Addressing the 10 Most Common Flaws in Cyber Incident Response Plans

Alexander Waintraub

Summer 2024

Cyber attacks are the new norm. It's not if anymore, it is when. In 2023, *45% of businesses had an incident response plan for cybersecurity*, *up from 33% of companies with IR plans in 2019*. While companies may have a response plan in place, there are common flaws that can significantly impact an organization's ability to navigate and recover from a cyber attack effectively and confidently. This whitepaper sheds light on the top ten most common flaws observed in IR plans and provides insights into how organizations can reinforce their resilience against cyber threats.

What is an Incident Response Plan and Why Do I Need One?

An Incident Response Plan (IRP) is a written document, formally approved by the senior leadership team, that helps your organization before, during, and after a confirmed or suspected security incident. Your IRP will clarify roles and responsibilities and will provide guidance on key activities. It should also include a list of key people who may be needed during a cybersecurity crisis.

IR plans serve as a proactive and strategic approach to handle all types of security incidents. It outlines the necessary steps to be taken, roles and responsibilities, communication strategies, and the overall framework to ensure a coordinated response. An incident response plan can provide a systematic approach to handling such cyber incidents.

"IRPs guide organizations through the incident from identification to lessons learned. The absence of a comprehensive IRP, organizations risk prolonged downtime, heightened financial losses, and reputational damage." says Niall Heffernan, Head of Information Security at CYGNVS.

Top 10 Most Common Flaws in IR Plans

1. "If you fail to plan, you are planning to fail." - Benjamin Franklin

Benjamin Franklin's timeless wisdom underscores the critical importance of having a well-defined incident response plan in place. Yet, despite the increasing prevalence of cyber threats, many organizations still lack a structured incident response plan. This oversight leaves them susceptible to prolonged downtime, heightened financial losses, and reputational damage in the event of a cyber incident.

How to Avoid:

Organizations must prioritize the establishment of a structured incident response plan tailored to their unique needs and risk profile. Additionally, it is imperative to regularly review and update the plan to incorporate emerging cyber threats and reflect organizational changes. This dynamic approach ensures that the incident response plan remains relevant and effective.

2. Lack of Defined Roles and Responsibilities

A critical flaw in many IR plans is the lack of clearly defined roles and responsibilities during an incident response engagement. Lack of clarity in roles and responsibilities can result in a chaotic response effort. During an incident, team members need a well-defined structure to act swiftly and effectively. Without this, critical tasks may be overlooked, and decision-making can become convoluted. The ambiguity can be disastrous during a cyber incident, leading to confusion and inefficiencies. You don't want to be delegating roles and responsibilities during the cyber incident! Team members might assume responsibility, and scramble to contain the incident, resulting in duplicated efforts or mistakes in the response efforts. Some organizations design generic organizational charts for each team to define their role during an incident. However, these efforts lack the specificity needed for a dynamic response environment. To enhance clarity, some organizations establish role-specific plans that detail responsibilities and actions for each team member. Regular simulations and drills then reinforce these roles, providing practical experience and ensuring that team members are well-prepared to execute their designated tasks during a real incident. Additionally, periodic reviews and updates to these plans help organizations adapt to evolving cyber threats, maintaining the relevance and effectiveness of defined roles and responsibilities.

How to Avoid:

Organizations should ensure that each team member has a clearly defined role during an incident. Designate specific responsibilities, such as communication lead, technical lead, and liaison with external entities. This clarity streamlines the response process and prevents overlaps or gaps in duties.

3. Built in a Silo

Many IR plans are developed in isolation, without adequate integration with IT recovery, cyber resilience, business continuity plans, or third-party providers. The isolation of IRPs from other critical organizational frameworks creates blind spots and inefficiencies. Without integration, internal and third-party response teams may overlook critical dependencies, fail to leverage available resources, or duplicate efforts, ultimately hindering the organization's ability to mount a cohesive and effective response.

How to Avoid:

Organizations should prioritize the integration of incident response planning with other key frameworks. This entails:

> ***Cross-Functional Collaboration****: Encourage collaboration and communication between teams responsible for incident response, IT recovery, cyber resilience, and business continuity. Cross-functional teams should work together to develop integrated response strategies that account for dependencies and align with broader organizational goals.*
>
> ***Regular Alignment Exercises****: Conduct regular alignment exercises to ensure that incident response plans are synchronized with other organizational frameworks. These exercises should involve key stakeholders from each relevant department and focus on identifying areas of overlap, dependencies, and potential gaps in response strategies.*
>
> ***Unified Approach:*** *Adopt a unified approach to incident response planning that considers the interconnectedness of various organizational functions. This approach should emphasize the importance of holistic response strategies that address not only the technical aspects of cyber incidents but also their broader impact on business operations and continuity.*

4. Inadequate Communication Strategies

Inadequate communication strategies hinder an effective response during a cyber incident, and failing to establish a place to communicate securely and confidently may lead to delays, misinformation, and a fragmented response effort. Organizations fail to establish robust communication channels during a cyber incident, resulting in delays, misinformation, and a fragmented response. Communication breakdowns exacerbate the impact of incidents, impeding the timely sharing of critical information and hindering the coordination necessary for an effective response. In an incident with a mechanical engineering firm that was a victim of a ransomware attack in 2021, they were requested to use their personal emails for communications to mitigate the risk of alerting the threat actor. The lack of an IRP with establish secure communications protocols resulted in the IT team accidentally emailing the CEO’s compromised email – alerting the threat actor and compromising the IR efforts through manipulating the response efforts and exacerbating the incident.

Picture this: In 2022, a technology company fell victim to a ransomware attack. In the midst of the chaos and with no established protocol in place, they resorted to using personal email accounts, unaware that the CEO's email had been compromised. Unbeknownst to them, every message exchanged inadvertently alerts the threat actor, allowing them to manipulate response efforts and exacerbate the incident further. Relying on standard communication tools can be a recipe for disaster. Email chains, messaging apps, and personal devices offer convenience but lack the security needed for effective incident response.

How to Avoid:

Implement and prioritize the use of a secure out-of-band cyber incident response solution to facilitate swift and secure communication during a security incident. Clear communication protocols should be established, ensuring that all team members and third-party providers are familiar with how to communicate through the secure platform. Regular training and drills can reinforce these protocols, empowering the incident response team to communicate confidently and effectively in the face of adversity.

5. Neglecting Legal Engagement and Regulatory Compliance

When legal and regulatory considerations are sidelined in incident response planning, organizations inadvertently create blind spots in their defense strategies. Failure to engage legal counsel early and adhere to regulatory requirements can lead to a cascade of legal actions, hefty fines, and irreparable damage to the organization's reputation. Legal and regulatory compliance should just be a box to tick, but a fundamental pillar of incident response.

How to Avoid:

The key to mitigating this flaw lies in proactive engagement with legal counsel from the outset of incident response planning. By involving legal experts early in the incident, organizations can gain invaluable insights into their legal obligations and regulatory compliance requirements. This ensures that incident response plans are developed with a thorough understanding of the legal implications, thereby minimizing the risk of legal exposure.

6. Inadequate External Third-Party Engagement

No organization possesses all the expertise and resources needed to combat the full cyber threat spectrum alone. Effective incident response often requires collaboration with external entities beyond the organization's boundaries including cybersecurity experts, legal, PR, law enforcement agencies etc. However, many organizations fail to establish or engage external entities, limiting their ability to effectively respond and leaving their organizations vulnerable to prolonged disruptions and increased damage.

How to Avoid:

Proactively foster partnerships with external entities, including cybersecurity experts, legal, PR, cyber insurance, law enforcement agencies, industry peers, etc. to enhance the organization's incident response capabilities. Engage with these partners and establish clear communication channels and collaboration frameworks. By leveraging the expertise, resources, and support of external partners, organizations can strengthen their resilience and readiness to respond to incidents effectively.

7. Static Plans that Fail to Incorporate Modern Environments

Static IR plans are akin to relying on outdated maps in a changing terrain. Cyber threats are not static; they evolve and adapt to exploit vulnerabilities in modern technologies and infrastructures. Failure to incorporate these advancements into IR plans results in blind spots and inefficiencies. Many organizations print out their plans, put them in their drawer for safe keeping, and forget it’s even there. Other organizations save their IR plans on mapped drives, hoping threat actors will never look there, and yet that’s the first place they do look.

How to Avoid:

Dynamically and proactively update your organization’s IRPs to reflect changes in technology, infrastructure, and threats. Regularly assess, test, and incorporate lessons learned into your dynamic plans. By adopting a proactive approach to updating IR plans and embracing the nuances of modern environments, organizations can enhance their resilience against evolving cyber threats and navigate through crises with confidence.

8. Failure to Consider Worst-Case Scenarios

One of the critical flaws observed in incident response plans is the failure to account for worst-case scenarios. Cybercriminals are constantly developing new tactics and techniques to breach organizational defenses. These scenarios, such as destructive ransomware attacks or extortion tactics, pose significant threats to organizations, yet many IR plans overlook them, leaving organizations vulnerable and ill-prepared to respond effectively.

How to Avoid:

Conduct scenario-based planning exercises to identify and prepare for worst-case scenarios; scenarios like ransomware incidents, insider threat, business email compromises, ensure your organization has a comprehensive assessment of capabilities, preparedness, backup processes, and communication strategies during these cyber attacks.

These exercises should involve key stakeholders from across the organization and focus on identifying potential threats, vulnerabilities, and response strategies. Develop response strategies and plans tailored to these scenarios and regularly review and update them to ensure your organization is ready.

9. Failure to Test and Execute Plans

Coach often said, "Practice makes perfect.” Preparation is key! Yet many organizations overlook testing and executing their IR plans. This ultimately leaves gaps and inefficiencies that only become apparent during an actual incident. The absence of rigorous testing and execution not only undermines the efficacy of the IR plan but also jeopardizes the organization's overall cyber resilience, making it susceptible to unforeseen challenges that could have been mitigated through proactive preparation and validation.

How to Avoid:

Establishing a regular testing schedule for incident response plans is paramount. This schedule should include a variety of exercises, such as tabletop simulations, scenario-based drills, and full-scale crisis simulations, to exercise different types of cyber incidents and response scenarios. Conduct post-exercise debriefs to analyze performance, capture lessons learned, and update plans accordingly. Continuous practicing, learning, and refinement ensures that incident response plans remain current, effective, and aligned with the organization's needs and threat intelligence.

10. Failure to Execute Plans

Even with meticulously crafted IR plans, some organizations stumble at the final hurdle: execution. This failure to execute effectively during a cyber incident can stem from a myriad of reasons, including inadequate training, resource limitations, or suboptimal decision-making processes.

How to Avoid:

By prioritizing training, conducting regular exercises, reinforcing skills, and empowering team members, organizations can significantly enhance their ability to execute the IR plan effectively during a cyber incident. This proactive approach not only strengthens the organization's resilience but also instills confidence among stakeholders and demonstrates a commitment to cyber readiness.

Conclusion:

While strong cyber incident response is important, most plans crumble in predictable areas. Addressing these systematic gaps, organizations can establish reliable resilience when navigating an incident. It is crucial to respond based on integrated capabilities rather than relying solely on static plans, thereby demonstrating true cyber readiness. Incident Response planning plays a pivotal role in directing organizations through the complexities of cybersecurity incidents, ensuring a structured approach during times of panic. Having well-defined guidance and workflow ensures all the necessary steps are taken for the recovery and restoration of the organization.

To strengthen defenses and mitigate the effects of cyber threats, organizations need to proactively address the common vulnerabilities highlighted in this whitepaper. Effective response necessitates a commitment to ongoing improvement, enhanced collaboration, and the development of an all-encompassing strategy that cohesively combines people, processes, and technology. By undertaking these concerted efforts, organizations can confidently confront and surmount the challenges presented by cyber incidents.