



Information Security – #5 Incident Response

Overview

Taking steps to protect personal information can go a long way toward preventing a security breach. Nevertheless, breaches can happen and that's why organizations should have a response plan in place before an incident occurs.

#5: Information Security – Incident Response

Ensure your organization's incident response plan addresses these important areas:

- *Team.* Senior management sets the tone for an organization's commitment to data security. Designate a well-respected senior official to head up your response team.
- *Plan.* Once you've put together your response team, have them draft plans for how your business will respond to different types of security incidents. Sample scenarios may include a lost laptop, servers hacked, internal theft of data, etc.
- *Timely.* If your staff suspects a breach, investigate it immediately. Waiting days to convene a committee can waste precious time.
- *Disconnect.* If you suspect a computer breach, immediately sever the compromised computer's access to the Internet and to your network. To assess the impact, ask your IT staff to preserve any available network logs, file transfer logs, system logs, and access reports. Also investigate if intruders opened files or placed new programs on your computer.
- *Contact.* Consider whom to inform in the event of an incident, both inside and outside your company. You may need to notify consumers, law enforcement agencies, customers, credit bureaus, and other businesses that may be affected by the breach. In addition, about 40 states have laws addressing data breaches. Have that information on file before you need it.

Publication and Author Information

Jim Kelton is Managing Principal of Altius IT (www.AltiusIT.com), an IT security audit, security consulting, and risk management company based in Costa Mesa, California. Mr. Kelton has over 30 years of experience in the Information Technology industry and is recognized as a security expert. He is certified by the Information Systems Audit and Control Association (ISACA) as:
Certified Information Systems Auditor (CISA)
Certified in Risk and Information Systems Controls (CRISC)
Certified in the Governance of Enterprise IT (CGEIT)



He sits on the Board of Directors of the following associations and organizations:

- Association of Professional Consultants (APC)
- International Association of Professional Security Consultants (IAPSC)
- Technology Professionals Association (TPA)