud 17% 26% MOST COMMON 39% Junior employees 37% PERPETRATORS 33% 30% Senior or middle management employees 26% 33% Vendors/suppliers Agents and/or intermediaries 26% 27% Joint venture partners 26% 23% 19% Customers 26% MOST COMMON 79% 85% Assets (physical security systems, stock inventories, tagging, asset register) ANTI-FRAUD MEASURES 77% 83% Financial (financial controls, fraud detection, internal audit, external audit, anti-money laundering policies) have implemented the anti-fraud measure. 83% 82% Information (IT security, technical countermeasures) MOST COMMON MEANS OF 44% By a whistle-blower at our company 42% Percentage of respondents that 2% points above global average of 85% Cyber Security experienced a cyber incident in the past 12 months. Global avg 26% Email-based phishing attack 25% Insider theft of customer or employee data 21% 19% 23% Data breach resulting in loss of customer or employee data 19% 17% Data breach resulting in loss of IP/trade secrets/R&D 19% Denial of service attack 19% 14%

DISCOVERY

Fraud

FRAUD

PERPETRATORS

Security

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

Accidental placement of sensitive data that was indexed by a search engine (e.g., Google)

Freelance/temporary employees

Ex-employees

Joint venture partners

Customer records

Employee records

Physical assets/money

points above global average of 68% **11%**

14%

20% 6%

10%

51%

40% 38%

13%

13%

13% 13%

44%

40%

36%

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

Top responses given by survey respondents.

TECHNOLOGY, MEDIA, AND TELECOMS

	,		Top Toppended give		
	Percentage of respondents		=	equal to 2015	
Fraud	79	79 affected by fraud in the past 12 months.		points below gl average of 82%	obal Global av
MOST COMMON TYPES OF	Theft of physica	I assets or stock		35%	29%
FRAUD	Information thef	t, loss, or attack		30%	24%
	Management co	onflict of interest		25%	21%
MOST COMMON	Junior employee	es		42%	39%
PERPETRATORS	Senior or middle	e management employees		36%	30%
	Ex-employees			27%	27%
	Freelance/temp	orary employees		22%	27%
	Vendors/supplie	prs		22%	26%
	Regulators			22%	14%
MOST COMMON	Assets (physical s	security systems, stock inventories, tagging, asset register)		82%	79%
ANTI-FRAUD MEASURES Percentage of respondents who have	Financial (financia	al controls, internal/external audit, anti-money laundering policies)		79%	77%
implemented the anti-fraud measure.	Partners, clients	s, and vendors (due diligence)		79%	77%
	Risk (risk officer a	nd risk management system)		79%	78%
MOST COMMON MEANS OF DISCOVERY	Through an inter	rnal audit		40%	39%
Cyber Security	77	Percentage of respondents that experienced a cyber incident in the past 12 months.	♥ 8%	points below gl average of 85%	lobal Global a
MOST COMMON TYPES OF	Virus/worm infe	station		37%	33%
CYBER INCIDENT	Email-based phi	ishing attack		32%	26%
	Data deletion or	loss due to system issues		23%	24%
MOST COMMON PERPETRATORS	Freelance/temp	orary employees		23%	14%
MOST COMMON TARGET	Physical assets/	/money		48%	38%
	Trade secrets/R	&D/IP		43%	40%
	Company/emplo	byee identity		43%	36%
Security	72	Percentage of respondents that experienced a security incident in the past 12 months.	♠ 4%	points above g average of 68%	lobal 6 Global a
MOST COMMON TYPES OF	Theft or loss of I	P		46%	38%
SECURITY INCIDENTS	Environmental ri	isk		33%	27%
	Geographic and	l political risk		26%	22%
MOST COMMON PERPETRATORS	Freelance/temp	orary employees		27%	16%
RESPONDENTS COMPANIES	Workplace viole	nce		28%	27%
ARE MOST LIKELY TO FEEL HIGHLY VULNERABLE TO	Terrorism			21%	18%
THE FOLLOWING SECURITY RISKS	Environmental ri	isk		18%	20%

TRANSPORTATION, LEISURE, AND TOURISM

Fraud		ercentage of respondents affected y fraud in the past 12 months.	▲ 10%▲ 3%	points above 2015 points above gl average of 82%	
MOST COMMON TYPES OF	Theft of physical ass	sets or stock		33%	29%
FRAUD	Vendor, supplier, or	procurement fraud		30%	26%
	Regulatory or comp	liance breach		26%	21%
MOST COMMON	Junior employees			39%	39%
PERPETRATORS	Agents and/or intern	nediaries		35%	27%
	Freelance/temporary	y employees		30%	27%
	Senior or middle ma	anagement employees		26%	30%
	Joint venture partne	rs		22%	23%
MOST COMMON	Information (IT securit	ty, technical countermeasures)		89%	82%
ANTI-FRAUD MEASURES Percentage of respondents who have	Assets (physical secur	rity systems, stock inventories, tagging, asset register)		87%	79%
implemented the anti-fraud measure.	Board of director en	gagement in cyber security policies and proceduress		85%	75%
	Staff (background scre	eening)		85%	74%
	Risk (risk officer and ris	sk management system)		78%	78%
MOST COMMON MEANS OF DISCOVERY	By a whistle-blower	at our company		46%	44%
Cyber Security	87 ex	ercentage of respondents that xperienced a cyber incident the past 12 months.	1 2%	points above gl average of 85%	obal Global avg
MOST COMMON TYPES OF	Virus/worm infestation	ion		37%	33%
CYBER INCIDENT	Alteration or change	e of customer data		31%	16%
	Data deletion or loss	s due to system issues		30%	24%
MOST COMMON PERPETRATORS	Ex-employees			19%	20%
MOST COMMON TARGET	Customer records			51%	51%
	Physical assets/mor	ney		51%	38%
	Employee records			45%	40%
	Trade secrets/R&D/I	IP		45%	40%
Security	70 e>	ercentage of respondents that xperienced a security incident in ne past 12 months.	♠ 2%	points above gl average of 68%	Global avg
MOST COMMON TYPES OF	Theft or loss of IP			43%	38%
SECURITY INCIDENTS	Workplace violence			30%	23%
	Environmental risk			26%	27%
MOST COMMON	Permanent employe	ees of our own company		24%	17%
PERPETRATORS	Ex-employees			24%	23%
RESPONDENTS ARE MOST	Workplace violence			41%	27%
LIKELY TO FEEL HIGHLY VULNERABLE TO THE	Environmental risk			35%	20%
FOLLOWING SECURITY RISKS	Theft or loss of IP			31%	19%