Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

1 Access Control

1.1 Definition[edit]

Access Control. Means to ensure that access to assets is authorised and restricted based on business and security requirements.

1.2 Reference[edit]

- ISO/IEC 27000:2018

2 Accountability

2.1 Definition[edit]

Accountability. Property that ensures that the actions of an entity may be traced uniquely to that entity.

In the GDPR context the principle of accountability intends to ensure that controllers are more generally in control and in the position to ensure and demonstrate compliance with Data Protection principles in practice.

Accountability requires that controllers put in place internal mechanisms and control systems that ensure compliance and provide evidence (such as audit reports) to demonstrate compliance to external stakeholders, including supervisory authorities.

2.2 Reference[edit]

- ISO/IEC 2382:2015
- EDPS Glossary

3 Advanced Persistent Threat

3.1 Definition[edit]

Advanced Persistent Threat (APT) is a Threat Actor that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple threat vectors.

The advanced persistent threat:

- pursues its objectives repeatedly over an extended period of time;
- adapts to defenders? efforts to resist it; and
- is determined to execute its objectives.

3.2 Reference[edit]

- Adapted from NIST

4 Asset

4.1 Definition[edit]

Asset is a very broad term that means a resource of monetary or other value (Economic Resource) that is owned by an entity and/or provides benefit to some party.

An asset is something of either tangible or intangible value that is worth protecting, including people, information, infrastructure, finances and reputation. It may be a durable object, which produces a flow of goods and/or services over time (Productive Asset).

- Anything controlled by an organization as a result of past actions that the organization signifies as important or valuable.
- Specifically, a recognized asset is an entry in an entity's Balance Sheet statement.

4.2 Reference[edit]

- ISACA Fundamentals
- IFRS Framework

4.3 Disclaimer[edit]

5 Attack Vector

5.1 Definition[edit]

Attack Vector in the context of IT Risk / Cyber Risk denotes the fully specified sequence of operations that may enable unauthorized access and use of digital systems.

The set of all attack vectors in denoted the Attack Surface.

5.2 Categories[edit]

- Web Applications (HTTP)
- Other Network protocols
- Database Servers

5.3 See Also[edit]

- Wikipedia on Attack Surface

---

6 Authentication

6.1 Definition[edit]

Authentication. It is the verification of the identity of a user by a system or service. It may also denote methods used to verify the origin of a message or to verify the identity of a participant connected to a system and to confirm that a message has not been modified or replaced in transit.

7 Authenticity

7.1 Definition[edit]

Authenticity. Property that an entity is what it claims to be.

7.2 Reference[edit]

- ISO/IEC 27000:2018

8 Availability

8.1 Definition[edit]

Availability. Property of being accessible and usable on demand by an authorised entity. It is a metric which measures the percentage, normally computed over a periodical basis (such as a month) and net of planned or unplanned service downtimes of service coverage.

8.2 Examples[edit]

- In procurement finance, it is the amount of money that is available for drawing to the assignor. This would be the value of all approved receivables multiplied by the pre-agreed prepayment percentage less any amounts already paid to the assignor.
- In the context of Business Continuity it is indicating the presence of staff or organizational resources (buildings, applications) etc. in support of business functions

8.3 Reference[edit]

- ISO/IEC 27000:2018

9 Campaign

9.1 Definition[edit]

Campaign. A grouping of coordinated adversarial behaviours that describes a set of malicious activities that occur over a period of time against one or more specific targets.

9.2 Reference[edit]

- Adapted from STIX

10 Compromise

10.1 Definition[edit]

Compromise. Violation of the security of an Information System, leading to a collection of compromised assets

10.2 Reference[edit]

- Adapted from ISO 21188:2018

11 Compromised Asset

11.1 Definition[edit]

Compromised Asset is any information asset that were compromised during a Cyber Incident.

?Compromised? refers to any loss of confidentiality/possession, integrity/authenticity, availability/utility (primary security attributes). Naturally, an incident can involve multiple assets and affect multiple attributes of those assets.

11.2 References[edit]

- VERIS

12 Confidentiality

12.1 Definition[edit]

Confidentiality. Property that information is neither made available nor disclosed to unauthorised individuals, entities, processes or systems. In a general sense refers to the duty not to share information with persons who are not qualified to receive that information (see Article 5(f) of Regulation (EU) 2016/679 and Article 4(f) of Regulation (EU) 2018/1725).

In a more specific sense, it refers to the confidentiality of communications provided for in Article 5 of the E-privacy Directive 2009/136/EC and in Article 36 of Regulation (EU) 2018/1725.

12.2 References[edit]

- EDPS Glossary
- Adapted from ISO/IEC 27000:2018

13 Course of Action

13.1 Definition[edit]

Course of Action. (CoA) An action or actions taken to either prevent or respond to a cyber incident. It may describe technical, automatable responses but can also describe other actions such as employee training or policy changes.

13.2 Reference[edit]

- Adapted from STIX

14 Cyber

14.1 Definition[edit]

Cyber. Relating to, within, or through the medium of the interconnected information infrastructure of interactions among persons, processes, data, and information systems.

14.2 Reference[edit]

- Adapted from CPMI-IOSCO (citing NICCS)

15 Cyber Advisory

15.1 Definition[edit]

Cyber Advisory. Notification of new trends or developments regarding a cyber threat to, or vulnerability of, information systems. This notification may include analytical insights into trends, intentions, technologies or tactics used to target information systems.

15.2 Reference[edit]

- Adapted from NIST

16 Cyber Alert

16.1 Definition[edit]

Cyber Alert. Notification that a specific cyber incident has occurred or a cyber threat has been directed at an organisation?s information systems.

16.2 Reference[edit]

- Adapted from NIST

17 Cyber Attack

17.1 Contents

17.2 Definition[edit]

A Cyber Attack is a specific form of Cyber Risk/IT Security Risk that involves an attack to an organizations digital asses by an external agent

17.2.1 Cyber Attack Purpose[edit]

Attacks performed from the internet or outside networks for different purposes

- fraud
- espionage
- activism / sabotage
- cyber terrorism

17.2.2 Cyber Attack Techniques[edit]

- social engineering
- intrusion attempts through the exploitation of vulnerabilities
- deployment of malicious software resulting in taking control of internal IT systems

17.3 Other Types of Cyber Attack[edit]

- Execution of fraudulent payment transactions by hackers through the breaking or circumvention of the security of e-banking and payment services and/or by attacking and exploiting security vulnerabilities in the internal payment systems of the institution.
- Execution of fraudulent securities transactions by hackers through the breaking or circumvention of the security of the e-banking services that also provide access to the customer?s securities accounts.
- Attacks on communication connections and conversations of all kinds or IT systems with the objective of collecting information and/or committing frauds.

17.4 Examples[edit]

NB: The detailed examples are drawn from financial industry specifics

- APT (Advanced Persistent Threat) for taking control of internal systems or stealing information (e.g. identity theft related information, credit card information).
- Malicious software (e.g. ransomware) that encrypts data with the aim of blackmail.
- Infection of internal IT systems with Trojan horses for committing malicious system actions in a hidden manner.
- Exploitation of IT system and/or (web) application vulnerabilities (e.g. SQL injection ...) to gain access to the internal IT system.
- Attacks against e-banking or payment services, with objective to commit unauthorised transactions.
- The creation and sending out of fraudulent payment transactions from within the internal payment systems of the institution (e.g. fraudulent SWIFT messages).
- Pump and dump attacks where the attackers gain access to e-banking securities accounts of customers and place fraudulent buying or selling orders to influence the market price and /or make gains based on previously established securities positions.
- Eavesdropping/intercepting unprotected transmission of authentication data in plain-text.

18 Cyber Event

18.1 Definition[edit]

Cyber Event. Any observable occurrence (Risk Event) in an information system. Cyber events sometimes provide indication that a Cyber Incident is occurring.

18.2 Reference[edit]

- Adapted from NIST (definition of ?Event?)

19 Cyber Incident

19.1 Definition[edit]

Cyber Incident. A Cyber Event that:

- jeopardizes the cyber security of an information system or the information the system processes, stores or transmits or
- violates the security policies, security procedures or acceptable use policies, whether resulting from malicious activity or not.

19.2 References[edit]

- Adapted from NIST (definition of ?Incident?)

20 Cyber Incident Response Plan

20.1 Definition[edit]

Cyber Incident Response Plan. The documentation of a predetermined set of instructions or procedures to respond to and limit consequences of a cyber incident.

20.2 Reference[edit]

- Adapted from NIST (definition of ?Incident Response Plan?) and NICCS

21 Cyber Resilience

21.1 Definition[edit]

Cyber Resilience. The ability of an organisation to continue to carry out its mission by anticipating and adapting to cyber threats and other relevant changes in the environment and by withstanding, containing and rapidly recovering from cyber incidents.

21.2 Reference[edit]

- Adapted from CERT Glossary (definition of ?Operational resilience?), CPMI-IOSCO and NIST (definition of ?Resilience?)

22 Cyber Risk

22.1 Definition[edit]

Cyber Risk is an informal name for IT Security Risk

22.2 Reference[edit]

- Adapted from CPMI-IOSCO, ISACA Fundamentals (definition of ?Risk?) and ISACA Full Glossary (definition of ?Risk?)

23 Cyber Risk Glossary

23.1 Definition[edit]

A Glossary for Cyber Risk terms based on[1]

Term	Definition
Access Control	Means to ensure that access to assets is authorised and restricted based on business and security requirements.
Accountability	Property that ensures that the actions of an entity may be traced uniquely to that entity.
Advanced Persistent Threat	(APT) A threat actor that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple threat vectors. The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders? efforts to resist it; and (iii) is determined to execute its objectives.
Asset	Something of either tangible or intangible value that is worth protecting, including people, information, infrastructure, finances and reputation.
Authenticity	Property that an entity is what it claims to be.
Availability	Property of being accessible and usable on demand by an authorised entity.
Campaign	A grouping of coordinated adversarial behaviours that describes a set of malicious activities that occur over a period of time against one or more specific targets.
Compromise	Violation of the security of an information system.
Confidentiality	Property that information is neither made available nor disclosed to unauthorised individuals, entities, processes or systems.
Course of Action	(CoA) An action or actions taken to either prevent or respond to a cyber incident. It may describe technical, automatable responses but can also describe other actions such as employee training or policy changes.
Cyber	Relating to, within, or through the medium of the interconnected information infrastructure of interactions among persons, processes, data, and information systems.
Cyber Advisory	Notification of new trends or developments regarding a cyber threat to, or vulnerability of, information systems. This notification may include analytical insights into trends, intentions, technologies or tactics used to target information systems.
Cyber Alert	Notification that a specific cyber incident has occurred or a cyber threat has been directed at an organisation?s information systems.
Cyber Event	Any observable occurrence in an information system. Cyber events sometimes provide indication that a cyber incident is occurring.
Cyber Incident	A cyber event that: i. jeopardizes the cyber security of an information system or the information the system processes, stores or transmits; or ii. violates the security policies, security procedures or acceptable use policies, whether resulting from malicious activity or not.
Cyber Incident Response Plan	The documentation of a predetermined set of instructions or procedures to respond to and limit consequences of a cyber incident.
Cyber Resilience	The ability of an organisation to continue to carry out its mission by anticipating and adapting to cyber threats and other relevant changes in the environment and by withstanding, containing and rapidly recovering from cyber incidents.
Cyber Risk	The combination of the probability of cyber incidents occurring and their impact.
Cyber Security	Preservation of confidentiality, integrity and availability of information and/or information systems through the cyber medium. In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved.
Cyber Threat	A circumstance with the potential to exploit one or more vulnerabilities that adversely affects cyber security.
Data Breach	Compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to data transmitted, stored or otherwise processed.
Defence-in-Depth	Security strategy integrating people, processes and technology to establish a variety of barriers across multiple layers and dimensions of the organisation.
Denial of Service	(DoS) Prevention of authorised access to information or information systems; or the delaying of information system operations and functions, with resultant loss of availability to authorised users.
Detect Function	Develop and implement the appropriate activities to identify the occurrence of a cyber event.
Distributed Denial of Service	(DDoS) A denial of service that is carried out using numerous sources simultaneously.

Term	Definition
Exploit	Defined way to breach the security of information systems through vulnerability.
Identify Function	Develop the organisational understanding to manage cyber risk to assets and capabilities.
Identity and Access Management	(IAM) Encapsulates people, processes and technology to identify and manage the data used in an information system to authenticate users and grant or deny access rights to data and system resources.
Incident Response Team	(IRT) [also known as CERT or CSIRT] Team of appropriately skilled and trusted members of the organisation that handles incidents during their life cycle.
Indicators of Compromise	(IoCs) Identifying signs that a cyber incident may have occurred or may be currently occurring.
Information Sharing	An exchange of data, information and/or knowledge that can be used to manage risks or respond to events.
Information System	Set of applications, services, information technology assets or other information-handling components, which includes the operating environment.
Integrity	Property of accuracy and completeness.
Malware	Software designed with malicious intent containing features or capabilities that can potentially cause harm directly or indirectly to entities or their information systems.
Multi-Factor Authentication	The use of two or more of the following factors to verify a user?s identity: -- knowledge factor, ?something an individual knows?; -- possession factor, ?something an individual has?; -- biometric factor, ?something that is a biological and behavioural characteristic of an individual?.
Non-Repudiation	Ability to prove the occurrence of a claimed event or action and its originating entities.
Patch Management	The systematic notification, identification, deployment, installation and verification of operating system and application software code revisions. These revisions are known as patches, hot fixes and service packs.
Penetration Testing	A test methodology in which assessors, using all available documentation (e.g. system design, source code, manuals) and working under specific constraints, attempt to circumvent the security features of an information system.
Protect Function	Develop and implement the appropriate safeguards to ensure delivery of services and to limit or contain the impact of cyber incidents.
Recover Function	Develop and implement the appropriate activities to maintain plans for cyber resilience and to restore any capabilities or services that were impaired due to a cyber incident.
Reliability	Property of consistent intended behaviour and results.
Respond Function	Develop and implement the appropriate activities to take action regarding a detected cyber event.
Situational Awareness	The ability to identify, process and comprehend the critical elements of information through a cyber threat intelligence process that provides a level of understanding that is relevant to act upon to mitigate the impact of a potentially harmful event.
Social Engineering	A general term for trying to deceive people into revealing information or performing certain actions.
Tactics, Techniques and Procedures	(TTPs) The behaviour of a threat actor. A tactic is the highest-level description of this behaviour, while techniques give a more detailed description of behaviour in the context of a tactic, and procedures an even lower-level, highly detailed description in the context of a technique.
Threat Actor	An individual, a group or an organisation believed to be operating with malicious intent.
Threat Assessment	Process of formally evaluating the degree of threat to an organisation and describing the nature of the threat.
Threat Intelligence	Threat information that has been aggregated, transformed, analysed, interpreted or enriched to provide the necessary context for decision-making processes.
Threat-Led Penetration Testing	(TLPT) [also known as Red Team Testing] A controlled attempt to compromise the cyber resilience of an entity by simulating the tactics, techniques and procedures of real-life threat actors. It is based on targeted threat intelligence and focuses on an entity?s people, processes and technology, with minimal foreknowledge and impact on operations.
Threat Vector	A path or route used by the threat actor to gain access to the target.
Traffic Light Protocol	(TLP) A set of designations used to ensure that information is shared only with the appropriate audience. It employs a pre-established colour code to indicate expected sharing boundaries to be applied by the recipient.
Verification	Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled.
Vulnerability	A weakness, susceptibility or flaw of an asset or control that can be exploited by one or more threats.
Vulnerability Assessment	Systematic examination of an information system, and its controls and processes, to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures and confirm the adequacy of such measures after implementation.

23.2 References[edit]

1. ? ESB, Cyber Lexicon, 2018

24 Cyber Run

24.1 Definition[edit]

A **Cyber Run** is a specific Bank Run scenario in which a significant cyber attack on a bank?s deposits, whether by theft, data corruption, or denial of access, may lead wholesale depositors in the same and other large banks to withdraw their funds rapidly enough to threaten the liquidity of these institutions or the effectiveness of the payment system.[1]

24.2 See Also[edit]

- Systemic Cyber Risk

24.3 References[edit]

1. ? Duffie, D. and Younger, J. (2019), ?Cyber runs: How a cyber attack could affect U.S. financial institutions?.

25 Cyber Security

25.1 Definition[edit]

Cyber Security. Preservation of confidentiality, integrity and availability of information and/or information systems through the cyber medium. In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved.

25.2 Reference[edit]

- Adapted from ISO/IEC 27032:2012

26 Cyber Threat

26.1 Definition[edit]

Cyber Threat. A circumstance with the potential to exploit one or more vulnerabilities that adversely affects Cyber Security.

26.2 Reference[edit]

- Adapted from CPMI-IOSCO

27 Data Breach

27.1 Definition[edit]

Data Breach. Compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to data transmitted, stored or otherwise processed.

27.2 See Also[edit]

- Security Breach

27.3 Reference[edit]

- Adapted from ISO/IEC 27040:2015

28 Data Breaches List

This is a frozen copy (January 2019) of the List of data breaches. It is included here with modifications to enable the automated processing of the data.

Entity	Year	Records	Organization type	Method	Sources
object	datetime64	int64	category	category	object
21st Century Oncology	2016	2,200,000	healthcare	hacked	[1][2]
Accendo Insurance Co.	2011	175,350	healthcare	poor security	[3][4]
Bedford/St. Martin's	2012-2014	unknown	retail	unknown	[5]
Australian Immigration Department	2015	G20 world leaders	government	accidentally published	[6]
Barnes & Noble	2012	63 stores	retail	hacked	[7][8]
Adobe Systems	2013	152,000,000	tech	hacked	[9][10]
Advocate Medical Group	2013	4,000,000	healthcare	lost / stolen media	[11][12]
AerServ (subsidiary of InMobi)	2018	75,000	advertising	hacked	[13]
Affinity Health Plan, Inc.	2009	344,579	healthcare	lost / stolen media	[14]
Ameritrade	2005	200,000	financial	lost / stolen media	[15]
Ancestry.com	2015	300,000	web	poor security	[16]
Ankle & Foot Center of Tampa Bay, Inc.	2010	156,000	healthcare	hacked	[17]
Anthem Inc.	2015	80,000,000	healthcare	hacked	[18][19]
AOL	2004	92,000,000	web	inside job, hacked	[20][21]
AOL	2006	20,000,000	web	accidentally published	[22]
AOL	2014	2,400,000	web	hacked	[23]
Apple, Inc./BlueToad	2012	12,367,232	tech, retail	accidentally published	[24]
Apple	2013	275,000	tech	hacked	[25]
Apple Health Medicaid	2016	91,000	healthcare	poor security	[26]
Ashley Madison	2015	32,000,000	web	hacked	[27]
AT&T	2008	113,000	telecoms	lost / stolen computer	[28]
AT&T	2010	114,000	telecoms	hacked	[29]
Auction.co.kr	2008	18,000,000	web	hacked	[30]
Automatic Data Processing	2005	125,000	financial	poor security	[31]
AvMed, Inc.	2009	1,220,000	healthcare	lost / stolen computer	[32]
Bailey's Inc.	2015	250,000	retail	hacked	[33]
The Bank of New York Mellon	2008	12,500,000	financial	lost / stolen media	[34]
Betfair	2010	2,300,000	web	hacked	[28]
Bethesda Game Studios	2011	200,000	gaming	hacked	[35]
Bethesda Game Studios	2018		gaming	accidentally published	[36]
BlankMediaGames	2018	7,633,234	gaming	hacked	[37][38]
Blizzard Entertainment	2012	14,000,000	gaming	hacked	[39][40]
BlueCross BlueShield of Tennessee	2009	1,023,209	healthcare	lost / stolen media	[41]
BMO and Simplii	2018	90,000	banking	poor security	[42]
British Airways	2018	380,000	transport	hacked	[43][44]
British Airways	2015	tens of thousands	retail	hacked	[45]

Entity	Year	Records	Organization type	Method	Sources
California Department of Child Support Services	2012	800,000	government	lost / stolen media	[28][46]
CardSystems Solutions Inc. (MasterCard, Visa, Discover Financial Services and American Express)	2005	40,000,000	financial	hacked	[47][48]
Cathay Pacific Airways	2018	9,400,000	transport	hacked	[49]
CareFirst BlueCross Blue Shield - Maryland	2015	1,100,000	healthcare	hacked	[50]
Central Coast Credit Union	2016	60,000	financial	hacked	[51]
Central Hudson Gas & Electric	2013	110,000	energy	hacked	[52]
CheckFree Corporation	2009	5,000,000	financial	hacked	[53]
China Software Developer Network	2011	6,000,000	web	hacked	[54]
Chinese gaming websites (three: Duowan, 7K7K, 178.com)	2011	10,000,000	web	hacked	[55]
Citigroup	2005	3,900,000	financial	lost / stolen media	[56]
Citigroup	2011	360,083	financial	hacked	[57]
Citigroup	2013	150,000	financial	poor security	[58]
City and Hackney Teaching Primary Care Trust	2007	160,000	healthcare	lost / stolen media	[59]
Colorado government	2010	105,470	healthcare	lost / stolen computer	[60]
Community Health Systems	2014	4,500,000	healthcare	hacked	[61]
Philippines Commission on Elections	2016	55,000,000	government	hacked	
Compass Bank	2007	1,000,000	financial	inside job	[28][62]
Bank of America	2005	1,200,000	financial	lost / stolen media	[63]
Countrywide Financial Corp	2006	2,600,000	financial	inside job	[28]
Countrywide Financial Corp	2011	2,500,000	financial	inside job	[64]
Centers for Medicare & Medicaid Services	2018	75,000	healthcare	hacked	[65]
Cox Communications	2016	40,000	telecoms	hacked	[66]
Crescent Health Inc., Walgreens	2013	100,000	healthcare	lost / stolen computer	[52][67]
CVS	2015	millions	retail	hacked	[68]
Dai Nippon Printing	2007	8,637,405	retail	inside job	[69]
Data Processors International (MasterCard, Visa, Discover Financial Services and American Express)	2008	8,000,000	financial	hacked	[70]
Defense Integrated Data Center (South Korea)	2017	235 GB	military	hacked	[71]
Deloitte	2017		consulting, accounting	poor security	[72]
Democratic National Committee	2016	19,252	political		[73]
US Department of Homeland Security	2016	30,000	government	poor security	[74][75]
Domino's Pizza (France)	2014	600,000	web	hacked	[76]
UK Driving Standards Agency	2007	3,000,000	government	lost / stolen media	[77]
Dropbox	2012	unknown	web	hacked	[78]
Drupal	2013	1,000,000	web	hacked	[79]
DSW Inc.	2005	1,400,000	retail	hacked	[80]
Dun & Bradstreet	2013	1,000,000	tech	hacked	[81][82]
eBay	2014	145,000,000	web	hacked	[83]
Educational Credit Management Corporation	2010	3,300,000	financial	lost / stolen media	[84]
Eisenhower Medical Center	2011	514,330	healthcare	lost / stolen computer	[85]
Embassy Cables	2010	251,000	government	inside job	[86]

Entity	Year	Records	Organization type	Method	Sources
Emergency Healthcare Physicians, Ltd.	2010	180,111	healthcare	lost / stolen media	[85][87]
Emory Healthcare	2012	315,000	healthcare	poor security	[85]
Erie County Medical Center	2017	unknown	healthcare	poor security	[88]
Equifax	2017	143,000,000	financial, credit reporting	poor security	[89][90]
European Central Bank	2014	unknown	financial	hacked	[91][92]
Evernote	2013	50,000,000	web	hacked	[93][94]
Excellus BlueCross BlueShield	2015	10,000,000	healthcare	hacked	[95]
Experian - T-Mobile US	2015	15,000,000	telecoms	hacked	[96][97]
EyeWire	2016	unknown	tech	lost / stolen computer	[98]
Facebook	2018	50,000,000	social network	poor security	[99][100][101][102][103][104]
Facebook	2013	6,000,000	web	accidentally published	[105]
Federal Reserve Bank of Cleveland	2010	400,000	financial	hacked	[28]
Fidelity National Information Services	2007	8,500,000	financial	inside job	[106]
Florida Department of Juvenile Justice	2013	100,000	government	lost / stolen computer	[52]
Friend Finder Networks	2016	412,214,295	web	poor security / hacked	[107][108]
Formspring	2012	420,000	web	accidentally published	[109]
Gamigo	2012	8,000,000	web	hacked	[110]
Gap Inc.	2007	800,000	retail	lost / stolen computer	[111]
Gawker	2010	1,500,000	web	hacked	[112][113]
Global Payments	2012	7,000,000	financial	hacked	[114]
Gmail	2014	5,000,000	web	hacked	[115]
Google Plus	2018	500,000	social network	poor security	[116][117][118]
Greek government	2012	9,000,000	government	hacked	[119]
Grozio Chirurgija	2017	25,000	healthcare	hacked	[120][121][122]
GS Caltex	2008	11,100,000	energy	inside job	[123][124]
Gyft	2016	unknown	web	hacked	[125][126]
Hannaford Brothers Supermarket Chain	2007	4,200,000	retail	hacked	[127]
Health Net	2009	500,000	healthcare	lost / stolen media	[128]
Health Net ? IBM	2011	1,900,000	healthcare	lost / stolen media	[129]
Heartland	2009	130,000,000	financial	hacked	[130][131]
Heathrow Airport	2017	2.5GB	transport	lost / stolen media	[132][133][134]
Hewlett Packard	2006	200,000	tech, retail	lost / stolen media	[135]
Hilton Hotels	2015	unknown	hotel	hacked	[136]
Home Depot	2014	56,000,000	retail	hacked	[137]
Honda Canada	2011	283,000	retail	poor security	[138]
Hyatt Hotels	2015	250 locations	hotel	hacked	[139][140]
Internal Revenue Service	2015	720,000	financial	hacked	[141][142]
Inuvik hospital	2016	6,700	healthcare	inside job	[143]
Iranian banks (three: Saderat, Eghtesad Novin, and Saman)	2012	3,000,000	financial	hacked	[144]
Jefferson County, West Virginia	2008	1,600,000	government		[28][145]

Entity	Year	Records	Organization type	Method	Sources
				accidentally published	
JP Morgan Chase	2010	2,600,000	financial	lost / stolen media	[146]
JP Morgan Chase	2014	76,000,000	financial	hacked	[147]
KDDI	2006	4,000,000	telecoms	hacked	[148]
Kirkwood Community College	2013	125,000	academic	hacked	[52][149]
KM.RU	2016	1,500,000	web	hacked	[150]
Korea Credit Bureau	2014	20,000,000	financial	inside job	[151]
Kroll Background America	2013	1,000,000	tech	hacked	[81][82]
KT Corporation	2012	8,700,000	telecoms	hacked	[152][153]
LexisNexis	2014	1,000,000	tech	hacked	[81][82]
Landry's, Inc.	2015	500 locations	restaurant	hacked	[154][155]
Lincoln Medical & Mental Health Center	2010	130,495	healthcare	lost / stolen media	[85][156]
LinkedIn, eHarmony, Last.fm	2012	8,000,000	web	accidentally published	[157][158]
Living Social	2013	50,000,000	web	hacked	[159][160]
MacRumors.com	2014	860,000	web	hacked	[161]
Mandarin Oriental Hotels	2014	10 locations	hotel	hacked	[162][163]
Marriott International	2018	500,000,000	hotel	hacked	[164][165]
Massachusetts Government	2011	210,000	government	poor security	[28]
Massive American business hack including 7-Eleven and Nasdaq	2012	160,000,000	financial	hacked	[166]
US Medicaid	2012	780,000	government, healthcare	hacked	[28]
Medical Informatics Engineering	2015	3,900,000	healthcare	hacked	[167]
Memorial Healthcare System	2011	102,153	healthcare	lost / stolen media	[168][85]
Michaels	2014	3,000,000	retail	hacked	[169]
Militarysingles.com	2012	163,792	web, military	accidentally published	[170]
Ministry of Education (Chile)	2008	6,000,000	government	accidentally published	[171][172]
Monster.com	2007	1,600,000	web	hacked	[173]
Morgan Stanley Smith Barney	2011	34,000	financial	lost / stolen media	[28]
Mozilla	2014	76,000	web	poor security	[174]
MyHeritage	2018	92,283,889	genealogy	unknown	[175]
NASDAQ	2014	unknown	financial	hacked	[176]
Natural Grocers	2015	93 stores	retail	hacked	[177]
Neiman Marcus	2014	1,100,000	retail	hacked	[178][179]
Nemours Foundation	2011	1,055,489	healthcare	lost / stolen media	[85][180]
Network Solutions	2009	573,000	tech	hacked	[181][182]
New York City Health & Hospitals Corp.	2010	1,700,000	healthcare	lost / stolen media	[85]
New York State Electric & Gas	2012	1,800,000	energy	inside job	[28]
New York Taxis	2014	52,000	transport	poor security	[183]
Nexon Korea Corp	2011	13,200,000	web	hacked	[184]
NHS	2011	8,300,000	healthcare	lost / stolen media	[185]
Nintendo	2013	240,000	gaming	hacked	[186]
Nival Networks	2016	1,500,000	gaming	hacked	[187]

Entity	Year	Records	Organization type	Method	Sources
Norwegian Tax Administration	2008	3,950,000	government	accidentally published	[188]
Ofcom	2016	unknown	telecom	inside job	[189]
US Office of Personnel Management	2015	21,500,000	government	hacked	[190][191]
Office of the Texas Attorney General	2012	6,500,000	government	accidentally published	[192]
Ohio State University	2010	760,000	academic	hacked	[28]
Orbitz	2018	880,000	web	hacked	[193]
Oregon Department of Transportation	2011	unknown	government	poor security	[28]
OVH	2013	undisclosed	web	hacked	[194]
Patreon	2015	2.3 million	web	hacked	[195]
Popsugar	2018	123,857	fashion	hacked	[196]
Premera	2015	11,000,000	healthcare	hacked	[197]
Puerto Rico Department of Health	2010	515,000	healthcare	hacked	[85]
Quora	2018	100,000,000	Question & Answer	hacked	[198]
Rambler.ru	2012	98,167,935	web	hacked	[199][200]
RBS Worldpay	2008	1,500,000	financial	hacked	[201]
Reddit	2018	unknown	web	hacked	[202][203]
Restaurant Depot	2011	200,000	retail	hacked	[28]
RockYou!	2009	32,000,000	web, gaming	hacked	[204]
Rosen Hotels	2016	unknown	hotel	hacked	[205]
San Francisco Public Utilities Commission	2011	180,000	government	hacked	[206]
Scottrade	2015	4,600,000	financial	hacked	[207]
Scribd	2013	500,000	web	hacked	[208][209]
Seacoast Radiology, PA	2010	231,400	healthcare	hacked	[85][210]
Sega	2011	1,290,755	gaming	hacked	[211]
Service Personnel and Veterans Agency (UK)	2008	50,500	government	lost / stolen media	[212]
SingHealth	2018	1,500,000	government, database	hacked	[213]
Slack	2015	500,000	tech	poor security	[214]
SnapChat	2013	4,700,000	web, tech	hacked	[215]
Sony Online Entertainment	2011	24,600,000	gaming	hacked	[216][217]
Sony Pictures	2011	1,000,000	web	hacked	[218]
Sony Pictures	2014	100 terabytes	media	hacked	[219]
Sony PlayStation Network	2011	77,000,000	gaming	hacked	[220]
South Africa police	2013	16,000	government	hacked	[221]
South Carolina Government	2012	6,400,000	healthcare	inside job	[85][222]
South Shore Hospital, Massachusetts	2010	800,000	healthcare	lost / stolen media	[28]
Southern California Medical-Legal Consultants	2011	300,000	healthcare	hacked	[28]
Spartanburg Regional Healthcare System	2011	400,000	healthcare	lost / stolen computer	[85][223]
Stanford University	2008	72,000	academic	lost / stolen computer	[28][224]
Starbucks	2008	97,000	retail	lost / stolen computer	[28]
Starwood Hotels including Westin Hotels and Sheraton Hotels	2015	54 locations	hotel	hacked	[225][226]
State of Texas	2011	3,500,000	government		[227]

Entity	Year	Records	Organization type	Method	Sources
				accidentally published	
Steam	2011	35,000,000	web	hacked	[228]
Stratfor	2011	935,000	military	accidentally published	[229]
Supervalu	2014	200 stores	retail	hacked	[230]
Sutter Medical Center	2011	4,243,434	healthcare	lost / stolen computer	[85][231]
Syrian government (Syria Files)	2012	2,434,899	government	hacked	[232][233]
Taobao	2016	20,000,000	retail	hacked	[234]
Taringa!	2017	28,722,877	web	hacked	[235]
Target Corporation	2014	70,000,000	retail	hacked	[236][237]
TaxSlayer.com	2016	unknown	web	hacked	[238]
TD Ameritrade	2007	6,300,000	financial	hacked	[239]
TD Bank	2012	260,000	financial	hacked	[240][241]
TerraCom & YourTel	2013	170,000	telecoms	accidentally published	[242][243]
Texas Lottery	2007	89,000	government	inside job	[28]
Ticketfly (subsidiary of Eventbrite)	2018	26,151,608	ticket distribution	hacked	[244]
Tianya Club	2011	28,000,000	web	hacked	[245]
TK / TJ Maxx	2007	94,000,000	retail	hacked	[246][247]
T-Mobile, Deutsche Telecom	2006	17,000,000	telecoms	lost / stolen media	[248][249]
Tricare	2011	4,901,432	military, healthcare	lost / stolen computer	[28]
Triple-S Salud, Inc.	2010	398,000	healthcare	lost / stolen media	[85]
Trump Hotels	2014	8 locations	hotel	hacked	[250][251]
Tumblr	2013	65,469,298	web	hacked	[252]
Twitch.tv	2015	unknown	tech	hacked	[253]
Twitter	2013	250,000	web	hacked	[254]
Typeform	2018	unknown	tech	poor security	[49]
Uber	2014	50,000	tech	poor security	[255]
Uber	2017	57,000,000	transport	hacked	[256]
Ubisoft	2013	unknown	gaming	hacked	[257]
Ubuntu	2013	2,000,000	tech	hacked	[258]
UCLA Medical Center, Santa Monica	2015	4,500,000	healthcare	hacked	[259]
UK Home Office	2008	84,000	government	lost / stolen media	[260]
UK Ministry of Defence	2008	1,700,000	government	lost / stolen media	[261]
UK Revenue & Customs	2007	25,000,000	government	lost / stolen media	[262]
Under Armour	2018	150,000,000	Consumer Goods	hacked	[263]
University of California, Berkeley	2009	160,000	academic	hacked	[264]
University of California, Berkeley	2016	80,000	academic	hacked	[265]
University of Maryland, College Park	2014	300,000	academic	hacked	[266]
University of Central Florida	2016	63,000	academic	hacked	[267]
University of Miami	2008	2,100,000	academic	lost / stolen computer	[28]
University of Utah Hospital & Clinics	2008	2,200,000	academic	lost / stolen media	[28]
University of Wisconsin?Milwaukee	2011	73,000	academic	hacked	[28]

Entity	Year	Records	Organization type	Method	Sources
UPS	2014	51 locations	retail	hacked	[268]
U.S. Army	2011	50,000	military	accidentally published	[28]
U.S. Army (classified Iraq War documents)	2010	392,000	government	inside job	[269]
U.S. Department of Defense	2009	72,000	military	lost / stolen media	[28]
U.S. Department of Veteran Affairs	2006	26,500,000	government, military	lost / stolen computer	[270]
U.S. law enforcement (70 different agencies)	2011	123,461	government	accidentally published	[271]
National Archives and Records Administration (U.S. military veterans' records)	2009	76,000,000	military	lost / stolen media	[272]
U.S. government (United States diplomatic cables leak)	2010	260,000	military	inside job	[273]
National Guard of the United States	2009	131,000	military	lost / stolen computer	[28]
Verizon Communications	2016	1,500,000	telecoms	hacked	[274]
Virginia Department of Health	2009	8,257,378	government, healthcare	hacked	[28]
Virginia Prescription Monitoring Program	2009	531,400	healthcare	hacked	[28]
Vodafone	2013	2,000,000	telecoms	inside job	[275]
VTech	2015	5,000,000	retail	hacked	[276]
Walmart	2015	millions	retail	hacked	[68]
Washington Post	2011	1,270,000	media	hacked	[277]
Washington State court system	2013	160,000	government	hacked	[278][279]
Weebly	2016	43,430,316	web	hacked	[280][281][282]
Wendy's	2015	unknown	restaurant	hacked	[283][284]
Wordpress	2018			hacked	[285]
Writerspace.com	2011	62,000	web	hacked	[286]
Xat.com	2015	6,054,459	web	social engineering	[287]
Yahoo	2013	3,000,000,000	web	hacked	[288][289]
Yahoo	2014	500,000,000	web	hacked	[290][291][292][293][294]
Yahoo Japan	2013	22,000,000	tech, web	hacked	[295]
Yahoo! Voices	2012	450,000	web	hacked	[296][297]
Yale University	2010	43,000	academic	accidentally published	[28]
Zappos	2012	24,000,000	web	hacked	[298]

1. ? "21st Century Oncology notifies 2.2 million of hacking, data breach", *CBS12*, March 14, 2016
2. ? "Oh No, Not Again...Chalk Up Yet Another Health Data Breach", *National Law Review*, March 14, 2016
3. ? Template:Cite web
4. ? Template:Cite web
5. ? Template:Cite web
6. ? Template:Cite web
7. ? Template:Cite news
8. ? Template:Cite web
9. ? Template:Cite web
10. ? Template:Cite web
11. ? Template:Cite web
12. ? Template:Cite web
13. ? Template:Cite web
14. ? Template:Cite web

15. ? Template:Cite web
16. ? Template:Cite news
17. ? Template:Cite web
18. ? Template:Cite web
19. ? Template:Cite web
20. ? Template:Cite web
21. ? Template:Cite web
22. ? Template:Cite web
23. ? Template:Cite web
24. ? Template:Cite web
25. ? Template:Cite web
26. ? "91,000 state Medicaid clients warned of data breach", *The Seattle Times*, Feb. 9, 2016
27. ? Template:Cite web
28. ^ Template:Cite web
29. ? Template:Cite web
30. ? Template:Cite web
31. ? Template:Cite web
32. ? Template:Cite web
33. ? "Attacker compromises information of 250K in Bailey's data breach", *SC Magazine*, March 16, 2016
34. ? Template:Cite web
35. ? Template:Cite web
36. ? Template:Cite web
37. ? Template:Cite web
38. ? Template:Cite web
39. ? Template:Cite web
40. ? Template:Cite web
41. ? Template:Cite web
42. ? Template:Cite news
43. ? Template:Cite web
44. ? Template:Cite web
45. ? Template:Cite web
46. ? [1]Template:Dead link
47. ? Template:Cite web
48. ? Template:Cite news
49. ^ Template:Cite web
50. ? Template:Cite web
51. ? "Breached Credit Union Comes Out of its Shell", Krebs on Security, Feb. 25, 2016
52. ^ Template:Cite web
53. ? Template:Cite web
54. ? Template:Cite web
55. ? Template:Cite web
56. ? Template:Cite news
57. ? Template:Cite web
58. ? Template:Cite web
59. ? Template:Cite web
60. ? Template:Cite web
61. ? Template:Cite web
62. ? Template:Cite web
63. ? Template:Cite news
64. ? Template:Cite web
65. ? Template:Cite news
66. ? "Cox Communications Investigates Data Breach Affecting 40K Employees", *Info Security Magazine*, March 7, 2016
67. ? Template:Cite web
68. ^ Template:Cite news
69. ? Template:Cite web
70. ? Template:Cite web
71. ? Template:Cite web
72. ? Template:Cite web
73. ? Template:Cite news
74. ? "Breach Exposes Data From Thousands of DHS Employees", *PC Magazine*, Feb. 8, 2016

75. ? "Hackers Get Employee Records at Justice and Homeland Security Depts.", *New York Times*, Feb. 8, 2016
76. ? Template:Cite web
77. ? Template:Cite news
78. ? Template:Cite web
79. ? Template:Cite web
80. ? Template:Cite news
81. ^ Template:Cite web
82. ^ Template:Cite web
83. ? Template:Cite web
84. ? Template:Cite web
85. ^ Template:Cite web
86. ? Template:Cite web
87. ? Template:Cite web
88. ? Template:Cite web
89. ? "Equifax data breach may affect nearly half the US population", Sept 7, 2017
90. ? "Equifax had patch 2 months before hack and didn't install it, security group says", Sept 14, 2017
91. ? Template:Cite web
92. ? Template:Cite web
93. ? Template:Cite web
94. ? Template:Cite web
95. ? Template:Cite web
96. ? "Massive Data Breach At Experian Exposes Personal Data For 15 Million T-Mobile Customers", *Huffington Post*, Oct. 2, 2015
97. ? "Experian data breach affects 15 million people including T-Mobile customers", *Fortune*, Oct. 1, 2015
98. ? "Security: Data Breach & Old Password Expiration", *Eyewire*, Feb. 23, 2016
99. ? Template:Cite web
100. ? Template:Cite web
101. ? Template:Cite web
102. ? Template:Cite web
103. ? Template:Cite news
104. ? Template:Cite web
105. ? Template:Cite web
106. ? Template:Cite web
107. ? Template:Cite web
108. ? Template:Cite web
109. ? Template:Cite web
110. ? Template:Cite web
111. ? Template:Cite web
112. ? Template:Cite web
113. ? Template:Cite web
114. ? Template:Cite web
115. ? Template:Cite web
116. ? Template:Cite web
117. ? Template:Cite web
118. ? Template:Cite web
119. ? Template:Cite web
120. ? Template:Cite news
121. ? Template:Cite news
122. ? Template:Cite web
123. ? Template:Cite web
124. ? Template:Cite web
125. ? "Gyft Notifies Users of Data Breach", *Low Cards*, Feb. 8, 2016
126. ? "Gyft Notifies Affected Users of Security Incident", *BusinessWire*, Feb. 5, 2016
127. ? Template:Cite web
128. ? Template:Cite web
129. ? Template:Cite web
130. ? Template:Cite web
131. ? Template:Cite web
132. ? Template:Cite news
133. ? Template:Cite web
134. ? Template:Cite web

135. ? Template:Cite web
136. ? Template:Cite web
137. ? Template:Cite web
138. ? Template:Cite web
139. ? Template:Cite web
140. ? Template:Cite web
141. ? Template:Cite web
142. ? "IRS taxpayer data theft seven times larger than originally thought", *CNN*, Feb. 26, 2016
143. ? Template:Cite news
144. ? Template:Cite web
145. ? Template:Cite web
146. ? Template:Cite web
147. ? Template:Cite web
148. ? Template:Cite web
149. ? Template:Cite web
150. ? Template:Cite web
151. ? Template:Cite web
152. ? Template:Cite web
153. ? Template:Cite web
154. ? Template:Cite web
155. ? Template:Cite web
156. ? Template:Cite web
157. ? Template:Cite web
158. ? Template:Cite web
159. ? Template:Cite web
160. ? Template:Cite web
161. ? Template:Cite web
162. ? Template:Cite web
163. ? Template:Cite web
164. ? "Marriott Data Breach Is Traced to Chinese Hackers as U.S. Readies Crackdown on Beijing", *New York Times*, Dec. 11, 2018
165. ? Template:Cite web
166. ? Template:Cite web
167. ? Template:Cite web
168. ? Template:Cite web
169. ? Template:Cite web
170. ? Template:Cite web
171. ? Template:Cite news
172. ? Template:Cite web
173. ? Template:Cite news
174. ? Template:Cite web
175. ? Template:Cite web
176. ? Template:Cite web
177. ? Template:Cite web
178. ? Template:Cite news
179. ? Template:Cite web
180. ? Template:Cite web
181. ? Template:Cite web
182. ? Template:Cite web
183. ? Template:Cite web
184. ? Template:Cite web
185. ? Template:Cite web
186. ? Template:Cite web
187. ? Template:Cite news
188. ? Template:Cite web
189. ? "Ofcom tackles mass data breach of TV company information", *The Guardian*, March 10, 2016
190. ? Template:Cite news
191. ? Template:Cite web
192. ? Template:Cite web
193. ? Template:Cite web
194. ? Template:Cite web

195. ? Template:Cite web
196. ? Template:Cite web
197. ? Template:Cite web
198. ? Template:Cite news
199. ? Template:Cite web
200. ? Template:Cite web
201. ? Template:Cite web
202. ? Template:Cite news
203. ? Template:Cite news
204. ? Template:Cite web
205. ? "Rosen Hotels warns customers of 18-month data breach", *Orlando Sentinel*, March 8, 2016
206. ? Template:Cite web
207. ? Template:Cite web
208. ? Template:Cite web
209. ? [2]Template:Dead link
210. ? Template:Cite web
211. ? Template:Cite web
212. ? Template:Cite news
213. ? Template:Cite news
214. ? Template:Cite web
215. ? Template:Cite web
216. ? Template:Cite web
217. ? Template:Cite web
218. ? Template:Cite web
219. ? Template:Cite web
220. ? Template:Cite web
221. ? Template:Cite web
222. ? Template:Cite web
223. ? Template:Cite web
224. ? Template:Cite web
225. ? Template:Cite web
226. ? Template:Cite web
227. ? Template:Cite web
228. ? Template:Cite web
229. ? Template:Cite web
230. ? Template:Cite web
231. ? Template:Cite web
232. ? Template:Cite news
233. ? Template:Cite news
234. ? Template:Cite web
235. ? Template:Cite news
236. ? Template:Cite web
237. ? Template:Cite web
238. ? Template:Cite web
239. ? Template:Cite web
240. ? Template:Cite web
241. ? Template:Cite web
242. ? Template:Cite web
243. ? Template:Cite web
244. ? Template:Cite web
245. ? Template:Cite web
246. ? Template:Cite web
247. ? Template:Cite web
248. ? http://www.datalossdb.org
249. ? http://www.informationweek.com/security/attacks/t-mobile-lost-17-million-subscribers-per/
250. ? Template:Cite web
251. ? Template:Cite web
252. ? Template:Cite web
253. ? Template:Cite web
254. ? Template:Cite web

255. ? Template:Cite web
256. ? Template:Cite news
257. ? Template:Cite web
258. ? Template:Cite web
259. ? Template:Cite web
260. ? Template:Cite news
261. ? Template:Cite news
262. ? Template:Cite news
263. ? Template:Cite web
264. ? Template:Cite web
265. ? "Data breach affects 80,000 UC Berkeley faculty, students and alumni", Fox News, Feb. 28, 2016
266. ? "University of Maryland computer security breach exposes 300,000 records", Washington Post, Feb. 19, 2014
267. ? Template:Cite web
268. ? Template:Cite news
269. ? Template:Cite web
270. ? Template:Cite web
271. ? Template:Cite web
272. ? Template:Cite web
273. ? Template:Cite web
274. ? "Verizon's Data Breach Fighter Gets Hit With, Well, a Data Breach", *Fortune* magazine, March 24, 2016
275. ? Template:Cite web
276. ? Template:Cite news
277. ? Template:Cite web
278. ? Template:Cite web
279. ? Template:Cite web
280. ? Template:Cite web
281. ? Template:Cite web
282. ? Template:Cite web
283. ? Template:Cite web
284. ? Template:Cite news
285. ? Template:Cite web
286. ? Template:Cite web
287. ? Template:Cite web
288. ? Template:Cite web
289. ? Template:Cite web
290. ? Template:Cite web
291. ? Template:Cite web
292. ? Template:Cite web
293. ? Template:Cite news
294. ? Template:Cite web
295. ? Template:Cite web
296. ? Template:Cite web
297. ? "Yahoo Voices Breach Exposes 453,000 Passwords", *PC Magazine*, July 12, 2012
298. ? Template:Cite web

29 Defence-in-Depth

29.1 Definition[edit]

Defence-in-Depth. Security strategy integrating people, processes and technology to establish a variety of barriers across multiple layers and dimensions of the organisation.

29.2 Reference[edit]

- Adapted from NIST and FFIEC

30 Denial of Service

30.1 Definition[edit]

Denial of Service. (DoS) Prevention of authorised access to information or information systems; or the delaying of information system operations and functions, with resultant loss of availability to authorised users.

30.2 Reference[edit]

- Adapted from ISO/IEC 27033-1:2015

31 Detect Function

31.1 Definition[edit]

Detect Function. Develop and implement the appropriate activities to identify the occurrence of a cyber event.

31.2 See Also[edit]

- Risk Management Jobs

31.3 Reference[edit]

- Adapted from NIST Framework

32 Distributed Denial of Service

32.1 Definition[edit]

Distributed Denial of Service. (DDoS) A denial of service that is carried out using numerous sources simultaneously.

32.2 Reference[edit]

- Adapted from NICCS

33 Environmental Hazards

33.1 Definition[edit]

The **Environmental Hazards** sub-category of Cyber Risk includes natural events such as earthquakes and floods, but also hazards associated with the immediate environment or infrastructure in which digital assets are located. The latter encompasses power failures, electrical interference, pipe leaks, and atmospheric conditions.

33.2 References[edit]

- VERIS

34 Exploit

34.1 Definition[edit]

Exploit. Defined way to breach the security of information systems through vulnerability.

34.2 Reference[edit]

- ISO/IEC 27039:2015

35 Hacking

35.1 Definition[edit]

Hacking is defined as all attempts to intentionally access or harm information assets without (or exceeding) authorization by circumventing or thwarting logical security mechanisms.

Examples includes brute force, SQL injection, cryptanalysis, denial of service attacks, etc.

35.2 References[edit]

- VERIS

36 Identify Function

36.1 Definition[edit]

Identify Function. Develop the organisational understanding to manage cyber risk to assets and capabilities.

36.2 See Also[edit]

- Risk Management Jobs

36.3 Reference[edit]

- Adapted from NIST Framework

37 Identity and Access Management

37.1 Definition[edit]

Identity and Access Management. (IAM) Encapsulates people, processes and technology to identify and manage the data used in an information system to authenticate users and grant or deny access rights to data and system resources.

37.2 Reference[edit]

- Adapted from ISACA Full Glossary

38 Incident Response Team

38.1 Definition[edit]

Incident Response Team. (IRT) [also known as CERT or CSIRT] Team of appropriately skilled and trusted members of the organisation that handles incidents during their life cycle.

38.2 Reference[edit]

- ISO/IEC 27035-1:2016

39 Indicators of Compromise

39.1 Definition[edit]

Indicators of Compromise. (IoCs) Identifying signs that a cyber incident may have occurred or may be currently occurring.

39.2 Reference[edit]

- Adapted from NIST (definition of ?Indicator?)

40 Information Sharing

40.1 Definition[edit]

Information Sharing. An exchange of data, information and/or knowledge that can be used to manage risks or respond to events.

40.2 Reference[edit]

- Adapted from NICCS

41 Information System

41.1 Definition[edit]

Information System. Set of applications, services, information technology assets or other information-handling components, which includes the operating environment.

41.2 Reference[edit]

- Adapted from ISO/IEC 27000:2018

42 Information Theft

42.1 Definition[edit]

Information Theft is the fraudulent acquisition of information assets (data) by parties external or internal to the organization. Such information may be stored in physical form (e.g. paper records) or digitally, in which case it is a type of IT Risk

42.2 Examples[edit]

There is a wide variety of attack vectors, depending on the storage/transmission mechanisms, for example

- Document Theft / Copying
- Database Theft
- Credit Card Number, ATM Spoofing, PIN Capturing

42.3 See Also[edit]

- Wikipedia on Data Theft

---

43 Integrity

43.1 Definition[edit]

Integrity. Property of accuracy and completeness. The safeguarding of accuracy and completeness of assets, particularly data records.

43.2 Reference[edit]

- ISO/IEC 27000:2018

44 Malware

44.1 Definition[edit]

Malware is a class of Threat Action under Cyber Risk. It involves software designed with malicious intent containing features or capabilities that can potentially cause harm directly or indirectly to entities or their information systems.

Malware is any malicious software, script, or code run on a device that alters its state or function without the owner?s informed consent.

44.2 Examples[edit]

- viruses
- worms
- spyware
- keyloggers
- backdoors, etc.

44.3 Reference[edit]

- Adapted from ISO/IEC 27032:2012
- VERIS

45 Misuse

45.1 Definition[edit]

Misuse is a Cyber Risk sub-category defined as the use of entrusted organizational resources or privileges for any purpose or manner contrary to that which was intended.

Includes administrative abuse, use policy violations, use of non-approved assets, etc. These actions can be malicious or non-malicious in nature. Misuse is exclusive to parties that enjoy a degree of trust from the organization, such as insiders and partners.

45.2 References[edit]

- VERIS

46 Multi-Factor Authentication

46.1 Definition[edit]

Multi-Factor Authentication. The use of two or more of the following factors to verify a user?s identity: -- knowledge factor, ?something an individual knows?; -- possession factor, ?something an individual has?; -- biometric factor, ?something that is a biological and behavioural characteristic of an individual?.

46.2 Reference[edit]

- Adapted from ISO/IEC 27040:2015 and ISO/IEC 2832- 37:2017 (definition of ?biometric characteristic?)

47 Non-Repudiation

47.1 Definition[edit]

Non-Repudiation. Ability to prove the occurrence of a claimed event or action and its originating entities.

47.2 Reference[edit]

- ISO 27000:2018

48 Patch Management

48.1 Definition[edit]

Patch Management. The systematic notification, identification, deployment, installation and verification of operating system and application software code revisions. These revisions are known as patches, hot fixes and service packs.

48.2 Reference[edit]

- NIST

49 Penetration Testing

49.1 Definition[edit]

Penetration Testing. A test methodology in which assessors, using all available documentation (e.g. system design, source code, manuals) and working under specific constraints, attempt to circumvent the security features of an information system.

49.2 Reference[edit]

- NIST

50 Physical Action

50.1 Definition[edit]

Physical Actions is the sub-category of Cyber Risk that encompasses deliberate threats to digital assets that involve proximity, possession, or force.

It Includes theft, tampering, snooping, sabotage, local device access, assault, etc.

VERIS classification note: Natural hazards and power failures are often classified under physical threats. We include such events in the Environmental Hazards category and restrict the Physical category to intentional actions perpetrated by a human actor. This is done for several reasons, including the assessment of threat frequency and the alignment of controls.

51 Protect Function

51.1 Definition[edit]

Protect Function. Develop and implement the appropriate safeguards to ensure delivery of services and to limit or contain the impact of cyber incidents.

51.2 See Also[edit]

- Risk Management Jobs

51.3 Reference[edit]

- Adapted from NIST Framework

52 Recover Function

52.1 Definition[edit]

Recover Function. Develop and implement the appropriate activities to maintain plans for cyber resilience and to restore any capabilities or services that were impaired due to a cyber incident.

52.2 See Also[edit]

- Risk Management Jobs

52.3 Reference[edit]

- Adapted from NIST Framework

53 Reliability

53.1 Definition[edit]

Reliability. Property of consistent intended behaviour and results.

53.2 Reference[edit]

- ISO/IEC 27000:2018

54 Respond Function

54.1 Definition[edit]

Respond Function. Develop and implement the appropriate activities to take action regarding a detected cyber event.

54.2 See Also[edit]

- Risk Management Jobs

54.3 Reference[edit]

- Adapted from NIST Framework

55 Situational Awareness

55.1 Definition[edit]

Situational Awareness. The ability to identify, process and comprehend the critical elements of information through a cyber threat intelligence process that provides a level of understanding that is relevant to act upon to mitigate the impact of a potentially harmful event.

55.2 Reference[edit]

- CPMI-IOSCO

56 Social Engineering

56.1 Definition[edit]

Social Engineering. A general term for trying to deceive people into revealing information or performing certain actions. In the context of Cyber Risk in particular, social tactics employ deception, manipulation, intimidation, etc to exploit the human element, or users, of information assets. Includes pretexting, phishing, blackmail, threats, scams, etc.

56.2 Reference[edit]

- Adapted from FFIEC
- VERIS

57 Systemic Cyber Risk

57.1 Contents

57.2 Definition[edit]

Systemic Cyber Risk concerns the possibility that Cyber Risk events may reach Systemic Risk proportions, especially in the context of the Financial Services industry

57.3 Background[edit]

To date, the financial sector has not experienced any cyber incidents that have threatened financial stability. However, as argued in[1] an intentional incident with the goal of destabilising the financial system could, in certain circumstances, trigger a systemic crisis.

57.4 See Also[edit]

- Cyber Run

57.5 References[edit]

1. ? ESRB, Systemic Cyber Risk, February 2020

58 Tactics, Techniques and Procedures

58.1 Definition[edit]

Tactics, Techniques and Procedures. (TTPs) The behaviour of a Threat Actor.

A tactic is the highest-level description of this behaviour, while techniques give a more detailed description of behaviour in the context of a tactic, and procedures an even lower-level, highly detailed description in the context of a technique.

58.2 Reference[edit]

- Adapted from NIST 800-150

59 Technical Error

59.1 Definition[edit]

Technical Error broadly encompasses anything done (or left undone) incorrectly or inadvertently by any agent involved in the operation, maintenance or other support of digital infrastructure

Technical errors include:

- omissions
- misconfigurations
- programming errors
- trips and spills
- malfunctions, etc.

It does NOT include:

- something done (or left undone) intentionally or by default that later proves to be unwise or inadequate
- errors triggered by Environmental Hazards

59.2 References[edit]

- VERIS

60 Threat

60.1 Definition[edit]

Threat. A combination of the Risk, the consequence of that risk, and the likelihood that the negative event will take place. A potential cause of an unwanted incident, which may result in harm to individuals, a system or organization, the environment, or the community.

60.2 Issues and Challenges[edit]

- The term threat implies to a larger extent that there is explicit malicious intent (by an agent) behind the risk.

61 Threat Action

61.1 Definition[edit]

Threat Action in the context of IT Security Risk is the specific set of activities used by a Threat Actor to create a Cyber Incident

Threat actions describe what the threat actor(s) did to cause or contribute to the incident. Every incident has at least one, but most will comprise multiple actions (and often across multiple categories).

61.1.1 VERIS Taxonomy of Threat Actions[edit]

The VERIS taxonomy[1] recognizes 7 distinct actions:

- Malware
- Hacking
- Social Engineering
- Misuse
- Physical Action
- Technical Error
- Environmental Hazards

61.2 References[edit]

1. ? http://veriscommunity.net/actions.html

62 Threat Actor

62.1 Contents

62.2 Definition[edit]

Threat Actor. An individual, a group or an organisation believed to be operating with malicious intent and causing or contributing to a Cyber Incident

There can be more than one actor involved in any particular incident, and their actions can be malicious or non-malicious, intentional or unintentional, causal or contributory. VERIS recognizes three primary categories of threat actors:

- External
- Internal, and
- Partner.

62.2.1 External Actors[edit]

External threats originate from sources outside of the organization and its network of partners. Examples include criminal groups, lone hackers, former employees, and government entities. Also includes God (as in ?acts of?), ?Mother Nature,? and random chance. Typically, no trust or privilege is implied for external entities.

62.2.2 Internal Actors[edit]

Internal threats are those originating from within the organization. This encompasses company full-time employees, independent contractors, interns, and other staff. Insiders are trusted and privileged (some more than others).

62.3 Partners[edit]

Partners include any third party sharing a business relationship with the organization. This includes suppliers, vendors, hosting providers, outsourced IT support, etc. some level of trust and privilege is usually implied between business partners.

62.4 References[edit]

- Adapted from STIX
- Adapted from VERIS

63 Threat Analysis

63.1 Definition[edit]

Threat Analysis. The process of evaluating threats to identify unacceptable concentrations of risk to activities and single points of failure.

64 Threat Assessment

64.1 Definition[edit]

Threat Assessment. Process of formally evaluating the degree of Threat to an organisation and describing the nature of the threat.

64.2 Notes[edit]

It is a type of Risk Analysis. It may involve the construction of a Threat Model

64.3 Reference[edit]

- Adapted from NIST

65 Threat Intelligence

65.1 Definition[edit]

Threat Intelligence denotes Threat Information that has been aggregated, transformed, analysed, interpreted or enriched to provide the necessary context for decision-making processes.

65.2 Reference[edit]

- NIST 800-150

66 Threat Model

66.1 Contents

66.2 Definition[edit]

A **Threat Model** is a formal representation of the risk landscape faced by an individual or organization that explicitly focuses on risks that can be classified as threats.

66.3 Classification[edit]

- Attacker centric, focusing on Threat Actor identification and analysis
- Asset centric, focusing on Asset identification and analysis
- System centric

66.4 Examples[edit]

66.4.1 VERIS A4 Threat Model[edit]

A cyber incident is viewed as a series of events that adversely affects the information assets of an organization. The VERIS classification employs the A4 threat model[1]: Every cyber incident is comprised of the following elements (the 4 A?s)

- Actors: Whose actions affected the asset?
- Threat Action: What actions affected the asset?
- Assets: Which assets were affected?
- Attributes: How the asset was affected?

66.5 References[edit]

1. ? VERIS Incident Description

67 Threat Model versus Risk Model

67.1 Threat Model versus Risk Model[edit]

The concepts of Threat Model and Risk Model have some overlap but also significant differences in context and implications.

67.2 Overlap Areas[edit]

- A Threat is a type of Risk Factor that explicitly involves the malicious intend of an Agent. It is thus a subset of an overall Risk landscape which in the domain of Information Technology would be most broadly covered under IT Risk.
- Constructing a threat model can be considered a type of Risk Analysis

67.3 Differences and Nuance[edit]

- The term model in threat model means primarily a conceptual identification of a system's characteristics (it is a system model). The term model in risk model frequently implies a Quantitative Risk Model

68 Threat Vector

68.1 Definition[edit]

Threat Vector is a path or route used by the Threat Actor to gain access to the target.

68.2 Notes[edit]

- It may be an element in constructing a Threat Model

68.3 Reference[edit]

- Adapted from ISACA Fundamentals

69 Threat-Led Penetration Testing

69.1 Definition[edit]

Threat-Led Penetration Testing (TLPT), also known as Red Team Testing is a controlled attempt to compromise the cyber resilience of an entity by simulating the tactics, techniques and procedures of real-life threat actors.

TLPT is based on targeted Threat Intelligence and focuses on an entity?s people, processes and technology, with minimal foreknowledge and impact on operations.

69.2 Reference[edit]

- G-7 Fundamental Elements

70 Traffic Light Protocol

70.1 Definition[edit]

Traffic Light Protocol. (TLP) A set of designations used to ensure that information is shared only with the appropriate audience. It employs a pre-established colour code to indicate expected sharing boundaries to be applied by the recipient.

70.2 Reference[edit]

- Adapted from FIRST

71 Verification

71.1 Definition[edit]

Verification. Confirmation, through the provision of evidence, that specified requirements have been fulfilled.

- In the context of Supply Chain Finance It is a service offered by the factor/financier to establish the validity of a debt/receivable before its due payment date.
- In the context of Cyber Risk it is the confirmation, through the provision of objective evidence, that specified requirements have been fulfilled.

71.2 Reference[edit]

- ISO/IEC 27042:2015

72 Vulnerability

72.1 Definition[edit]

Vulnerability. A weakness, susceptibility or flaw of an asset or control that can be exploited by one or more threats. The degree to which a person, asset, process, information, infrastructure or other resources are exposed to the actions or effects of a risk, event or other occurrence. The conditions determined by physical, social, economic and environmental factors or processes which increase the susceptibility of an individual, a community, assets or systems to the impacts of hazards.

72.2 See Also[edit]

- For positive factors which increase the ability of people to cope with hazards, see also the definitions of ?Capacity? and ?Coping Capacity?

72.3 Reference[edit]

- Adapted from CPMI-IOSCO and ISO/IEC 27000:2018
- https://www.undrr.org/terminology/vulnerability

73 Vulnerability Assessment

73.1 Definition[edit]

Vulnerability Assessment. Systematic examination of an information system, and its controls and processes, to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures and confirm the adequacy of such measures after implementation.

73.2 See Also[edit]

- Vulnerability

73.3 Reference[edit]

- Adapted from NIST