GOVERNOR ERIC J. HOLCOMB'S
INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY
302 West Washington Street, IGC-South, Room E208
Indianapolis, IN 46204

Author: Dobran, Bojana

Title: "Upgrade Your Security Incident Response Plan (CSIRP) : 7 Step Checklist"

Website: phoenixnap.com

Organization: phoenixNAP Global IT Services

Date: 10 March 2019

URL: https://phoenixnap.com/blog/cyber-security-incident-response-plan

Accessed: 21 Oct 2019

Synopsis: In this article you will learn:

- Why every organization needs a cybersecurity incident response policy for business continuity.
- The Seven critical security incident response steps (in a checklist) to mitigate data loss.
- What should be included in the planning process to ensure business operations are not interrupted?
- Identify which incidents require attention & When to initiate your response.
- How to use threat intelligence to avoid future incidents.

Upgrade Your Security Incident Response Plan (CSIRP) : 7 Step Checklist

MARCH 10, 2019 | IN SECURITY STRATEGY, DATA PROTECTION, DISASTER RECOVERY | BY BOJANA DOBRAN

In this article you will learn:

- Why every organization needs a cybersecurity incident response policy for business continuity.
- The Seven critical security incident response steps (in a checklist) to mitigate data loss.
- What should be included in the planning process to ensure business operations are not interrupted?
- Identify which incidents require attention & When to initiate your response.
- How to use threat intelligence to avoid future incidents.

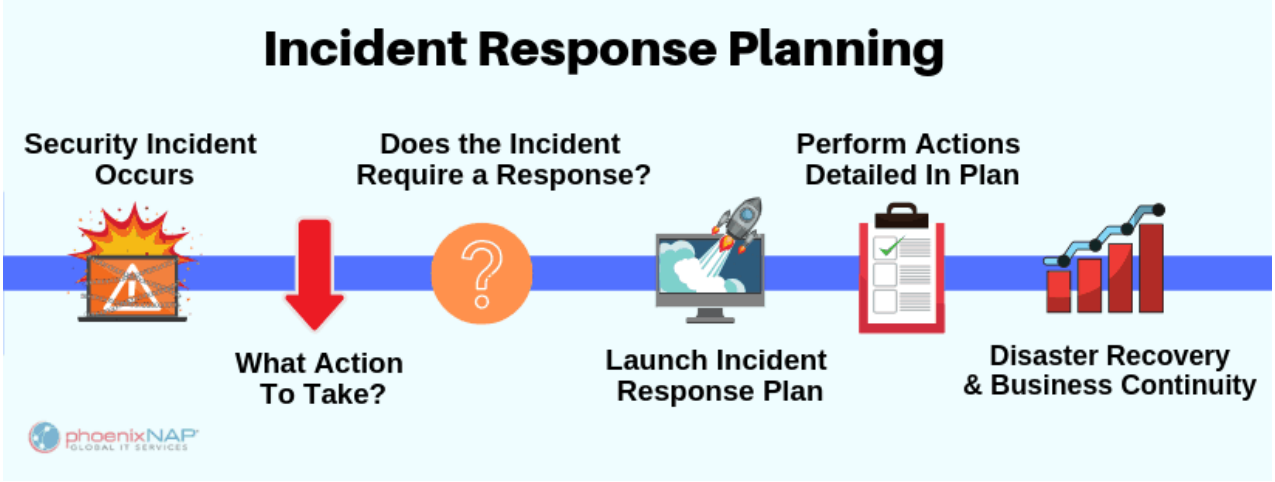
What if your company's network was hacked today? The business impact could be massive.

Are you prepared to respond to a data security breach or cybersecurity attack? In 2019, it is far more likely than not that you will go through a security event.

If you have data, you are at risk for cyber threats. Cybercriminals are continually

developing new strategies to breach systems. Proper planning is a must. Preparation for these events can decrease the damage and loss you and your stakeholder's.

Having a clear, specific, and current cybersecurity incident response plan is no longer optional.



Cyber incident plan flow chart

What is an Incident Response Plan?

An incident response (IR) plan is the guide for how your organization will react in the event of a security breach.

Incident response is a well-planned approach to addressing and managing reaction after a cyber attack or network security breach. The goal is to minimize damage, reduce disaster recovery time, and mitigate breach-related expenses.

Definition of the Incident response life cycle.

Cybersecurity Incident Response Checklist, in 7 Steps

During a breach, your team won't have time to interpret a lengthy or tedious action plan.

Keep it simple; keep it specific.

Checklists are a great way to capture the information you need while staying compact, manageable, and distributable. Our checklist is based on the 7 phases of incident response process which are broken down in the infographic below.

1 CONDUCT A COMPLETE RISK ASSESSMENT

The primary purpose of a risk assessment is to identify likelihood vs. severity of risks in critical areas.. Make sure it is always current.

2 IDENTIFY KEY TEAM MEMBERS & STAKEHOLDERS

Name your stakeholders and those with decision-making authority. This could include senior management, customers, and business partners.

3 DEFINE SECURITY INCIDENT TYPES

You need to know exactly when to initiate your security incident response. Your plan should define what counts as an incident and who is in charge of activating the plan.

4 INVENTORY RESOURCES & ASSETS

Your company has systems and resources available. Make the most of all of your departments and teams.. Create a list of these assets.

5 PLAN HIERARCHY OF INFORMATION FLOW

Take a look at your assets above. What are the steps that need to happen to execute different processes?

Share this Image On Your Site, Copy & Paste

```
</p><br /><p><strong>Please include attribution to phoenixnap.com with this graphic.</strong></p><br /><p><a href='https://phoenixnap.com/blog/cyber-security-incident-response-plan'><img src='https://phoenixnap.com/blog/wp-content/uploads/2019/03/csirt-checklist.png' alt='CSIRT Incident Checklist' width='800px' border='0' /></a></p><br /><p>
```

1. Focus Response Efforts with a Risk Assessment

If you haven't done a potential incident risk assessment, now is the time. The primary purpose of any risk assessment is to identify likelihood vs. severity of risks in critical areas. If you've done a cybersecurity risk assessment, make sure it is current and applicable to your systems today. If It's out-of-date, perform another evaluation.

Examples of a high-severity risk are a security breach of a privileged account with access to sensitive data. This is especially the case if the number of affected users is high. If the likelihood of this risk is high, then it demands specific contingency planning in your IR plan. The Department of Homeland Security provides an excellent Cyber Incident Scoring System to help you assess risk.

Use your risk assessment to identify and prioritize severe, likely risks. Plan

appropriately for medium and low-risk items as well. Doing this will help you avoid focusing all your energy on doomsday scenarios. Remember, a “medium-risk” breach could still be crippling.

2. Identify Key Team Members and Stakeholders

Identify key individuals in your plan now, both internal and external to your CSIRT. Name your stakeholders and those with decision-making authority. This could include senior management, customers, and business partners.

Document the roles and responsibilities of each key person or group. Train them to perform these functions. People may be responsible for sending out a PR statement, activating procedures to contact authorities, or performing containment activities to minimize damage from the breach.

Store multiple forms of contact information both online and offline. Plan to have a variety of contact methods available (don’t rely exclusively on email) in case of system interruptions.

3. Define Incident Types and Thresholds

You need to know exactly when to initiate your IT security incident response. Your response plan should define what counts as an incident and who is in charge of activating the plan.

Know the kinds of cybersecurity attacks that can occur — stay-up-to-date on the latest trends and new types of data breaches that are happening.

Defining potential security incidents can save critical time in the early stages of breach detection. The stronger your CSIRT’s working knowledge of incident types and what they look like, the faster you can invoke a targeted active response.

Educate those outside your CSIRT, including stakeholders. They should also be familiar with these incident definitions and thresholds. Establish a clear communication plan to share information amongst your CSIRT and other key individuals to convey this

information.

4. Inventory Your Resources and Assets

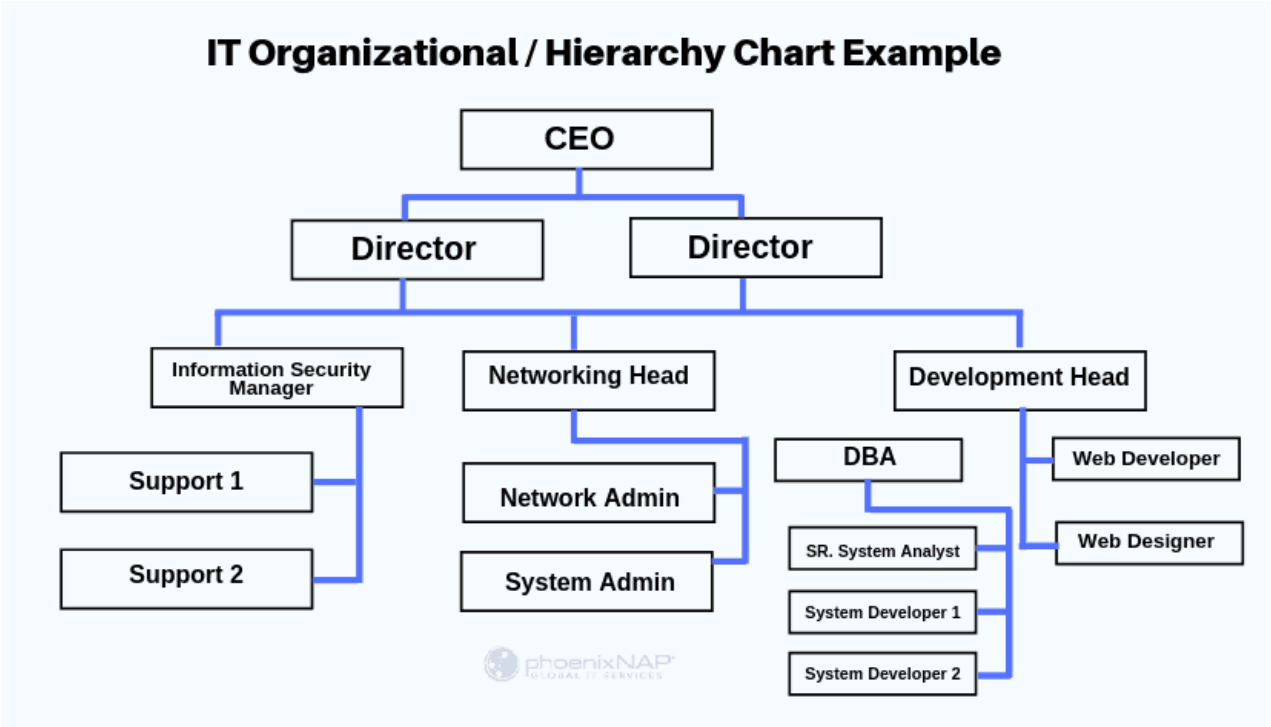
IR response depends on coordinated action across many departments and groups. You have different systems and resources available, so make the most of all of your departments and response teams.

Create a list of these assets, which can include:

- Business Resources: Team members, security operations center departments, and business partners are all businesses resources. These should consist of your legal team, IT, HR, a security partner, or the local authorities.
- Process Resources: A key consideration is to evaluate the processes you can activate depending on the type and severity of a security breach. Partial containment, “watch and wait” strategies, and system shutdowns like web page deactivation are all resources to include in your IR plan.

Once you have inventoried your assets, define how you would use them in a variety of incident types. With careful security risk management of these resources, you can minimize affected systems and potential losses.

5. Recovery Plan Hierarchies and Information Flow



Take a look at your assets above.

What are the steps that need to happen to execute different processes? Who is the incident response manager? Who is the contact for your security partner?

Design a flowchart of authority to define how to get from Point A to Point B. Who has the power to shut down your website for the short term? What steps need to happen to get there?

Flowcharts are an excellent resource for planning the flow of information. NIST has some helpful tools explaining how to disseminate information accurately at a moment's notice. Be aware that this kind of communication map can change frequently. Make special plans to update these flowcharts after a department restructure or other major transition. You may need to do this outside your typical review process.

6. Prepare Public Statements

Security events can seriously affect an organizations reputation. Curbing some of the adverse effects around these breaches has a lot to do with public perception. How you interface with the public about a potential incident matters.

Some of the best practices recognized by the IAPP include:

- Use press releases to get your message out.
- Describe how (and with whom) you are solving the problem and what corrective action has been taken.
- Explain that you will publish updates on the root cause as soon as possible.
- Use caution when talking about actual numbers or totalities such as “the issue is completely resolved.”
- Be consistent in your messaging
- Be open to conversations after the incident in formats like Q&A’s or blog posts

Plan a variety of PR statements ahead of time. You may need to send an email to potentially compromised users. You may need to communicate with media outlets. You should have statement templates prepared if you need to provide the public with information about a breach.

How much is too much information? This is an important question to ask as you design your prepared PR statements. For these statements, timing is key – balance fact-checking and accuracy against timeliness.

Your customers are going to want answers fast, but don’t let that rush you into publishing incorrect info. Publicizing wrong numbers of affected clients or the types of data compromised will hurt your reputation. It’s much better to publish metrics you’re sure about than to mop up the mess from a false statement later.

7. Prepare an Incident Event Log

During and after a cybersecurity incident, you are going to need to track and review multiple pieces of information. How, when, and where the breach was discovered and addressed? These details and all supporting info will go into an event log. Prepare a template ahead of time, so it is easy to complete.

This log should include:

Location, time, and nature of the incident discovery
- Communications details (who, what, and when)
- Any relevant data from your security reporting software and event logs

After an information security incident, this log will be critical. A thorough and effective incident review is impossible without a detailed event log. Security analysts will lean on this log to review the efficacy of your response and lessons learned. This account will also support your legal team and law enforcement both during and after threat detection.

How Often Should You Review Your Incident Response Procedures?

To review the steps in your cybersecurity incident response checklist, you need to test it. Run potential scenarios based on your initial risk assessment and updated security policy.

Perhaps you are in a multi-user environment prone to phishing attacks. Your testing agenda will look different than if you are a significant target for a DDoS attack. At a minimum, annual testing is suggested. But your business may need to conduct these exercises more frequently.

Planning Starts Now For Effective Cyber Security Incident Response

If you don't have a Computer Security Incident Response Team (CSIRT) yet, it's time to make one. The CSIRT will be the primary driver for your cybersecurity incident response plan. Critical players should include members of your executive team, human resources, legal, public relations, and IT.

Your plan should be a clear, actionable document that your team can tackle in a variety of scenarios, whether it's a small containment event or a full-scale front-facing site interruption.

Protecting your organization from cybersecurity attacks is a shared process.

Partnering with the experts in today's security landscape can make all the difference between a controlled response and tragic loss. Contact PhoenixNAP today to learn more about our global security solutions.

Recent Posts

- Microservices: Importance of Continuous Testing with Examples
- Defining a Data Breach and How to Prevent One
- NSX-V vs NSX-T: Discover the Key Differences
- Cloud-Native Application Architecture: The Future of Development?
- What is Managed Hosting? Top Benefits For Every Business

Bojana Dobran

Sr. Marketing Specialist at phoenixNAP. Researcher and writer in the fields of cloud computing, hosting, and data center.

YOU MAY ALSO BE INTERESTED IN:

- Information Security Risk Management: Plan, Steps, & Examples
- What is a Security Operations Center (SOC)? Best Practices, Benefits, & Framework
- RTO (Recovery Time Objective) vs RPO (Recovery Point Objective)
- Definitive 7 Point Disaster Recovery Planning Checklist
- Business Continuity vs Disaster Recovery: What's The Difference?
- 2019 Disaster Recovery Statistics That Will Shock Business Owners