



GB/Z 20986—2007

Information security technology-Guidelines for the category and classification of
Information security incidents

.....

.....

1	1
2	1
3	1
4	2
4.1	2
4.2	2
4.2.1	2
4.2.2	A	2
4.2.3	D	3
4.2.4	C	3
4.2.5	FF	3
4.2.6	D	4
4.2.7	4
5	4
5.1	4
5.1.1	4
5.1.2	4
5.1.3	4
5.1.4	4
5.2	5
5.2.1	5
5.2.2	5
5.2.3	5
5.2.4	5
5.2.5	5

- 1)
- 2)
- 3)
- 4)
- 5)

1

2

2.1

information system

2.2

information security incident

3

MI	Malware Incidents
CVI	Computer Virus Incidents
WI	Worms Incidents
THI	Trojan Horses Incidents
BI	Botnets Incidents
BAI	Blended Attacks Incidents
WBPI	Web Browser Plug-Ins Incidents
NAI	Network Attacks Incidents
DOSAI	Denial of Service Attacks Incidents
BDAI	Backdoor Attacks Incidents
VAI	Vulnerability Attacks Incidents
NSEI	Network Scan & Eavesdropping Incidents
PI	Phishing Incidents
II	Interference Incidents
IDI	Information Destroy Incidents
IAI	Information Alteration Incidents
IMI	Information Masquerading Incidents
ILEI	Information Leakage Incidents
III	Information Interception Incidents

		7	
	a)	DOSAI	
		CPU	
	b)	BDAI	
	c)	VAI	
	d)	NSEI	
	e)	PI	
	f)	II	
	g)	ONAI	6
4.2.3		IDI	
			6
	a)	IAI	
	b)	IMI	
	c)	ILEI	
	d)	III	
	e)	ILOI	
	f)	OIDI	5
4.2.4		ICSI	
			4
	a)		
	b)		
	c)		
	d)		4
4.2.5		FF	

a) SHF

b) PSFF

c) MDA

d) IF-OT 3

4.2.6 DI

4.2.7 OI 6

5

5.1

5.1.1

5.1.2

5.1.3

a)

b)

c)

d)

5.1.4

a)

b)

c)

d)

5.2

5.2.1

5.2.2

a)

b)

5.2.3

a)

b)

5.2.4

a)

b)

5.2.5

a)

b)

