It’s Not If But When: How to Build Your Cyber Incident Response Plan

Lucie Hayward, Managing Consultant
Michael Quinn, Associate Managing Director

EACH DAY SEEMS TO BRING NEWS OF YET ANOTHER COMPANY DEALING WITH A DATA BREACH. Personally, your first reaction might be to make sure that your data is not among the information compromised. But after that, are you professionally worried because you don't know — at least, not with any amount of certainty — how your company will respond if your network is hacked?

One of the best ways to gain some peace of mind when it comes to data breaches is to create and regularly test an incident response plan (IRP). Creating an IRP does not have to be a lengthy, intimidating process. In fact, according to the National Institute of Standards and Technology (NIST), an IRP simply provides "the instructions and procedures an organization can use to identify, respond to, and mitigate the effects of a cyber incident."[1]

In this article, we will provide a high-level view of how to build an IRP and the types of questions you will want to address as you begin planning.

Getting Your Terminology Right

Incident, event, breach … they all mean the same thing, right? Actually, no, not at all.

NIST defines a **computer incident** as a "violation, or imminent threat of violation, of computer security policies, acceptable use policies, or standard security practices." While NIST's definition is a good starting point, many organizations find that it is too broad for their business.

Therefore, it is probably more useful to expand the NIST definition of an incident to any "violation, or imminent threat of violation, of computer security policies, acceptable use policies, or standard security practices **that has significant potential to lead to:**

- **Negative impact to the company's reputation**
- **Inappropriate access to PII, PHI, or customer data**
- **Loss of intellectual property or funds**

So how is a **computer event** different from an incident? According to NIST, "An event is any observable occurrence in a system or network." For our purposes, what is more helpful is that NIST defines adverse computer events as "… events with a negative consequence, such as system crashes, packet floods, unauthorized use of system privileges, unauthorized access to sensitive data, and execution of malware that destroys data."

Now we come to the term **breach**. A breach generally describes when an organization has lost control of certain types of sensitive data, i.e., PII, PHI, or customer data. Be very careful when using the word breach in communications around an incident, and speak with your counsel before issuing any public statements.

Assembling Your Incident Response Team (IRT)

As you prepare to develop your IRP, you should also assemble your incident response team (IRT). Generally, the following professionals should be part of your IRT to ensure coverage of specific incident-related issues:

- General Counsel (Legal)
- Chief Information Security Officer or Chief Information Officer (Management)
- Technical Leads (such as Security, Network, or Infrastructure)
- Human Resources
- Public Relations/Marketing
- Risk Management/Insurance
- Business Subject Matter Experts (as needed)

Although it is common to have one single team, another option is to create a core team and bring on ad hoc members as needed. Also, be sure to assign alternate members with decision-making authority should a team member be unavailable when an incident arises.

[1] NIST SP 800-34 Rev.1 Contingency Planning Guide for Federal Information Systems

Building Your IRP – Seven Important Steps

The following activities are based on best practices that Kroll has developed helping organizations build their IRPs.

1

Determine authority to call an incident. Your IRP should clearly state who has the authority to declare an incident. As soon as this person or team declares an incident, it should automatically invoke the IRP and convene the incident response team (IRT).

2

Assign IRT responsibilities. Outline the roles of everyone on the IRT, and clearly define each team member's responsibilities. In the event of an incident, having this clarity will minimize confusion when tough decisions will need to be made.

3

Do not assign severity levels. While it may seem initially helpful to describe categories of severity and ramp up the response accordingly, the risk is too great that an incident can be mislabeled. Every declared incident should be considered a top priority, with all hands on deck.

4

Establish communications procedures and responsibilities. Determine how communication will flow. For example, how will the IRT communicate securely:

- Where will you meet (war rooms)?
- Is it safe to use corporate email?
- What should be communicated verbally, what should be written?

Additionally, assign who will communicate with external parties, such as outside counsel, your insurance carrier, law enforcement, the media, and regulators. Likewise, decide who will report to company executives and the board of directors/trustees.

5

Gather pertinent information. Where possible, have critical information compiled in preparation for an incident. For example, being able to quickly access network and critical application diagrams can help your team quickly begin the investigation.

It is also important to gather and centrally store contact information, to include after-hours numbers, for members of the IRT, their alternates (back-ups), and key stakeholders, such as executives and legal counsel. You should also include information for critical vendors or service providers. Incidents don't always happen when it's convenient, and this will allow you to quickly reach key resources, even when out of business hours.

6

Outline the process. It is human nature for teams that are responsible for various systems to want to try and fix something before having to escalate the problem. Unfortunately, because the dwell time from when a problem is detected to the time when response starts is increasingly important, this behavior has hurt many an organization.

Clearly indicate when the team must be convened and outline in detail all the steps in the process, including escalation points. Start with the incident report and end with lessons learned. While you should not get bogged down with internal status reports, make sure the IT and Security teams know this process by heart and do not delay in reporting a problem.

7

Review and test the plan. Review the plan quarterly and make updates accordingly. For example, pay special attention to any technology, policies, or roles that may have changed in the intervening time. Also ensure that contact information has been updated for your team members and outside resources. After initially testing your plan, schedule annual tests to identify any gaps.

For an initial test, a tabletop exercise can be a very enlightening process because it demonstrates the readiness of your organization to respond to cyber incidents. The key objectives in the tabletop exercise are:

- Identify gaps in the current IRP
- Strengthen communication between stakeholders
- Familiarize all participants with key definitions and decision-making criteria
- Enable participants to adapt this IRP to the dynamic nature of cyber incidents

Outside experts such as Kroll, with significant experience in helping clients prevent, prepare for, and manage breaches, can facilitate both the development of your IRP/IRT as well as the tabletop exercises.

In today's busy world, we understand that it can be difficult for professionals to dedicate time to a simulation exercise. However, experiencing a data breach without an incident response plan and without an incident response team will be a much longer process — and often carries more significant damage to your company and its reputation. In these days when all networks are under constant attack, having an IRP can help you and your company manage a cyber incident with confidence.

About Kroll

Kroll is the leading global provider of risk solutions. For more than 40 years, Kroll has helped clients make confident risk management decisions about people, assets, operations, and security through a wide range of investigations, cyber security, due diligence and compliance, physical and operational security, and data and information management services. Headquartered in New York with more than 50 offices across nearly 30 countries, Kroll has a multidisciplinary team of over 2,000 employees and serves a global clientele of law firms, financial institutions, corporations, non-profit institutions, government agencies, and individuals.

These materials have been prepared for general information purposes only and do not constitute legal or other professional advice. Always consult with your own professional and legal advisors concerning your individual situation and any specific questions you may have.

CONTACT

Lucie Hayward | Managing Consultant
lucie.hayward@kroll.com | +1 615.577.6726

Michael Quinn | Associate Managing Director
michael.quinn@kroll.com | +1 202.384.6946

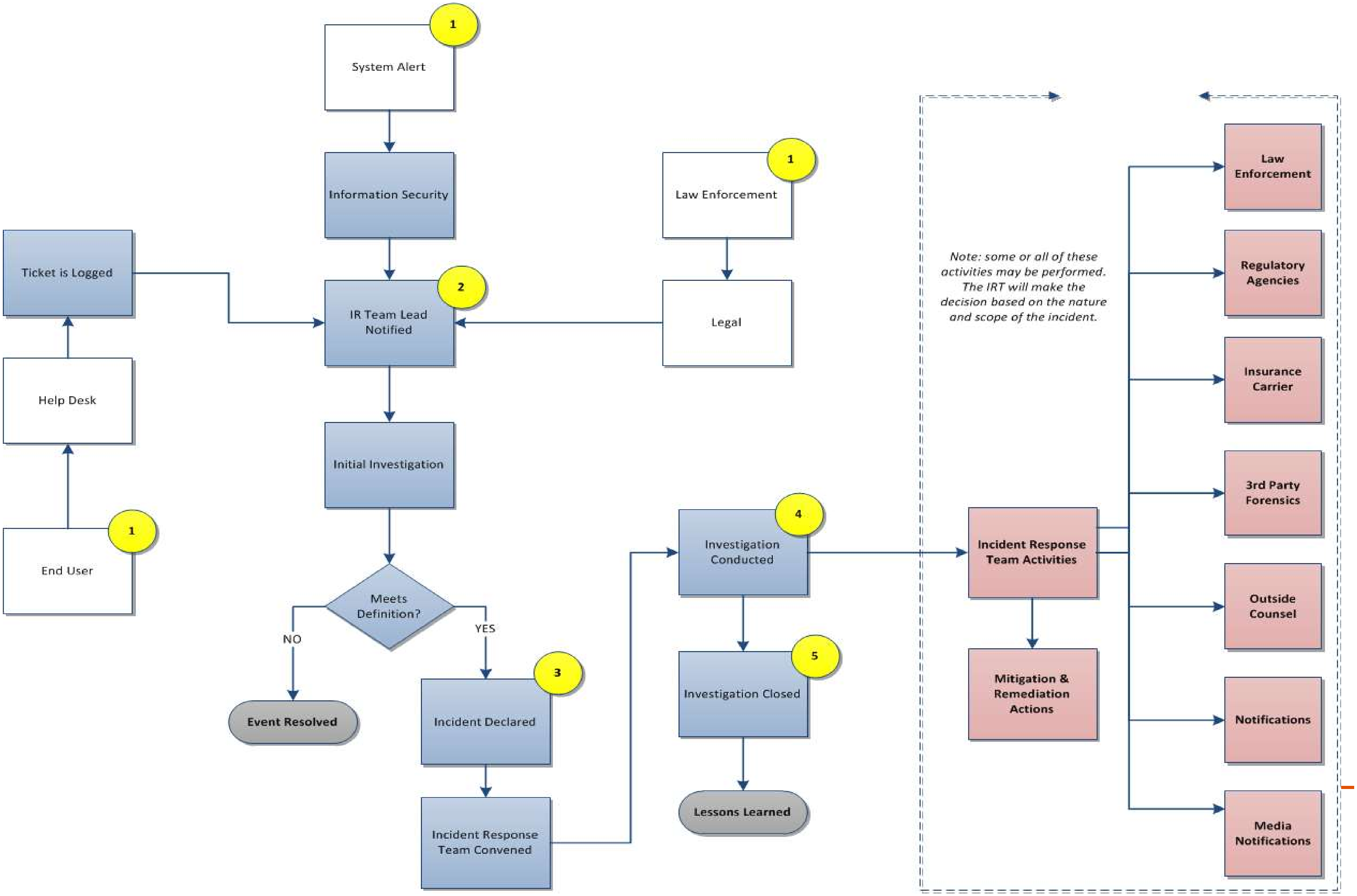
kroll.com

Definition

A *computer security incident* is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices, that *has significant potential* to lead to the following:

- Negative impact to the company's reputation
- Inappropriate access to PII or PHI or customer data
- Loss of IP or Funds

Incident Response Plan (IRP)



1 System Alert

Information Security

1 Law Enforcement

Legal

Ticket is Logged

2 IR Team Lead Notified

Help Desk

1 End User

Initial Investigation

Meets Definition?

NO

Event Resolved

YES

3 Incident Declared

Incident Response Team Convened

4 Investigation Conducted

5 Investigation Closed

Lessons Learned

Note: some or all of these activities may be performed. The IRT will make the decision based on the nature and scope of the incident.

Incident Response Team Activities

Mitigation & Remediation Actions

Law Enforcement

Regulatory Agencies

Insurance Carrier

3rd Party Forensics

Outside Counsel

Notifications

Media Notifications