8 STEPS TO TAKE BEFORE A CYBER INCIDENT OCCURS
Before formulating a cyber incident response plan, you should first determine which of your organizations data, assets, and services warrant the most protection.

**BEST-PRACTICE GUIDANCE ON CYBER INCIDENTS**

The U.S. Department of Justice’s "Best Practices for Victim-Response and Reporting of Cyber Incidents" outlines steps companies should take before, during, and after a cyber incident and provides a summary checklist. Included in the guidance are the Justice Department’s positions on the legal permissibility of a number of monitoring techniques and the impermissibility of many forms of "hacking back."

**8 STEPS TO TAKE BEFORE AN INCIDENT OCCURS**

The guidance emphasizes the importance of planning before an incident occurs and states that organizations should do the following:

1. **IDENTIFY YOUR CROWN JEWELS.**
   - The expense and resources required to protect an enterprise may force an organization to prioritize its efforts and may shape planning.
   - Before formulating a cyber incident response plan, an organization should first determine which data, assets, and services warrant the most protection.
   - The guidance suggests that this prioritization of protection is an important first step in preventing a cyber intrusion or an attack from causing catastrophic harm.

2. **HAVE AN ACTIONABLE PLAN**
   - Organizations should have a plan in place before an intrusion occurs.
   - This plan should provide specific, concrete procedures to follow in the event of a cyber incident.
   - The procedures should address these points:
     - Who has lead responsibility for different elements of an organization's response?
     - How to contact critical personnel at any time.
     - How to proceed if critical personnel are unreachable.
     - What mission-critical data, networks, or services should be prioritized.
     - How to preserve data related to the intrusion in a forensically sound manner.
• Which criteria will be used to ascertain whether data owners, customers, or partner companies should be notified?
• Procedures for notifying law enforcement and others.

3. HAVE APPROPRIATE TECHNOLOGY AND SERVICES IN PLACE
• This may include off-site data backup, intrusion-detection capabilities, and data loss prevention technologies. The technology should already be installed, tested, and ready to deploy.

4. HAVE APPROPRIATE AUTHORIZATION TO PERMIT NETWORK MONITORING
• An organization should adopt the mechanisms necessary for obtaining user consent to monitor users' communications so it can detect and respond to a cyber incident.

5. ENSURE LEGAL COUNSEL IS FAMILIAR WITH TECHNOLOGY AND CYBER INCIDENT MANAGEMENT
• Having readily available access to advice from lawyers well acquainted with cyber incident response can speed up an organization's decision making and help ensure that a victim organization's incident response activities remain on firm legal footing.

6. ENSURE ORGANIZATION POLICIES ALIGN WITH THE INCIDENT RESPONSE PLAN
• An organization should review its personnel and human resource policies to ensure they will reasonably minimize the risk of cyber incidents, including "insider threats." Proper personnel and IT policies may help prevent a cyber incident.

7. ENGAGE WITH LAW ENFORCEMENT BEFORE AN INCIDENT OCCURS
• Having a point of contact and a preexisting relationship will facilitate any subsequent interaction that may occur if an organization needs to enlist assistance from law enforcement agencies. On a federal level, these include the Federal Bureau of Investigation and the U.S. Secret Service.
8. ESTABLISH INFORMATION-SHARING RELATIONSHIPS

- Information-sharing organizations exist to provide details on new or commonly exploited vulnerabilities. Information Sharing and Analysis Centers have been created in each critical infrastructure sector.

RESPONDING TO AN INTRUSION

The guidance suggests that organizations first assess the nature and scope of the incident and determine whether it is an attack or just a technical glitch. If the incident is an intrusion or attack, the organization may consider rerouting network traffic, filtering or blocking a distributed denial-of-service attack or isolating all or parts of the compromised network.

The organization should preserve relevant forensic images and logs and notify relevant law enforcement agencies and other potential victims. Organizations are advised not to use compromised systems to communicate. Also, a victimized organization should not attempt to access, damage, or impair another system that may appear to be involved in the attack.

AFTER AN ATTACK OR INTRUSION

Once a victim organization has recovered from an attack, it should initiate measures to prevent similar attacks. In addition, it should conduct a post-incident review of the response and assess strengths and weaknesses of its performance. Response gaps and weaknesses should be noted and discussed, and necessary remedial action taken.
ABOUT RMA

The Risk Management Association (RMA) is a not-for-profit, member-driven professional association serving the financial services industry. Its sole purpose is to advance the use of sound risk principles in the financial services industry. RMA promotes an enterprise approach to risk management that focuses on credit risk, market risk, operational risk, securities lending, and regulatory issues.

Founded in 1914, RMA was originally called the Robert Morris Associates, named after American patriot Robert Morris, a signer of the Declaration of Independence. Morris, the principal financier of the Revolutionary War, helped establish our country’s banking system.

Today, RMA has approximately 1,900 institutional members. These include banks of all sizes as well as nonbank financial institutions.

RMA is proud of the leadership role its member institutions take in the financial services industry. Relationship managers, credit officers, risk managers, and other financial services professionals in these organizations with responsibilities related to the risk management function represent these institutions within RMA. Known as RMA Associates, these 18,500 individuals are located throughout North America and financial centers in Europe, Australia, and Asia.

No part of this publication may be reproduced, by any technique or process whatsoever, without the express written permission of the publisher.

Phone: 800-677-7621
Fax: 215-446-4101
Website: www.rmahq.org