securityMETRICS®

# Incident Response Plan Basics

## Identify

Identification (or detection) is the process where you determine whether you've actually been breached by looking for deviations from normal operations and activities.

- [ ] **Proactively search for a breach:**
  - [ ] Utilize FIM (File Integrity Monitoring)
  - [ ] Check Logs
    - [ ] Firewall
    - [ ] System
    - [ ] IDS/IPS
  - [ ] Notice any system anomalies
    - [ ] Malfunctioning antivirus software
    - [ ] Atypical log-in times
    - [ ] Presence of unexpected IPs
    - [ ] Unusual traffic
    - [ ] Reduced operating speed
- [ ] **Document how you've been breached and how you were notified by using these four high-probability scenarios:**
  - [ ] The breach is discovered internally (e.g., review of intrusion detection system logs, alerting systems, system anomalies, or anti-virus scan malware alerts)
  - [ ] Your bank informs you of a possible breach based on reports of customer credit card fraud

Get Incident Response Help →

- [ ] Law enforcement discovers the breach while investigating the sale of stolen card information
- [ ] A customer complains to you because your organization was the last place they used their card before it began racking up fraudulent charges

## Prepare

Preparation often takes the most effort in your incident response planning while being the most crucial step to protect your organization.

- [ ] Make an Incident Response plan:
  - [ ] Assign employees specific roles and responsibilities in case of a data breach
  - [ ] Ensure your employees receive proper training regarding their incident response roles and responsibilities
  - [ ] Develop and regularly conduct tabletop exercises
    - [ ] Evaluate your incident response plan
      - [ ] Make adjustments based on staff performance
  - [ ] Ensure that all aspects of your incident response plan (such as training, hardware, and software resources) are approved and funded in advance
- [ ] Update your Business Continuity Plan

## Once You've Been Breached

When you experience a breach, it's important to get your staff quickly involved in fixing the problem.

- [ ] Assemble your Incident Response team
- [ ] Inform franchisees of your Incident Response Plan (IRP)
- [ ] Train franchisees of immediate and long-term actions

Get Incident Response Help →

# Preserve Evidence

Preserving the valuable forensic evidence of your data breach is essential for identifying what information was stolen and how to prevent a future breach.

- [ ] When you discover a breach, remember:
  - [ ] Don't get rid of evidence
  - [ ] Don't do anything hasty
  - [ ] Don't wipe and re-install your systems (yet)
  - [ ] Follow your incident response plan

# Contain the Breach

To contain a breach, you must isolate the affected system(s) to prevent further damage.

- [ ] Implement your IRP
- [ ] Disconnect from the Internet
- [ ] Document the entire incident
- [ ] Disable remote access capability and wireless access points
- [ ] Change access control credentials (usernames and passwords)
- [ ] Segregate all hardware devices in the payment process
- [ ] Quarantine instead of deleting (removing) identified malware
- [ ] Preserve firewall settings, firewall logs, system logs, and security logs
- [ ] Restrict Internet traffic
- [ ] Contact your merchant processing bank
- [ ] Consider hiring a law firm experienced in managing data breaches

Get Incident Response Help →

# Consider Public Communication

The public, including those whose information was breached, needs to know quickly the scope of the breach and your plan for remediation.

- [ ] Determine how and when notifications will be made
- [ ] Know legislated mandatory time frames
- [ ] Identify who is responsible for public statements
- [ ] Seek the guidance of your legal counsel
- [ ] Inform employees not to announce the breach before your company announcement
- [ ] Craft specific statements about your breach by:
  - [ ] Deciding what type of organization you are
  - [ ] Finding what mandate you should follow
  - [ ] Researching who your target audience is
    - [ ] Publish statements through all or a mixture of:
      - [ ] Social media
      - [ ] Email
      - [ ] Your website
      - [ ] Local newspapers
      - [ ] News channels
      - [ ] Mail
      - [ ] Radio announcements

# Investigate and Fix Your Systems

Once you've identified the source and have taken the proper steps to prevent a future breach, it's time to go back online.

- [ ] Bring affected systems back online
- [ ] Ensure all systems have been:
  - [ ] Hardened
  - [ ] Patched
  - [ ] Replaced
  - [ ] Tested

# Think you've had a data breach?

Get Incident Response Help →

Get Incident Response Help →



securityMETRICS®