Security Incidents taxonomy Quick Reference Card (v0.1.0)

For ETSI and Club R2GS, designed and edited by Christophe Blad (Oppida) and Gérard Gaudin (G²C).

This Quick Reference Card summarizes the taxonomy of security incidents. Data are extracted from the ETSI GS ISI-002 V1.1.1 standard.

ATTRIBUTES	CATEGORIES	SUB-CATEGORIES
Origin ("Who and/or Why?")	Accident	Natural disaster
		Physical failure
		IS environment component unavailability
		Software malfunction: development, implementation
		Abnormal activity
	Unwitting or unintentional act (error)	Internal (employee)
		Internal (on-premises or off-premises service provider)
	Unawareness or carelessness or irresponsibility	Internal (employee)
		Internal (on-premises or off-premises service provider)
	Malicious act	External agent
		Internal (employee)
		Internal (business partner)
		Internal (on-premises or off-premises service provider)
Action ("What?")	Unauthorized access to a system and/or to information	Use of authorized user's identity (identity usurpation or user impersonation)
		Access to a network or a central system or an application via a pre-established foothold
		Technical intrusion on a network or a system or an application
		Intrusion on a central system or an application via a stolen (or lost) and ill-protected workstation having access to organisation's internal network through a VPN connection
		Usurpation of rights
		Other
	Unauthorized action on the information system and/or against the organisation	Website defacement
		Misappropriation of organization on-line resources i.e. connectivity, bandwidth or storage
		On a system or on a gateway towards a professional network destroying or disturbing action
		Obvious use of organisation's communication means for another use than the one paid for by the organisation (or excessive non-business use)
		Access from a professional workstation to an external online service that is possibly harmful to one's organisation (mainly loss of productivity or heavier overhead or further malicious activity enabled):
		Organisation's storage capacity use abuse (useless consumption of computer resources)
		Storage of inappropriate content in a PC
		By phone or by e-mail (not encrypted) sensitive data communication
		On a public Web site personal data entry
		Shutdown of log production and/or storage on a system or on an application
		Internal fraudulent action for personal enrichment or benefit: through computer or not (embezzlement)
		Internal fraudulent action for one's organization enrichment or benefit: through computer or not
		External fraudulent action on a VoIP or not voice system
		Groundless transaction modification or repudiation: concerns business partners (customers, distributors and suppliers)
		Transaction replay
		Communication or message or file decryption
		Access key illicit robbery for use on a system secured by cryptographic techniques
		Company member abilities abuse
		Miscommunication or misinformation: transmission of false information to a user by another one
		Other
	Installation of unauthorized software programs on a system (without the owner's consent)	Virus and worm. C&C (Command and Control) channel are not used
		Trojan horse and keylogger. C&C (Command and Control) channel are used and necessary
		Bot. C&C (Command and Control) channel are used and necessary
		Scareware. C&C (Command and Control) channel are used and necessary
		Spyware and adware. C&C (Command and Control) channel may be used
		Other
	Information system remote disturbance	Denial of service (DoS or DDoS)
		Disturbance of messaging system regular operations
		Other
	Social engineering attacks	Usurpation of organisation's acquaintance's identity to deceit a user and let him carry out a dangerous action to his organisation
		Baiting
		Blackmail or actions meant to scare
		Elicitation (subtle extraction of information through conversation)
		Hoax/scam
		Other
	Personal attack on organization's personnel or organization disturbance	Personal attack on organization's personnel
		Personal harassment
		Organization disturbance
	Physical intrusion or illicit action	Access to data of lost or stolen laptop, workstation, mobile device or removable storage device
		Collection of unattended documents
		Physical intrusion resulting in theft of information or equipment
		Physical intrusion resulting in information modification
		Physical intrusion resulting in information or equipment damages
		Intrusion in a piece of equipment installed in a public place
		Eavesdropping of radio waves
	Illicit activity carried out on the public Internet network (harming an organization)	Cybersquatting or domain forgery
		Pharming
		Counterfeiting or forgery of Web sites and/or services
		Phishing (targeting organization's general public customers' computers)

		Spreading false or secret information about an organization through unmoderated social networking
		Access to protected data over P2P networks
		Other
	Various errors (administration, handling, programming, general use)	Accidental removal or destruction of equipment or sensitive data
		Accidental modification of sensitive data
		Accidental leakage of protected data
		Programming error leading to system malfunction
		Configuration error leading to system malfunction
		Other
	Breakdown or malfunction	Physical failure
		Unavailability due to environmental failure
		Abnormal activity
	Environmental events (due to a natural disaster)	Water discharge
		Fire
		Temperature effects
		By a spoiling gas infection
		Other violent disasters

Technique ("How?")	**Unauthorized access to a system and/or to information**	Authentication attacks
		Use of a backdoor that has been installed during the software development stage or in production
		Various methods
		Technical methods for the 1st two kinds of events
		Other
	Unauthorized action on the information system and/or against the organization	Illicit partial or full modification of Web homepages content
		Partial misappropriation of organization's resources
		Dangerous commands sent to the application or underlying OS
		Concerns especially passwords or credentials
		Concerns especially phishing sites
		Log production and/or retention stopping via specific commands for one of the 2 following reasons: system or application performances improvement at security expense, concealment of an intrusion and/or of unauthorised actions via lack of traces
		Various methods for various security events
		Means for either events (external attackers) are first intrusions and then specific PABX commands sent to put incoming attacker-generated traffic through to end destinations or to create artificial traffic to fee-based attacker-owned voice servers
		Repudiation by a customer of a signed or not electronic order (fax,...) or modification of a previous not signed electronic order
		Replay attack
		2 methods: with a stolen key, without a key through algorithm breaking
		Employee's usage, with full knowledge of the facts, of the goods, credit, powers, name, brands or voices of his/her company, for direct or indirect personal purposes
		Company employee's misappropriation, at the expense of a third party, of funds, securities or assets provided to him/her and that s/he had accepted, in exchange for an agreement to return them, to represent them or to make a specific usage of them
		Situation triggered often by fear of telling a undesirable truth
		Other
	Installation of unauthorized software programs (malware) on a system (without the owner's consent)	Initial installation
		Spreading
		Similar initially to adware, with downloading of a malware
		Easier installation (generally without human interaction) than a malware
		Various methods similar to those above
	Information system remote disturbance	DoS methods
		DDoS methods
		Spam
		Sending of very oversized messages or attached pieces
	Social engineering attacks	Spear phishing or whaling
		Ransomware: technical (or not technical) means include
		Scareware
		Hoax
		Scam
	Personal attack on organization's personnel or organization disturbance	Abuse of one's situation to get any advantage by easiness or by greed
		Excessive (impossible to be met) requirements leading to organisation disturbance
	Physical intrusion or illicit action	Documents easy to rob by insiders on messy desks
		Physical intrusion into organisation's premises by unknown persons often achieved through some techniques of visitors welcome hostesses deceitfulness
		Concerns notably for information theft Pay at the Pump terminals, Automated Teller Machines (ATM), Point-of-Sale (POS) terminals, etc. via installation of hidden magnetic cards ID number and PIN reader devices
		Physical proximity and electromagnetic signals pick-up device required
	Illicit activity carried out on the public Internet network (harming an organisation)	Registration of a domain name corresponding with a name or brand to which no legitimate rights are held, for the sole purpose of preventing the name from later being assigned to its natural holder
		Attack on public DNS
		Total or partial duplication of a Website through systematic copying of its pages (mirroring)
		(Unwitting or malicious and motivated search using keywords targeted towards confidential or personal information) access and leak made possible through an accidental openness and/or sharing of resources on a user workstation P2P client
	Various errors (administration, handling, programming, general use)	Some similar situations of easy to make mistakes with sometimes serious consequences (to be recognised by everybody through user awareness and to be mitigated or avoided by some policies and procedures)
	Breakdown or malfunction	
	Environmental events (unavailability caused by a natural disaster)	All causes taken into account (accidental only)
		Overheated room due to an increase of the outdoor temperature (sun behind the glass...), local overheating due to amplified sun (effect of amplification glass power)
		All other natural and natural causes

Status	**Security event attempt (or occurrence) underway**	Preparation
		Underway
	Succeeded (or performed) security event	Target reached with real CIA consequences
	Failed security event	Event stopped before target hitting
		Event thwarted by existing measures before target hitting

Exploited vulnerability	**Behavioural vulnerability**	Illicit or dangerous protocols used
		Internet illicitly accessed
		Files illicitly transferred between the organization and the outside world
		Workstation used without complying the required security tools, configurations and rules
		Password illicitly handled or managed
		Authentication illicitly handled or managed
		Access rights illicitly granted
		Central systems or applications irrelevantly handled
	Software vulnerability	No classification is proposed for this category (see CWE)
	Configuration vulnerability	No classification is proposed for this category (see CCE)
	General security (organizational) vulnerability	Security organization
		Governance
		Development and testing
		Security operations
		Incident detection and management process
		Vulnerability or weakness detection and management process
		Auditing process
		Miscellaneous
	Conception vulnerability	Software
		General design
		Environment
	Material vulnerability	Hardware
		Network and systems
		Personnel and site
		Environment

Target (“On what kind of asset?”)	**Data bases and applications**	Perimeter
		Internal
		Public cloud
		Outsourcing (remotely)
	Systems	Perimeter
		Internal
		Public cloud
		Outsourcing (remotely)
	Networks and telecommunications	Low level devices
		High level communication
		Middleware
		Wireless devices
		Security
	Offline storage devices	Paper
		Electronic devices
		Magnetic devices
		Optical devices
	End-user devices	Local application software
		Multipurpose workstations
		Dedicated devices
	People	Employee
		Business partner
		On-premises or off-premises service provider
	Facilities and environment	Real estate
		Physical security devices or systems
		Various utilities
		Office furniture

CIA consequence	**Loss of confidentiality**	Personal identifiable information
		Professional secrecy
		Sensitive data (strategic plans, detailed internal financial reports, etc.)
		Intellectual property
		Defence classified
		Network and systems
		Security
	Loss of integrity	The different possible cases are too diversified to give a complete list. They range from financial fraud to Web defacement to accidental technical modification.
	Loss of availability	Performance decrease
		Full breakdown or malfunction (interruption without destruction or deletion)
		Deletion
		Physical destruction
		Physical loss or theft

Business impact	**Direct impact**	Disruption to business operations
		Loss of productivity
		Fraud
		Incident recovery costs
		Life or health consequences
	Indirect impact	Loss of competitive advantage
		Reputation damage
		Loss of market share
		Legal and regulatory costs