Types of Attacks Experienced

By Percent of Respondents

Type of Attack	2005	2006	2007	2008	2009	2010
Malware infection	74%	65%	52%	50%	64%	67%
Bots / zombies within the organization	added in 2007		21%	20%	23%	29%
Being fraudulently represented as sender of phishing messages	added in 2007		26%	31%	34%	39%
Password sniffing	added in 2007		10%	9%	17%	12%
Financial fraud	7%	9%	12%	12%	20%	9%
Denial of service	32%	25%	25%	21%	29%	17%
Extortion or blackmail associated with threat of attack or release of stolen data	option added in 2009				3%	1%
Web site defacement	5%	6%	10%	6%	14%	7%
Other exploit of public-facing Web site	option altered in 2009				6%	7%
Exploit of wireless network	16%	14%	17%	14%	8%	7%
Exploit of DNS server	added in 2007		6%	8%	7%	2%
Exploit of client Web browser	option added in 2009				11%	10%
Exploit of user's social network profile	option added in 2009				7%	5%
Instant messaging abuse	added in 2007		25%	21%	8%	5%
Insider abuse of Internet access or e-mail (i.e. pornography, pirated software, etc.)	48%	42%	59%	44%	30%	25%
Unauthorized access or privilege escalation by insider	option altered in 2009				15%	13%
System penetration by outsider	option altered in 2009				14%	11%
Laptop or mobile hardware theft or loss	48%	47%	50%	42%	42%	34%
Theft of or unauthorized access to PII or PHI due to mobile device theft/loss	option added in 2008			8%	6%	5%
Theft of or unauthorized access to intellectual property due to mobile device theft/loss	option added in 2008			4%	6%	5%
Theft of or unauthorized access to PII or PHI due to all other causes	option added in 2008			8%	10%	11%
Theft of or unauthorized access to intellectual property due to all other causes	option added in 2008			5%	8%	5%

2010 CSI Computer Crime and Security Survey

2010: 149 Respondents

Figure 10