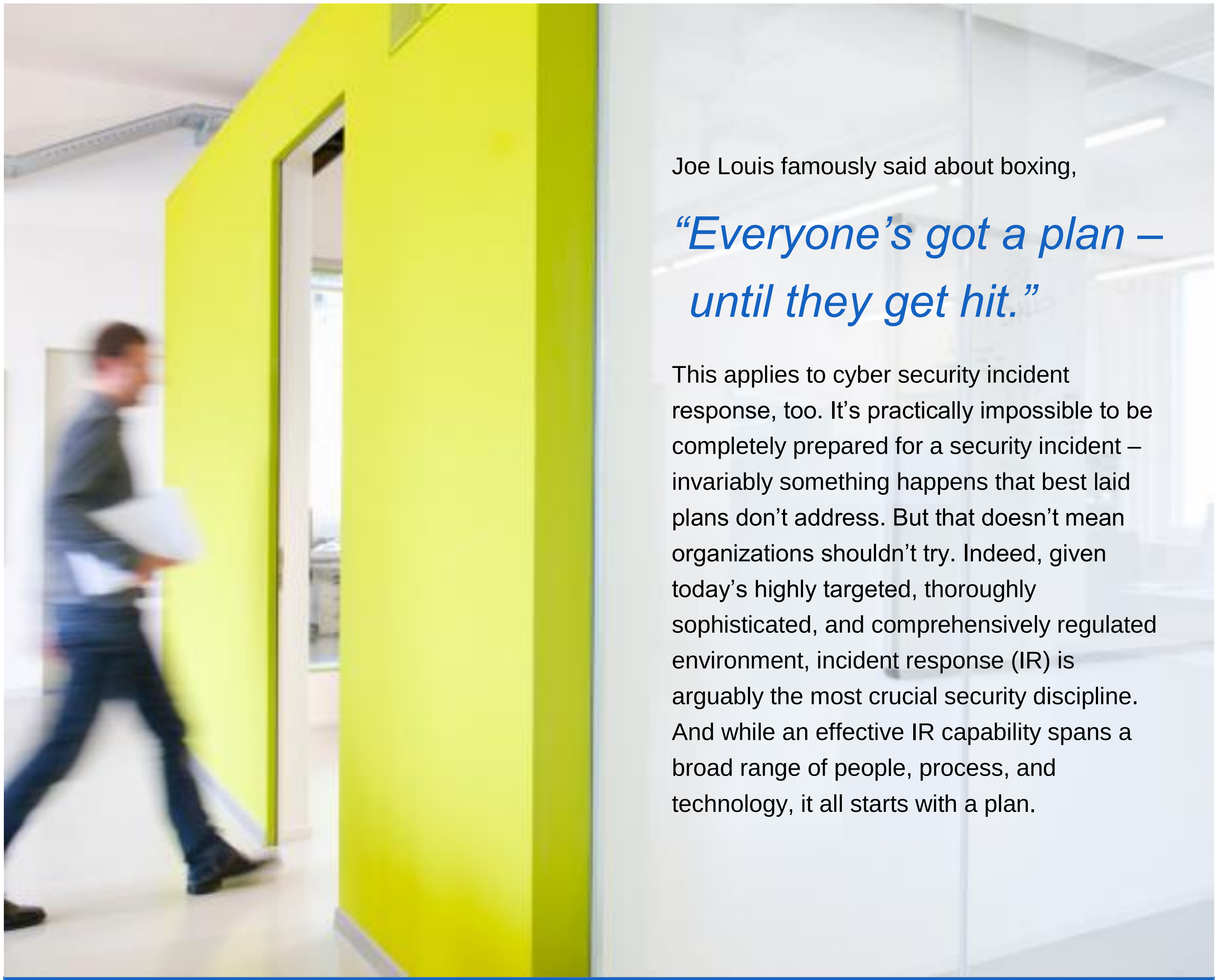
RESILIENT SYSTEMS AND HP WHITE PAPER

5 Steps to Improve Your Cyber Security Incident Response Plan

Richard White, Principal
HP Security Intelligence and Operational Consulting,
MBA CISSP CHP/CHSS

Ted Julian, VP of Product Management & Co-Founder
Resilient Systems



Joe Louis famously said about boxing,

“Everyone’s got a plan – until they get hit.”

This applies to cyber security incident response, too. It’s practically impossible to be completely prepared for a security incident – invariably something happens that best laid plans don’t address. But that doesn’t mean organizations shouldn’t try. Indeed, given today’s highly targeted, thoroughly sophisticated, and comprehensively regulated environment, incident response (IR) is arguably the most crucial security discipline. And while an effective IR capability spans a broad range of people, process, and technology, it all starts with a plan.

This white paper will review five steps organizations can take to improve their IR plans.

Step 1
Determine if there really is an incident

Step 2
Establish who is in charge

Step 3
Test and improve the plan

Step 4
Evaluate communications

Step 5
Measure the impact

Why you need an incident response plan

With security incidents increasing not only in volume, but also in complexity, and – unfortunately – damage, having a solid, reliable incident response plan and process specific to each individual organization seems like a no-brainer. After all, according to Ponemon institute, the average cost of data breach in the U.S. is over $5.4 million. There are a few factors that can positively impact this cost, and having an incident response is one of the most significant ones, with potential to decrease it by 15%.

Furthermore, according to a Ponemon Institute survey of privacy leaders in U.S.-based corporations, 81% of respondents indicated a need for an automated tool or system to deal with the data breach incident management process. Yet, only 23% have increase spending on incident response programs.

Why is that? At least in part, it's because the industry is shifting from a prevention and detection oriented mindset, to one that embraces response. After all, if breaches are inevitable then effective incident response is crucial to minimizing the impact of incidents when they happen. This is exactly what an incident response plan can address.

If you have an incident response plan, that's a great start. But keep in mind that no plan is perfect. Incident response plans require extensive documentation, testing, and validation before they can be called reliable. On top of that, incident response plans go stale over time, and must be refreshed annually, or whenever the organization makes any major changes.

Use the five steps described in this white paper to assess and improve your existing incident response plan – or write a brand new one.

Step 1
Determine if there really is an incident

Incidents rarely emerge fully formed. Rather they start as a set of indicators, often described as an event, that through investigation may turn into an incident that requires follow up, or not. The response plan should include a policy that sets the parameters, severity, and standards for when and how an incident is declared. This will define the criteria for a major and minor incident type and set the required procedures to be followed after each type of incident. Be sure to include any third party or vendor incident response procedures if they are likely to be involved.

When an incident is declared it should be assigned a severity level with an associated severity level assessment (SLA). SLAs must be standardized across the organization and can include response time definitions. Conflicts during an incident should be avoided at all costs by establishing a dispute resolution process when SLAs and severity definitions collide.

Redundancy of communications is a must due to the uncertainty over what channels will be unavailable. Maintain an overall communication and escalation plan with multiple paths of communication and alternates. The response team needs to initiate these communications, provide scheduled updates to the plan, begin documenting everything that has been discovered, and ask supporting groups for evidence preservation, as well.

Step 2
Establish who is in charge

When an event is escalated to an incident it is important to understand who is in charge; roles, responsibilities, and authority are for all members of the response team should be defined in advance. Policy-granting authority needed to fulfill the roles of team members must be clearly communicated across the organization.

The team should be trained properly to handle most incidents and have access to the resources they need. The right support groups need to be identified and contacted. For example, some incidents will require representation and expertise from legal, HR, communications, and executive leadership.

Other information that will be needed at this time includes:

- A complete list of assets
- Network diagrams
- Key resources
- Support services

After the incident is handled and operations begin to return to normal, it is time to assess what went right and which vulnerabilities persist.

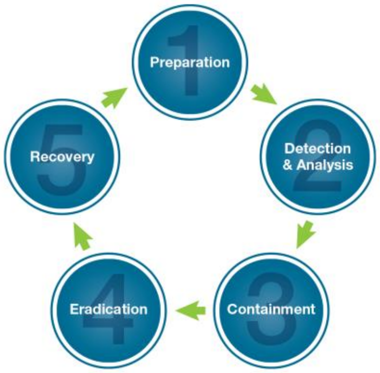
Step 3
Test and improve the plan

The response team needs to go over what happened.

They need to understand what should have been better by means of simulations such as:

- Drills
- Desktop exercises
- Functional exercises
- Full-scale exercises

All of these exercise scenarios are designed to stimulate technical, operational, communication, and/or strategic responses to cyber incidents with a view to reviewing and refining current capabilities.



Each exercise consists of determining what improvements could be made in:

1. Preparation
2. Detection and analysis
3. Containment and eradication of threats
4. Post-incident activity
5. Recovery process and getting back to business

At this point in the process, your company's overall goals should be to examine how well everyone involved, even those beyond the response team, performed at information sharing during the incident. Based on the results of the response, upper management can assess the response team's decision-making skills and evaluate how roles and responsibilities within the organization may need to change to strengthen security.

Many groups all throughout the organization should be involved in the evaluation process. Better coordination and understanding of incident management skills require consensus across multiple departments and entities. It will become clear in these sessions how sharing information on evaluating threats will benefit not only the organization but also the larger community in which it operates.

Step 4 Evaluate communications

In some ways, an incident response plan is only as good as its communication network. During critical incidences, time is of the essence and communication networks tend to be the first resource to break down for a number of reasons.

Therefore, it is crucial to review and test the communication plan before any incident. Incident response team members need to identify and contact their alternates. The same is true of their counterparts in the business and information technology teams. Do not neglect communication records for third parties and related vendors as well as their emergency contact procedures.

Finally, the communications plan needs to establish a protocol for identifying a crisis command center or war room and an alternate location. From that location, team members can launch a conference bridge to keep team members in contact on short notice. The conference leader should make sure the response team is able to access a centralized knowledge base or document repository.

That knowledge base should contain the most recent:

- Recovery plans
- Status updates
- Shared documents
- Stored Documents
- Template for communications

There are many reasons why communication plans can break down, including:

1. Email, voicemail, and text alerts may be ignored
2. Contact information may be wrong or simply out of date
3. On weekends, nights, and holidays, businesses may be closed and private phones turned off
4. The response plan may not have been updated recently enough
5. Customer-facing staff may quickly become overwhelmed with outside messages

Step 5 Understand the impact

There have been a number of high profile data breaches in the past few years, which have impacted millions of people. The growing threat of identity theft makes customers especially sensitive to any of their data being at risk. As a result, companies need to understand exactly what is at risk in each type of incident and how that could have a negative impact on the business.

The costs associated with the loss of data, loss of reputation, legal fees, customer abandonment, and repair costs can add up to a crippling blow from a relatively minor event. Evaluate the fallout from the exploitation of a moderate or severe security hole. Estimate the cost to bankruptcy from extended loss of business and where the greatest impacts would fall.

People outside the organization may learn of the event very rapidly. Identify the subgroup within the response team that will be responsible for handling media communications. The help desk needs to prepare an automated message to prevent the staff from becoming overwhelmed.

What’s next?

Security risks will be a part of business as long as business has something valuable to protect. Though people realize this fact in theory, it only becomes personal after an attack. Don’t wait until it is too late to assess what the damages may be in both direct and indirect costs. The first step in risk minimization is a thorough understanding of which resources are the most critical for business operations. Planning to protect those assets takes iterative testing and refinement of the response plan. Regular updates based on lessons learned and post-mortem are the most essential steps to be performed after an incident of any severity.

Prepare for the worst and strive for the perfect communication within your organization. Remember that when it comes to security procedures in the business world, recovery can be just as decisive as prevention and detection.

After you've evaluated and made improvements to your incident response plan, focus on streamlining the IR management process. Learn how you can automate incident response management – schedule a demo of our platform at resilientsystems.com/demo, and see how much time it can save you.

About Resilient Systems

Resilient Systems is the leading provider of incident management software empowering organizations to thrive in the face of cyberattacks and business crises. Our collaborative platform arms incident response teams with workflows, intelligence, and deep-data analytics to react faster, coordinate better, and respond smarter. Headquartered in Massachusetts, USA, Resilient Systems’ customers are some of the world’s most trusted brands. Visit us at resilientsystems.com.

About HP

HP is a leading provider of security and compliance solutions for the modern enterprise that wants to mitigate risk in their hybrid environment and defend against advanced threats. Based on market-leading products from HP ArcSight, HP Fortify, HP TippingPoint, and HP Atalla, the HP Security Intelligence Platform uniquely delivers the advanced correlation, application protection, and network defenses to protect today’s hybrid IT infrastructure from sophisticated cyber threats.

hp.com/go/sioc

Most Innovative Product

NUREMBERG GERMANY

One Alewife Center, Suite 450, Cambridge, Massachusetts 02140
US +1 617 206 3900 **UK** +44 (0) 118 949 7555
Follow Us Twitter @resilientsys
resilientsystems.com