KIVU
human • digital • business
ANALYSIS

INCIDENT RESPONSE CHECKLIST

The purpose of this checklist is to provide clients of Kivu Consulting, Inc. with guidance in the initial stages of an actual or possible data breach.

Clients are encouraged to use these questions to:

1. *Gather initial information for use by Kivu Consulting, Inc.'s experts during the subsequent investigation;*
2. *Identify the key stake-holders within the client organization and determine the specific roles for which they are responsible;*
3. *Commence the gathering and preservation of evidence.*

This checklist is not exhaustive and should be tailored for the specific elements of the client's environment, using input from Kivu Consulting, Inc.

This checklist is designed for informational purposes only and is not intended to be legal advice.

No portion of this document may be reproduced, reused or otherwise distributed in any form without prior written consent of Kivu Consulting, Inc.

KIVU CONSULTING, Inc.
44 Montgomery Street,
Suite 700
San Francisco, CA 94104
Tel: (415) 524-7320
Fax: (415) 524-7325
www.kivuconsulting.com

Kivu Incident Response Questionnaire

1. Investigate Incident Scope and Impact

Questions/requests to be addressed to IT/ HR/ Legal point-person(s).

1. What has been observed that lead to contacting Kivu Consulting?

   ○ Missing/ stolen computer

   ○ Internal finding of possible data breach

   ○ External report of possible data breach

   ○ Whistle-blower/ rumor

   ○ Other Please specify:______________________________

2. How were any problems or issues first detected?

   ○ IT IDS/ audit

   ○ External audit

   ○ Third party

   ○ Other Please specify:______________________________

3. When was the incident detected and by whom? (Build a timeline of events and list individuals involved.)

4. Who is aware of the incident within organization?

   ○ Senior management

   ○ Legal

   ○ IT

   ○ HR

   ○ Security

   ○ Other Please specify:________________________________

5. Which outside organization(s) are aware of incident?

   ○ Outside counsel

   ○ Third-party vendor

   ○ Law enforcement

   ○ Regulators

   ○ PR firm

   ○ Other Please specify:________________________________

6. Are there any requirements limiting the work to be performed by specific citizenship?

7. Which data sources were targeted and/ or affected by the incident?

   ○ Patient/ customer data

   ○ Employee data

   ○ Other Please specify:________________________________

8. What other recent security incidents occurred in the affected environment or organization?
    - Theft/ break-in
    - Employee misconduct
    - Issues with logs
    - Virus/malware/root kit detected
    - Other Please specify:______________________________
9. Is there any history of similar situations or patterns? If so, what?
    a. What changes were made to the affected systems or security controls?
10. Who is the primary incident response coordinator? Backup coordinator?
11. Who is authorized to make business decisions about affected operations and IT infrastructure?
    a. Who is the ultimate decision-maker for this incident?
12. What are the leading hypotheses for how the initial compromise transpired?
13. Are you aware of any compliance or legal obligations associated with this incident (e.g., PCI, HIPAA, breach notification laws, etc.)?
    a. Which stakeholders are responsible for in-house compliance, privacy or legal issues?
14. Where is evidence being preserved?

15. What is the current phase of the incident? (Select all that apply.)

○ Identification

○ Containment

○ Eradication

○ Recovery

16. Does the incident involve an outsourced party?

○ Business partner

○ Outsourced services

○ Alliances

○ Other Please specify:_______________________________

2. **Preliminary Review of Incident by Organization**

Questions/requests to be addressed to IT/ HR/ Legal point-person(s).

1. Who within the organization has been tasked with preserving evidence? (This includes affected workstations, hard drives, network logs, network backups, CCTV video, physical access logs, and cell phones.)
2. What evaluations were completed to define the scope and impact of the incident?
   - o IT
   - o HR/ Legal
   - o Security
3. What steps were taken to contain and mitigate the incident? (This includes, but is not limited to, retaining suspect computers, changing passwords, turning off remote access, acquiring log files, disconnecting infected systems from network, suspending employee access or group privileges.)
4. What tools were deployed or system commands executed within the affected environment and on affected systems as part of the initial investigation? Is there supporting documentation?
5. What logs were reviewed? If reviewed, what were the suspicious entries? What other unusual event or state information exists?
6. What notifications were sent by the infrastructure systems? (This may include unusual login access, exceeding monetary thresholds, file download alerts, intrusion detection, anti-virus, etc.) Who received notifications?
7. Are there unanswered questions about the incident or conflicting information?
8. What other analysis may be required?
9. Is law enforcement involved? Is there a search warrant/ subpoena?

3. Technical Assessment to Determine Scope and Impact

Questions/requests to be addressed to IT/IS point-person(s).

A. Infrastructure

1. Which persons within the organization can identify how the IT network functions? Specifically:
   - Firewalls, DMZ, Gateways, Access points
   - Network domains, Proxy, Domain controllers
   - Remote access and VPN
   - Intrusion Detection (ID) systems, Intrusion Prevention (IP) systems, SIEM
   - Anti-virus/ malware defenses (internal and on perimeter)
   - Network quarantine systems
   - Data storage
   - E-mail systems
   - ERP systems and any proprietary or specialty applications
   - Data leakage protection (DLP)
2. Is there a diagram or illustration of the affected network's topology and system architecture? Is there supporting documentation?
3. What are the physical locations of all affected IT infrastructure? (There may be multiple individuals and locations involved. Employee home-offices and personal computers may also be involved.)
4. Is any of the organization's IT infrastructure hosted by third-parties? (Create a list.)
5. What are the network restrictions for employee-users and other parties who had access?

6. What asset management and discovery tools are in use?
7. Is there an IT asset inventory report for all infrastructure components related to the incident? (If none in use, is there a current inventory of IT assets related to the incident? The report should contain hard and software information such as MAC Address and OS, network identification information such as host name and network address, and other system details.)
8. Identify where key employees in IT, HR, Legal and Security will be during the next 7-14 days. (User activity may need monitoring.)
9. Task IT with identifying (and providing to Kivu Consulting, Inc.) names/ details concerning:
   - Internet or hosted service providers
   - Internal IP ranges and external facing IP ranges
   - Naming conventions for organization's networked computers/ servers

B. Logging

1. What logs currently exist for the IT infrastructure? Which logs are currently running and active? Have any logging activity started after the event? Logging can include:
   a. Network
      i. Firewall
      ii. Routers
      iii. Wireless Access Points
      iv. Domain Controller
      v. Anti-Virus updates and issues

a. Network (continued)

   vi. ID and/or IP systems (IDPS)

   vii. Vulnerability management

   viii. Network quarantine servers

   ix. Network appliances

   x. File Servers (e.g. internal access of data)

   xi. Backups

   xii. Remote access to network

   xiii. Internet Access / Database

   xiv. Web proxies

   xv. Printers

b. Physical

   i. Automated building entry/ exit systems

   ii. Sign-in sheets

   iii. Video surveillance

   iv. Lists of key assignments or room access

2. What is the retention policy for security logs?

3. Are logs backed up or overwritten? If so, what frequency?

C. Security

1. When was the last security or vulnerability assessment conducted? If so, is there documentation available?
2. What security, IDS/IPS, vulnerability or network quarantine infrastructure components exist in the affected IT infrastructure? (This includes firewall hardware and software, user authentication systems, IDS/IPS systems, etc.)
3. Is there a network diagram or documentation that defines security component topology and architecture? (This includes perimeter security, DMZ, network address, virtual local area network, tunneling, etc.)
4. Are affected system established from standard builds (or images) that allow analysis and/ or re-building affected systems?
5. IT should begin an inventory of IT assets if not established:
   - Operating System versions and service patches of networked computers (servers and workstations)
   - Asset list (e.g. which employees have been assigned which computers)
   - Permissions of individuals/ group memberships
   - IT/ HR should put together all local and network policies, and proof they have been issued to employees and third parties/ consultants
6. Are IDS/IPS systems network and /or host-based?
   a. What kind? Version?
   b. Passive or Reactive?
   c. Are updates automatic or manual?
7. Are anti-virus systems network and/ or host-based?
   a. What kind? Version?

b. Definition updating policies?

c. Are updates automatic or manual?

8. What are password policies/ employee account audits? IT/ HR should begin compiling documentation showing organization's password policies and any employee audits. Review HR policies for employee computer and electronic device use.
9. Wireless Access Point Security type including authentication, encryption, etc.?
10. What e-mail systems and application are used by organization? What is the configuration? What is the security policy for email? Is there remote access? (This includes attachments scanned, dumpster set for deleted email recovery, and archived retention of all email.)
11. What file servers are in use?
    a. Type?
    b. Share permissions?
    c. File System?
    d. Achieved/Backed up?
12. Guest and remote access?
13. Who within IT is responsible for backup policies, continuity, and disaster recovery? Have they been informed of incident?

4. Incident Response Next Steps and Remediation

Questions/requests to be addressed to IT/ HR/ Legal point-person(s).

1. Are there an incident response plans, instructions or guidelines for the affected group(s)?
2. Which members of IT have been trained in incident response and/ or computer forensics? What was the training?
3. Which system or network components cannot go off-line without critical impact on business continuity?

4 What tools are available for Kivu Consulting's use to assess network and/ or host-based activity?

5. For purposes of analysis, what data can be removed from the organization/ third-party hosting for review at Kivu Consulting's computer labs? What safeguards (e.g., encryption) are required by the organization?
6. What backup-restore capabilities are available to recover from the incident?
7. If retained, who will Kivu Consultants be reporting to within the organization?

○ Senior Management

○ HR

○ Legal

○ IT

○ Security

○ Other Please specify:______________________________