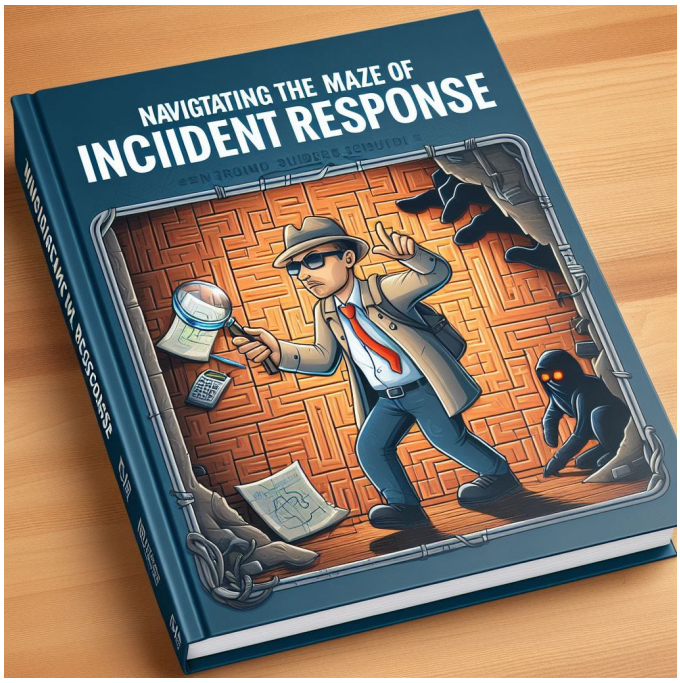

I. Introduction

The document "Navigating Incident Response" by Microsoft Security is a comprehensive guide designed to help organizations navigate the complexities of incident response (IR). It emphasizes the inevitability of cybersecurity incidents and the importance of starting an IR with a thorough understanding of the necessary actions, timing, and involved parties. The guide focuses on the people and processes critical to an effective response, including roles, management, burnout avoidance, and compliance with regulatory obligations.

As we delve into the analysis of this document, we will present a distilled summary of its key recommendations and strategies, aiming to equip organizations with the knowledge to swiftly contain threat actors and minimize business impact, while also preserving evidence and understanding compliance and regulatory obligations

II. Keypoints, findings of Maze

A. *Key Points and Takeaways:*

- Cybersecurity incidents are inevitable, and having a well-thought-out incident response plan is crucial for quick containment and recovery
- People and processes are at the core of an effective incident response, with clear roles, responsibilities, and management strategies to avoid burnout and ensure compliance
- Incident response methodologies are well-documented by NIST, including preparation, detection, containment, eradication, recovery, and lessons learned
- Governance is key, with roles such as Governance Lead, Incident Controller, and Investigation Lead being critical to the structure of the response
- Communication is essential, both internally and externally, to manage messaging and expectations during an incident
- Evidence preservation and collection are prioritized to enable a comprehensive investigation and to develop a full picture of the incident
- Shift planning and vendor engagement are important to ensure support across multiple time zones and from third-party IT services
- SITREPs (Situation Reports) provide proactive communication with stakeholders, maintaining a single source of truth about the incident
- Forensic investigation should be coordinated, prioritizing tasks based on risk, and include proactive network monitoring
- Out-of-band communications should be set up to ensure privacy and security during the response
- Containment strategies should be evidence-driven, balancing risk mitigation and service disruption
- Recovery planning should address long-term service restoration and hardening based on identified risks and security gaps
- Regulatory and legal obligations must be understood and addressed early in the response process

B. *Key Findings:*

- Only 26% of organizations have a consistently applied incident response plan, highlighting the need for better preparedness
- Common pitfalls during incident response include ineffective remediation, inadvertent evidence destruction, lack of documentation, and failure to engage with vendors and legal counsel early
- Vendor engagement is crucial for evidence acquisition and support during an incident, and proactive engagement ensures prioritization of requests
- Containment approaches should be tailored to the type of incident, with considerations for business impact and the potential alerting of the threat actor
- Communication leads play a vital role in controlling messaging and responding to requests for information, ensuring consistency and alignment with the investigation
- Legal and regulatory considerations are complex and vary by jurisdiction, necessitating early engagement with counsel to navigate mandatory reporting and compliance

C. *Key Actions and Escalation Points*

- **Stand up an incident command structure**: At the outset of an incident, it's important to establish a response model to manage the incident. This includes identifying key stakeholders who can help frame up a response structure
- **Identify workstream leads**: The guide suggests identifying leads for various workstreams, such as governance, incident control, investigation, infrastructure, communication, and regulatory compliance
- **Notify internal senior stakeholders**: The Governance Lead should proactively notify senior stakeholders and members of the Executive Leadership team that a major response is underway
- **Secure dedicated resources**: Whenever possible, dedicated resources should be assigned to the response,

or at a minimum be directed to prioritize response activities over other work

D. Best Practices

- **Preserve evidence and understand compliance obligations**: Beyond understanding the scope of the compromise and how to regain control, it's important to preserve evidence and understand your compliance and regulatory obligations
- **Maintain visibility and understanding of risk**: The Governance Lead should maintain oversight of the response to have a clear picture of the risk associated with the incident. This visibility should be maintained throughout the response, via situation reports produced by the Incident Controller
- **Manage major blockers**: The Governance Lead should provide support if the response team encounters an issue which cannot be resolved at the operational level. Typical issues may include resource requests from other parts of the business, escalation of requests to vendors and other third parties, and decisions that have wide-reaching business impact
- **Workstream management and tasking**: In the middle of a response, documentation of actions and tasks is often deprioritized in favor of rapid execution. As the response continues, this can create challenges. Therefore, it's important to document actions and tasks from the beginning

III. IRP

An Incident Response Plan (IRP) is a structured approach to handling security incidents, breaches, and cyber threats. A well-defined IRP can help organizations minimize loss and theft of data, mitigate the effects of cyberattacks, and reduce recovery time and costs. The key components of an IRP include:

- **Preparation**: This involves setting up an incident response team, defining their roles and responsibilities, and providing necessary training. It also includes preparing the necessary tools and resources for incident detection and response.
- **Detection**: This phase involves identifying potential security incidents, usually through the use of intrusion detection systems, firewalls, or data loss prevention (DLP) systems.
- **Containment**: Once an incident is detected, steps must be taken to prevent further damage. This could involve isolating affected systems or networks to prevent the incident from spreading.
- **Eradication**: This involves finding the root cause of the incident and removing affected systems from the network for forensic analysis.
- **Recovery**: Systems are restored and returned to normal operation, ensuring no remnants of the incident remain. This could involve patching software, cleaning systems, or even reinstalling entire systems if necessary.
- **Post-Incident Activity**: After the incident is handled, an analysis should be conducted to learn from the incident and improve future response efforts. This could involve updating the IRP, implementing new security measures, or providing additional training to staff

When considering incident response tools, there are several key considerations that organizations should keep in mind to ensure an effective and efficient response to cybersecurity incidents:

A. Integration with Existing Systems

Incident response tools should be able to integrate seamlessly with the organization's existing security infrastructure, such as firewalls, intrusion detection systems, and SIEM solutions. This integration allows for automated data collection and correlation, which can speed up the detection and analysis of security incidents.

B. Scalability

The tools should be scalable to handle the volume of data and the number of endpoints within the organization. As the organization grows, the tools should be able to accommodate an increasing amount of data and a larger network without performance degradation.

C. Evidence Preservation

During an incident, preserving evidence is crucial for a thorough investigation and potential legal proceedings. Incident response tools should facilitate the collection and preservation of digital evidence in a forensically sound manner, ensuring that it remains admissible in court if necessary.

D. Real-time Monitoring and Alerting

The ability to monitor the network in real-time and generate alerts for suspicious activities is essential. This enables the incident response team to quickly identify and respond to potential threats before they can cause significant damage.

E. Automation and Orchestration

Automation of repetitive tasks and orchestration of response actions can greatly improve the efficiency of the incident response process. Tools that offer automated workflows can help reduce the time to respond and mitigate threats, as well as minimize the potential for human error.

F. User-Friendly Interface

The tools should have an intuitive and user-friendly interface that allows incident responders to quickly navigate and use the features effectively, especially under the pressure of an active incident.

G. Comprehensive Reporting

Incident response tools should provide comprehensive reporting capabilities that allow for detailed analysis and documentation of incidents. This is important for post-incident reviews, compliance with regulatory requirements, and improving the organization's security posture.

H. Customization and Flexibility

Every organization has unique needs and requirements. Incident response tools should be customizable to fit the specific processes and workflows of the organization. They should also be flexible enough to adapt to changing threat landscapes and organizational changes.

I. Vendor Support and Community

Strong vendor support and an active user community can be invaluable resources for troubleshooting, sharing best practices, and staying informed about the latest threats and response strategies.

J. Legal and Regulatory Compliance

The tools should help organizations comply with legal and regulatory requirements related to incident response, such as mandatory reporting and privacy regulations. This includes features that support the management of regulatory/legal requirements and facilitate engagement with legal counsel when necessary.

IV. Roles and Responsibilities

A modified version of the incident response lifecycle model documented by the National Institute of Standards and Technology (NIST), which typically includes preparation, detection, containment, eradication, recovery, and post-incident activity or lessons learned.

It suggests a response model to manage the incident, which includes the following roles:

- **Governance Lead**: This role is typically filled by the CISO or CIO. They maintain visibility and understand the risk and impact to the wider business, and communicate with senior stakeholders
- **Incident Controller**: This role is typically filled by an ITSM/Security Operations Lead. They coordinate all operational workstreams to understand and contain the threat, and communicate the risk to the Governance Lead
- **Investigation Lead**: This role is typically filled by a Senior IR/Senior IT Operations Representative. They are responsible for understanding the overall compromise and communicating the associated risk
- **Infrastructure Lead**: This role is typically filled by a Senior IT Operations Representative. They are responsible for containing the threat by reducing the risk presented by the compromise
- **Communications Lead**: This role is typically filled by a Communications Specialist. They control messaging both externally and internally
- **Regulatory Lead**: This role is typically filled by an Internal Counsel/GRC Representative. They are responsible for the risk/impact assessment and management of regulatory/legal requirements to maintain compliance

Recommended Workstream Skillsets:

- **Governance Lead**: Operational oversight, maintaining visibility, understanding risk and impact, and communicating with senior stakeholders
- **Incident Controller**: Operational management and tasking, coordinating all operational workstreams, and communicating risk to the Governance Lead
- **Investigation Lead**: Forensic investigation to understand the overall compromise and communicate associated risk
- **Infrastructure Lead**: Threat containment by reducing the risk presented by the compromise
- **Communications Lead**: Stakeholder engagement and controlling messaging both externally and internally
- **Regulatory Lead**: Risk/impact assessment and management of regulatory/legal requirements to maintain compliance

Ensuring an Efficient and Effective Incident Response Plan:

- **Regularly Update the Plan**: Keep the incident response plan current with the evolving threat landscape and organizational changes
- **Test and Exercise**: Conduct regular drills and simulations to test the plan and identify areas for improvement
- **Clear Communication**: Establish and maintain clear communication channels for all stakeholders involved in the incident response
- **Documentation**: Ensure all actions and decisions are well-documented to avoid confusion and inefficiency
- **Vendor Engagement**: Proactively engage with vendors to support evidence acquisition and other response activities
- **Shift Planning**: Implement shift planning to prevent burnout and maintain a continuous response across multiple time zones

A. Governance Lead

The Governance Lead, who could be the CISO or CIO, is responsible for operational oversight. Their role is to maintain visibility and understand the risk and impact to the wider business, and to communicate with senior stakeholders. The Governance Lead should proactively notify senior stakeholders and members of the Executive Leadership team that a major response is underway. This ensures that other parts of the business are aware of the potential risk and that service disruption may occur while the incident is being managed

The Governance Lead should also secure dedicated resources for the response. Organizations without dedicated security teams often deputize resources from other parts of the business to assist with the response. These individuals then need to balance their existing workload with response activities. Whenever possible, dedicated resources should be assigned to the response, or at a minimum be directed to prioritize response activities over other work

The Governance Lead should maintain oversight of the response to have a clear picture of the risk associated with the incident. This visibility should be maintained throughout the response, via situation reports produced by the Incident Controller

The Governance Lead is also the response team's interface with both internal and external senior stakeholders. If the response team encounters an issue which cannot be resolved at the operational level, the Governance Lead should provide support. Typical issues which may need support from the Governance Lead include resource requests from other parts of the business, escalation of requests to vendors and other third parties, and ratifying and helping to communicate decisions which have wide-reaching business impact, such as mass password resets or disabling internet connectivity

B. Incident Controller

The Incident Controller is typically an ITSM/Security Operations Lead, whose primary responsibilities are operational management and tasking. This role involves coordinating all operational workstreams to understand, contain, and communicate the threat to the Governance Lead.

The Incident Controller is responsible for managing and tracking tasks for all operational workstreams to ensure actions are prioritized and documented. This is crucial because, during a response, documentation of actions and tasks is often deprioritized in favor of rapid execution. However, as the response continues, a lack of clear record of actions taken and decisions made can create confusion

The Incident Controller also plays a key role in maintaining visibility and understanding of risk. They produce situation

reports for the Governance Lead, who maintains oversight of the response to have a clear picture of the risk associated with the incident. This visibility should be maintained throughout the response

In the event of issues that cannot be resolved at the operational level, the Incident Controller can escalate to the Governance Lead. Typical issues that may require such escalation include resource requests from other parts of the business, escalation of requests to vendors and other third parties, and decisions that have wide-reaching business impact, such as mass password resets or disabling internet connectivity

The Incident Controller is a pivotal role in the incident response process, responsible for operational management, tasking, and communication of threats, as well as escalation of major issues to the Governance Lead

C. Investigation Lead

The Investigation Lead, typically a Senior IR/Senior IT Operations Representative, is responsible for conducting forensic investigations to understand the overall compromise and communicate the associated risk. This role is crucial in determining the scope, impact, and root cause of the incident, which informs the response strategy and helps prevent similar incidents in the future.

The Investigation Lead is expected to have a deep understanding of the organization's IT environment and the threat landscape. They should be skilled in digital forensics and incident response (DFIR), and be able to use various tools and techniques to analyze system logs, network traffic, and other data to identify indicators of compromise (IoCs)

The Investigation Lead works closely with the Incident Controller, providing regular updates on the investigation's progress and findings. These updates are crucial for maintaining visibility of the incident and understanding the associated risk

The Investigation Lead may also need to collaborate with external entities, such as law enforcement or third-party vendors, especially in cases involving legal issues or specialized technical expertise

The Investigation Lead plays a critical role in incident response, using their technical expertise to understand the incident, inform the response strategy, and communicate the risk to the Incident Controller and Governance Lead

D. Infrastructure Lead

This role is typically filled by a Senior IT Operations Representative and is responsible for containing the threat by reducing the risk presented by the compromise.

The Infrastructure Lead is one of several key roles in the incident response structure, which also includes the Governance Lead, Incident Controller, Investigation Lead, Communications Lead, and Regulatory Lead. Each of these roles has specific responsibilities and required skillsets

The Infrastructure Lead's main responsibility is threat containment. This involves taking actions to limit the spread and impact of a security incident within the organization's IT infrastructure. This role is crucial in managing the technical aspects of an incident response and ensuring that the threat is effectively contained to prevent further damage

The importance of having dedicated resources for each role in the incident response structure means that the individuals assigned to these roles should prioritize response activities over other work, whenever possible

In terms of required skills, the Infrastructure Lead should have expertise in infrastructure and architecture, as well as some knowledge in security operations, risk management, and digital forensics. The document provides a skill matrix that outlines the required and optional skillsets for each role in the incident response structure

E. Communications Lead

This role is responsible for controlling both internal and external messaging during a cybersecurity incident.

The Communications Lead is part of a larger incident response structure that includes other roles such as the Governance Lead, Incident Controller, Investigation Lead, Infrastructure Lead, and Regulatory Lead. Each of these roles has specific responsibilities and skillsets required to effectively manage and respond to a cybersecurity incident

The Communications Lead, specifically, is responsible for stakeholder engagement. This role is typically filled by a Communications Specialist. Their primary task is to control messaging both externally and internally. This involves communicating the status and details of the incident to relevant stakeholders within and outside the organization, ensuring that accurate and timely information is disseminated. This can help manage expectations, maintain trust, and prevent the spread of misinformation

The Communications Lead also works closely with the Governance Lead, who maintains visibility and understanding of the risk associated with the incident. The Governance Lead is responsible for operational oversight, maintaining visibility of the response, and understanding the risk and impact to the wider business. They communicate with senior stakeholders and ensure that they are aware of the incident and its potential impact

The Communications Lead plays a critical role in incident response, managing the flow of information and ensuring that all stakeholders are kept informed during a cyber-incident

F. Regulatory Lead

This role is typically filled by an Internal Counsel or Governance, Risk, and Compliance (GRC) Representative. The primary responsibilities of the Regulatory Lead are to conduct risk and impact assessments and manage regulatory and legal requirements to maintain compliance during a cyber-incident

The Regulatory Lead is part of a broader incident response structure that includes other roles such as the Governance Lead, Incident Controller, Investigation Lead, Infrastructure Lead, and Communications Lead. Each of these roles has specific responsibilities and required skillsets. For instance, the Governance Lead, typically a CISO or CIO, is responsible for operational oversight and maintaining visibility and understanding of risk. The Incident Controller, usually an ITSM/Security Operations Lead, coordinates all operational workstreams to understand, contain, and communicate the threat.

The Regulatory Lead's role is crucial in ensuring that the organization's response to a cybersecurity incident aligns with legal and regulatory requirements. This could include obligations under data protection laws, sector-specific regulations, or contractual obligations. The Regulatory Lead would also be responsible for liaising with regulatory bodies as necessary and managing any legal implications of the incident.