Incident Response Plan Guide

DISCLAIMER

This plan is not intended to be an all-inclusive incident response or cyber security plan.

Instead, it is a guide to highlight some of the key concerns and action items that should be taken into consideration when planning for the eventuality of a breach incident.

The reader should also consult with IT, legal, and public relations professionals, among others, in the preparation process

Prepared by:

ASSUREtrust™

INSUREtrust's digital security arm, ASSUREtrust, can provide a full range of IT security services.

www.insuretrust.com/assuretrust • Phone 770-200-8000 • Toll Free 888-WEB-RISK • Fax 770-200-8001

5185 Peachtree Parkway • Suite 230 • Norcross, GA 30092

SECTION I. PRE-INCIDENT RESPONSE

1. PURPOSE.

This Pre-Incident Response Plan outlines precautionary measures and planning steps to be taken in advance of an incident. The plan is intended to serve as a guideline in developing a pre and post-incident response strategy and ensuring all involved parties are identified. It is important to remember that an incident is not limited to a data breach, but could also include data leakage, service interruption, or other incidents that are counterproductive to your business.

2. PREPAREDNESS.

It is important to establish an incident response plan to ensure your company is ready to quickly respond to an incident, while minimizing the potential damage. The plan should be reviewed every year to ensure the information is current and relevant.

- ☐ IT team conducts regular penetration testing on the network to ensure its integrity and identify any potential vulnerability.
- ☐ Contract an outside vendor to conduct further, independent-party penetration testing.*
- ☐ Ensure backups are kept current to restore your system and verify file integrity.
- ☐ Conduct periodic disaster recovery drills so everyone is trained on procedure and locating key documents and equipment. Use a different scenario during each drill to maintain realism.
- ☐ Have internal or external audits done regularly to ensure the safety of the systems or network.*

2.1. Management plays a key role in establishing a security-conscious workplace and emphasizing the serious ramifications of a data breach.

- ☐ Key employee(s) should participate in cyber risk management training.*
- ☐ Undergo a process to determine significant cyber risk exposures, including a third-party security audit.*

** This service is available from INSUREtrust or one of its Vendor Partners.*

ASSUREtrust™

2.2. INCIDENT RESPONSE TEAM (IRT).

Name	Role	Work Phone	Cell Phone
1.			
2.			
3.			
4.			
5.			
6.			

2.3. STAKEHOLDERS.

In the event of a breach, stakeholders identified in the Pre-Incident Response Plan should be notified in the order shown. If you are unable to reach someone, leave a message and proceed to the next name on the list.

Name	Title/Position	Work Phone	Cell Phone
1.			
2.			
3.			
4.			
5.			
6.			

2.4. OFF-SITE DATA STORAGE.

Establish a vendor management plan in the event that data stored with an off-site vendor is breached. If possible, negotiate an indemnification provision that addresses losses that are the vendor's fault.

Storage Facility:	
Address:	
Primary Contact:	
Phone:	
Alternate Contact:	
Phone:	

ASSUREtrust™

3. SECURITY ASSESSMENT.

Establish a vendor management plan in the event that data stored with an off-site vendor is breached. If possible, negotiate an indemnification provision that addresses losses that are the vendor's fault.

How many records containing sensitive data does company have?	
Are the following types of PII stored in company's network?	
■ Names and addresses	
■ Social Security numbers	
■ Health information	
■ Payment information (credit cards numbers, bank account numbers, etc.)	
■ Other sensitive client information	
■ Company proprietary information, trade secrets, contracts, etc.	
How many external IP addresses does the company have?	
How many firewalls does the company have?	
How many externally facing web sites does the company have?	
Does the company have web site which allows users to input data?	
Is sensitive data (i.e, credit card or personally identifiable information) a part of the web site application?	

4. SECURITY AND ACCESS CONTROL.

Adhering to basic security protocols for your network will increase the security of your data. Keep in mind, some insurance carriers now require sensitive data stored on your network to be encrypted in order to receive coverage. Ensure you are in compliance with items below.

- ☐ Operating systems on all computers with access to network receive all security patches as soon as is practical.
- ☐ Antivirus software is in place on all computers and servers.
- ☐ ID/password authentication is required to access the network. Access to sensitive data is limited to employees with a need to know.
- ☐ Passwords, including those for wireless networks, are complex and change at least every 90 days.
- ☐ Encryption is in place on all data in transit as well as for all sensitive data at rest (Note: Some states regulate how sensitive information is encrypted, so know applicable laws.)
- ☐ Encryption is in place for all portable storage devices that contain sensitive information (i.e., flash drives, tablets, laptops, and cell phones).
- ☐ Procedures exist to obtain any data/information assets back from exiting employees and/or independent contractors. Credentials for exiting employees are removed immediately.
- ☐ A data destruction plan dictates retention timelines for electronic data.

5. BREACH DETECTION / RECOVERY.

The IT team should continually monitor your network logs for signs of any unusual activity or a breach.

- ☐ Back up all data on a daily basis at one or more locations, and keep backup tapes in a secure location separate from your server.
- ☐ Conduct a periodic inventory of the volume, types, and locations of sensitive data.
- ☐ Identify potential threat categories to devise an appropriate response plan.*

5.1. COMMON THREATS.

Some common incident categories are listed below. At a minimum, your security plan should address all of these.

- ✓ Malware (virus, Trojan horse, worm, etc.)
- ✓ Breach of firewall
- ✓ Privilege escalation
- ✓ Human threats (phishing, spoofing, leaked data, etc.)
- ✓ Spyware
- ✓ Denial of service attack

5.2. CUSTOMER CONTACT INFORMATION.

It is crucial that you ensure customer contact information is kept current and is in a usable format. Only keep customers' personal information in your system/database as long as you need it. In the event that customer data is compromised, you will have to notify those affected or potentially affected.

5.3. USEFUL CONTACT NUMBERS.

Don't wait until there is a data breach to establish a contact list of service providers. The situation will likely be chaotic and resources stretched thin.

SERVICE PROVIDED	Company / Contact Name	Contact Number
Insurance Agent/Agency		
Insurance Broker	INSUREtrust	888-WEB-RISK
Insurance Carrier		
IT Consulting Firm		
Public Relations Manager		
State Attorney General		
Local Law Enforcement		
Other		

5.4. DOCUMENTATION.

Educate your employees on how to properly document during an incident to make sure important findings are not missed or misunderstood post incident. All documents should be time stamped and include any commands entered into the system, actions taken, and observations.

** This service is available from INSUREtrust or one of its Vendor Partners.*

ASSUREtrust™

SECTION II. POST-INCIDENT RESPONSE

For the purposes of this document, we identify the four phases of incident response as follows: Discovery and Alert, Containment and Assessment, Response, and Recovery. Once a breach has occurred, contact your insurance agent and INSUREtrust for further information on post breach advice and consultation.

1. DISCOVERY AND ALERT.

The discovery phase begins with the identification of a threat. Threat detection can include but is not limited to an alert from an Intrusion Detection System (IDS), breach of the firewall detection, an alarm from a network monitoring system, antivirus alerts, or discovery of cyberfraud (such as phishing, spoofing, etc.).

2. CONTAINMENT AND ASSESSMENT.

Once a threat has been identified, the IRT should take necessary measures to contain the threat. Determine the severity of the incident (denial of service attack, compromised personal data, etc.). If possible, identify the source of the attack. If you are insured, notify your agent in writing, and ask that the agent notify the carrier per policy requirements.

3. RESPONSE.

It is not advisable to reboot your servers immediately following an incident because you will lose any information that could potentially help you identify the source and methodology of the attack. Make an initial damage assessment to determine the appropriate response measures. Notify the IRT and Stakeholders identified in the Pre-Incident Response Plan.

3.1. DATA BREACH.

In the event of a data breach, notify your agent, who can access resources from INSUREtrust.

4. RECOVERY.

Once you have ensured your system has been secured and any threats have been removed, restore your system to pre-incident operating condition (malware may have been installed to modify your system files).

- ☐ If necessary, perform a rebuild of your system.
- ☐ Reconfigure your network security features and test the system to ensure proper operation.
- ☐ INCIDENT CONTAINMENT. Coordinate with necessary entities to handle:
  - Data restoration
  - Third-party lawsuits
  - Breach of contract lawsuits (NDAs)
  - Regulatory fines and penalties
  - Breach notification costs
  - Content lawsuits
  - Computer forensics
  - Business interruption
  - Crisis management/public relations/brand restoration
  - Extortion

5. CLOSURE AND LESSONS LEARNED

Once all systems have been restored back to original pre-incident nature, make sure all that proper documentation has been completed. This includes any findings for future litigation, as well as documentation that could aid in learning better response techniques and in reducing vulnerabilities, should a future incident occur. The IRT should then have a Post-Incident meeting to discuss what issues could have been handled better in the Pre and Post-Incident process. Finally, check for any gaps within the IT security policy.

OTHER DOCUMENTS IN THIS SERIES THAT ARE USEFUL IN DEVELOPING A COMPREHENSIVE APPROACH TO DATA PRIVACY AND SECURITY:

IT Security Policy Guide

Social Media Policy Guide

ASSUREtrust™