

Security Incident Response Checklist

No	Procedures	Status	Notes
1	Do incident-response procedures exist?		
2	Are procedures understandable and up-to-date?		
3	Have all key personnel been trained in using the procedures?		
4	Do the procedures include instructions for contacting a security expert 24-hours-a-day, 7-days-a-week?		
5	If the security expert does not respond, does a procedure exist for escalating the problem to management?		
6	Is there a procedure for determining when to contact outside help, and whom to contact?		
7	Do procedures include notifying the CIO immediately when any break-in occurs, and again when the break-in is resolved?		
8	Has adequate funding been allotted for developing and maintaining incident responses to break-ins?		
9	Have key personnel actually attended all required training sessions?		
10	Have appropriate background checks been conducted on key personnel?		
11	Are communications between and among the system administration and security groups flowing smoothly?		
12	Are disaster-recovery plans in place?		
13	Do all systems have adequate security controls? ("Adequate" here means proven adequate by formal audit results.)		
14	Are system audit logs enabled?		
15	Are system logs periodically reviewed?		
16	Are the tools needed to detect an intrusion installed and operational?		
17	Can the detection software installed on your network detect unknown attacks?		
18	Can you detect and prevent attacks on the network and the host (a layered approach to detection)?		
19	Are attacks easy to trace back on your network?		