WeMakeBoxes Group Incident & Crisis Management Procedure

Submitted for David King

March 26, 2024

Document Version: 0.0.0
Document Owner: Doug Rogers, CISO

SECURITY INCIDENT? EMAIL: security-incident@wemakeboxes.org
IT INCIDENT? EMAIL: it-incident@wemakeboxes.org
URGENT OPERATIONAL TECH ISSUE? EMAIL: ot-incident@wemakeboxes.org
EMAIL NOT WORKING? SLACK: @security-incident, @it-incident, @ot-incident

An Important Note on Shelfware and Document Lifecycle: *It is the sincere belief of the author that there is little more useless in this world than shelfware: Documents that adorn a forgotten corner of a shared filesystem whose only function is to empower a compliance function to assert that the document exists. This document must be read by anyone who wishes to undergo incident preparedness training in order to serve as an Incident Commander, and everyone who could potentially serve in a Crisis Chair capacity. When they have finished reading it, they are invited to suggest edits to the document owner, and must also answer the following questions in a feedback form that will be distributed to them:*

- *Which part of this document did you find most boring? Do you think it could be made less so?*
- *Do you think there are any parts of this document where the wording could be simplified/made clearer?*
- *Are there any parts of this document that could be made shorter/be removed altogether without loss of meaningful information?*

Criticism may be harsh, but must be respectful. We believe it can be both.

Scoping

What this document is

This document defines the company's approach to incident and crisis management. It will state what incidents and crises are, when and how to declare them, how to conduct them, how to conclude them, and what to do in the aftermath. It will define a process for preparing for incidents and crises, including stressing the importance of stakeholder identification, and realistic Service Level Obligations (SLOs) for company services and processes. It will provide guidance on escalating an incident or crisis in the event that the team currently responding has determined that it is unable to resolve it.

What this document is not

This document is not a runbook. It will not tell employees precisely what to do in the event of an incident or crisis. It is to be read as part of training and preparation. It is not to be read during an incident, by that moment it is too late and it would be a poor use of a responders precious time. This document will not identify stakeholders exhaustively, nor will it define SLOs for any systems or machinery.

Common Questions

What qualifies as an incident?

NIST provides a good definition for an information security incident[2], we offer the following as a slight modification to encompass other kinds of incidents we may encounter, eg. with the tooling owned by the Operational Technology division of the company:

"An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of a company asset, service or function, or that constitutes a violation or imminent threat of violation of company policies or procedures."

This definition is intended to be a superset of the definition provided by NIST for an information security incident. If something appears to qualify as an information security incident per the NIST definition then it can safely be assumed that it qualifies as an incident under this one.

When to declare an incident?

Below is a list of some circumstances that may warrant an incident. It is not an exhaustive list, and it is also not a definitively correct list either. Declaring an incident will always be at the discretion of the employees responsible for a given company resource.

- A suspected or confirmed breach of information security has occurred.
- Service level obligations (SLOs) being breached.
- Security policies failing to be adhered to. If a breach of policy is not worthy of an incident, then the policy has not been respected, and it in effect has ceased to be the company's policy, regardless of where it has been written down.
- A lapse in health and safety that caused actual or potential harm to a person on company property, or in any other circumstance where the company could reasonably be argued to have a duty of care. A high standard should exist in all aspects of the business concerning health and safety.
- If an employee reasonably believes that the company is currently or in future will be breaking the law in any of the jurisdictions that it operates then this is certainly incident-worthy. Our policies in all aspects of the business will always strive to comply with the guidance of local legislation, however we must be humble and wary of the possibility that we could make a mistake, or that the law may change.

Incidents should be thought of as relatively routine events, and employees should not fear reprisal for raising incidents in error. There will be none. Post-mortems will be reviewed by more senior members of the company after the fact and a judgement will be made then on whether an incident was appropriate, in order to help the employee calibrate their instincts to raise incidents in future. The company has a strong bias to declaring an incident if in doubt.

Who can declare an incident?

An incident can be declared by anyone who has received incident readiness training. Others present for a situation may make an appeal to such a person to do so, but should not declare an incident themselves if a person with readiness training is present and disagrees that the situation warrants an incident declaration. In the event that no such person can be found then employees who have not had this training may declare an incident themselves. As an early step they may wish to try and escalate to a more senior entity that does have incident readiness training, however we acknowledge this may not always be possible.

How to report an incident-worthy event?

The email addresses listed at the top of this document are the primary way to report a security, IT or OT incident. The inboxes are monitored 24/7 and once a report has arrived the on-call engineer must acknowledge the issue and begin investigating within 10 minutes. The regional office that responds to the alert rotates between the 4 major offices: Birmingham, Essen, Detroit & Rio De Janeiro regardless where the email originally comes from. If the issue cannot be resolved by an engineer in a different region then the on-call engineer has the means to wake up an engineer in the appropriate region.

What qualifies as a crisis?

A crisis has many of the same qualities and criteria as an incident. The only difference really is the severity, and how it is handled. So a crisis is perhaps best defined by its characteristics in contrast to an incident:

- Where an incident is routine and expected to occur often, a crisis is rare, and unexpected
- An incident will generally be orderly and calm, a crisis will feel chaotic and stressful
- In an incident the chain of command remains clear and authority is uncontested. In a crisis the chain of command may have been broken, become unclear, or important actors may have become unreachable.
- The number of stakeholders in an incident will be relatively limited. The number of stakeholders in a crisis may run to an unmanageable tally.

When to declare a crisis?

When an ongoing incident, or a rapidly onset situation has begun to take a turn for the chaotic, and now satisfies some or all of the criteria of a crisis, consideration should be given to declaring a crisis and an appeal should be made to someone who can declare a crisis.

Who can declare a crisis?

The crisis management procedure should be invoked by an employee who has received crisis readiness training has been convinced that the situation satisfies the criteria for a crisis. If no such person is present and efforts to contact one have been unsuccessful then the most senior employee present should declare a crisis to begin managing the situation as best they can until they can contact more senior members of the company to do a handover to.

Incident Management Function

Roles and Responsibilities

The following roles shall exist within the scope of an incident:

- **Incident Commander:** The person who takes charge of the incident, and coordinates the actions of the other actors in the incident. It shall be their responsibility to assign roles to persons as they see fit at the start of the incident, and to adjust, expand or shrink their team as the incident progresses. It shall be this persons responsibility to declare the incident has been resolved.
- **Scribe:** The primary function of this role is to keep a timeline that accurately and concisely records important events in real time.
- **Communications (Comms):** This role encompasses the challenge of keeping stakeholders exactly as informed as they need to be and no more, and potentially also controlling a public-facing narrative.
- **Technical Lead:** If there is a technical aspect to the incident, as there often is, it will be necessary for someone to act as the lead coordinator of a technical team that is familiar with affected assets. This role is often rolled into that of the Incident Commander. We split it out here since we acknowledge that it is not a given that the Commander is technically knowledgeable about the affected assets. Nor do they absolutely have to be.
- **Technical Operator:** Depending on the size and scope of the incident this can be a role filled by many people. Their function is to do as instructed by the technical lead, and to use whatever technical knowledge they possess to help progress to mitigation.
- **Data Gatherer:** Their function is to collect as much telemetry, data and other forms of information about the affected assets while the incident is still progressing. If headcount to assist with the incident is abundant they may prove very useful, not only to expedite the drafting of a post-mortem, but also potentially during the incident itself. The Data Gatherer may discover things that will prove important to the Technical Operators. They may be expected to work closely with the scribe to provide context and evidence for the events that they are recording.

It is not a given that all of these roles shall be needed in every incident. However, we should be aware of them and their responsibilities should the Incident Commander require one of these roles to be filled.

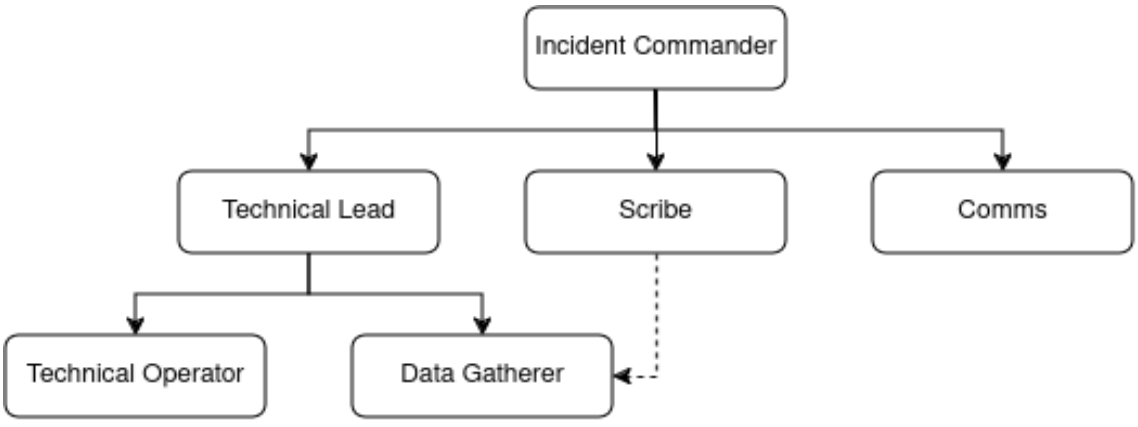

Figure 1: *Incident Management Command Structure.*

Figure 1 illustrates the command structure that should be assembled at the start of an incident. The Technical Lead and Commander are responsible for assembling the teams beneath them. The dotted line between the Scribe and Data Gatherer (DG) indicates that while the DG's suitability for the role and main function is to inform the Technical Operators investigation, they also have a responsibility to convey relevant technical information to the scribe, who in turn shall report to the Commander and Comms operator.

Incident Response Process

The overall process for incident response shall follow this pattern:

- **Incident Declaration:** An automatic alert has fired or other non-automated signal has been acknowledged by a person with incident preparedness training has acknowledged warrants an incident.
- **Appoint Commander and Subordinate Roles:** The person who declared the incident takes command. The command structure fleshed out in Figure 1 is assembled, consisting of as many persons as the incident commander sees fit. The incident commander creates an incident ticket based on a template in Jira, the company's case management tool. Then using the ticket ID as a UID they create a Slack channel to provide a common platform for communication for anyone who doesn't happen to be physically in the incident room.
- **Conduct Incident:** The following items will be pursued concurrently by each of the persons who have been assigned these roles. While there are no fixed numbers of people that should participate in an incident, it should be noted that there are three distinct roles here. Therefore the recommended minimum number of persons to properly conduct an incident is three.
  - **Strive For Mitigation:** Assisted by their Technical Operators and Data Gatherers the Technical Lead must strive for mitigation. They must *not* attempt to discover the root cause, nor should they attempt to solve any deeper underlying problems. Their only prerogative is mitigation. They must look to return the system to a state where it would not be necessary to declare an incident as fast as possible. Root cause analysis and fixing underlying issues can follow later.
  - **Document Events:** As soon as they are appointed the Scribe must create a document, ideally digital and shareable (eg. Google Docs) which they share in the Slack channel, and begin recording notable events as they occur, anything important that the Data Gatherer informs them of, and anything else that they, the Tech Lead or the Incident Commander advises them ought to be documented. If they have time they should begin to make an effort to backdate events and establish a timeline that precedes the incident declaration.
  - **Inform Stakeholders:** The Incident Commander and Comms operator shall work together to establish the identity of stakeholders and make a best effort to keep them informed of what they need to know and no more.
- **Resolve Incident:** On the advice of the Technical Lead, the Incident Commander declares resolution and the temporary command structure is disbanded. A post-mortem must be completed within 48 hours of the incident. The commander is ultimately responsible for this being delivered, but they may delegate the task.

Figure 2 illustrates a rough outline of how the *Strive For Mitigation* step of the Incident Response Procedure should be conducted. The principle is that first an expert in the affected system or asset should be sought. If one cannot be found, resort to a runbook. If a runbook does not exist, then make iterative discretionary attempts to mitigate the issue on a best effort basis. From all steps at all times, escalation is an option if the team does not feel adequately equipped to mitigate the incident.

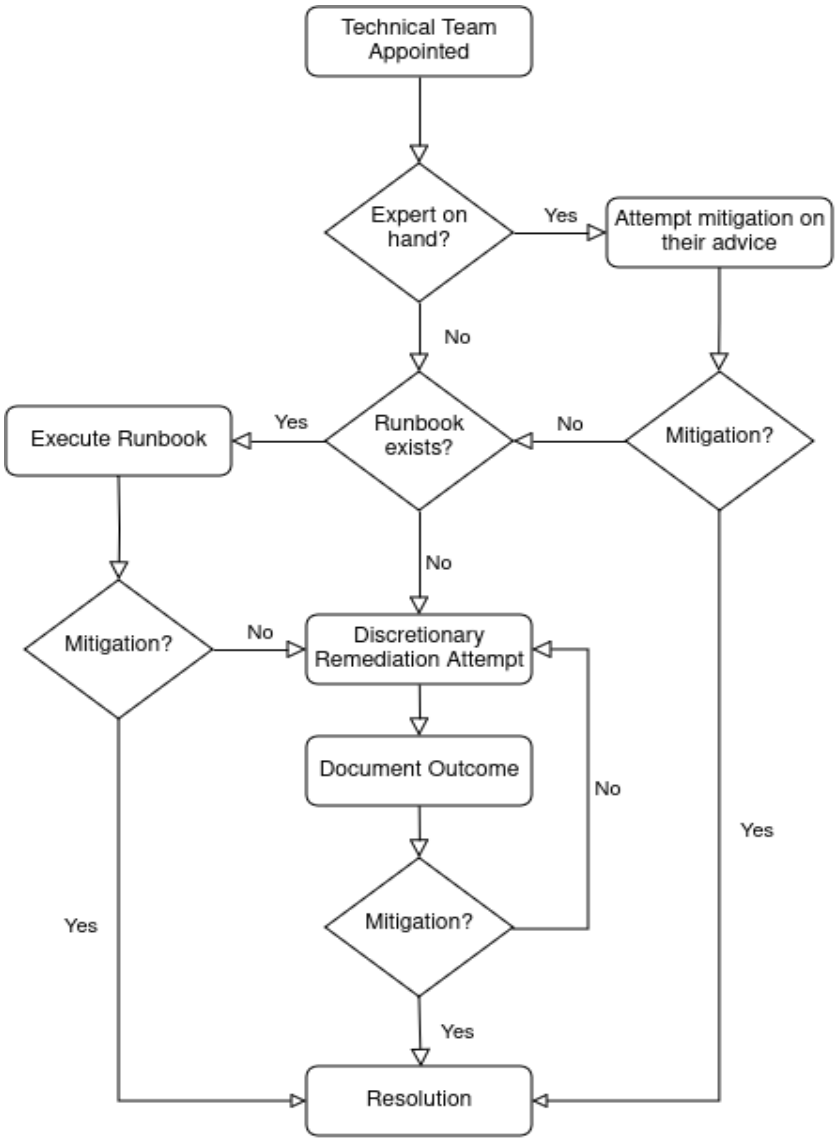

Figure 2: *Technical Incident Response Process.*

A Special Note On Security Incidents

Where the incident has a strong component of security embedded within it, for instance a malware attack against the company, additional care should be taken in the technical incident response process. As ever the response is at the discretion of the commander and their technical lead, but as a guide to them they should consider the following:

- Avoid logging into devices suspected of being affected by malicious software
- Do not destroy forensic evidence if it can possibly be prevented. Avoid rebooting, shutting down or powering down affected systems if possible. Leave things as they are found. We aim to follow evidence collection procedures in line with RFC 3227[1].
- While the preservation of forensic evidence is highly desirable, the integrity of company systems is paramount. When faced with a compromised asset that is threatening other systems, the most important thing is to isolate the asset and prevent the threat from metastasising. Even if that potentially means damaging or destroying the affected system.

- There is always the possibility that the company has been subject to malicious actions perpetrated by an insider at the company. It is therefore even more important than usual that stakeholders are kept informed on a need-to-know basis when it comes to security incidents.

Escalation

At any time the option is available to the incident commander, or any member of their team via an appeal to them, to escalate their incident to another office, a more senior employee, a more technically experienced employee, or simply a larger and more capable team, such as may exist for the global IT function in the Birmingham head office.

It is also an option available to the incident commander if they so choose to escalate to a trained crisis coordinator if they feel it is what the situation warrants. Making these kinds of calls shall be part of their training and will be at their discretion.

Crisis Management Process

The crisis management process is far simpler than that for the incident management process. Once a crisis committee has convened and a chair has been selected against a simple criteria: "Who in the room commands real pre-existing authority in this firm who is prepared to take on the responsibility?" The only thing to insist on is that someone is assigned to the role of comms operator and someone is assigned to the role of scribe. After that, the committee should have full discretion. By nature of the event that is unfolding it is very unlikely that any kind of written procedure would be useful. The guiding principles that must be borne in mind are as follows:

- Containment: Take ownership of the problem
- Threat Assessment: What is on our plate?
- Contingency Planning: What are the possible scenarios? What is the worst case?
- Proactive Response: Establish authority. What will we do and say? Control the narrative

Beyond this the team are expected to draw their experience from simulations, remain calm, and make a sincere best effort in service to the firm.

Preparedness

Training

There are two roles for which training is regarded as absolutely essential: Incident Commander and Crisis Chair. For both roles there will be a training plan defined in a separate document, at the conclusion of which they will have the opportunity to be graduated as a person who has been trained as an Incident Commander/Crisis Chair by serving in this role in an incident/crisis simulation. This graduation will not be a ceremony, the candidate must perform well in the assessment according to a set of criteria defined by the author of the simulation. They can fail if the simulation is not judged to have gone as well as it ought to.

Simulations

The workflows, processes and procedures in this document are deliberately vague and non-committal. This is because the author believes the only true way to be truly ready for an incident or a crisis is to run simulations. Regularly.

For each of Operational Technology, IT, and Information Security, there should be an incident simulation twice a year in each of the 4 major offices, for a total of 24 simulations per year. It shall be the responsibility of the local incident response team lead to coordinate the simulation, delegate the task of authoring it, and appointing an incident commander (ideally one for whom this will serve as their graduation test). Post-mortems should be submitted to the office of the CISO in Birmingham. Failure to do so shall be considered a serious dereliction of duty.

There shall also be an annual crisis simulation that will involve at least three members of the C-Suite in Birmingham. The post-mortem need not necessarily drive change in the same fashion as an incident one would, but it should occur and it should be a frank discussion among the executive about whether they felt the outcome was one they were happy with.

Stakeholder Management

A critical step of preparing for the kinds of incidents this function is expected to deal with is to define and publicise holders of static roles. The roles defined in the main incident management workflow are ephemeral, assumed sporadically for the purpose of the incident and forgotten again as soon as resolution is achieved. However, there are roles that are linked to a persons pre-existing authority/job and therefore must be known ahead of time. During an incident is too late to be attempting to work out who relevant stakeholders are.

A separate document shall be created to enumerate all important stakeholders within the business for the purposes of transparency and clear communication and attribution during an incident. More than merely a name and a job title, this list must state the processes and assets these people are associated with. Final accountability for the correctness of this document will lie with the office of the CISO. They will be obliged to maintain it proactively and to ensure on at least a quarterly basis that it is perfectly accurate.

This stakeholder document should include but absolutely not be limited to:

- General counsel and legal team
- IT Administrators
- Key decision makers within Human Resources
- The entire C-Suite
- Office managers
- Technical leads for operational technology in each region

- Physical security personnel
- Information security personnel

Service Level Obligations

One of the key criteria that was laid out earlier in this document for what potentially constitutes an incident was whether an SLO had been breached. For this to be a meaningful criteria it must be the case that all processes and services *have* an SLO. It is already a core function of the IT, information security and operational technology teams to maintain an asset inventory. It is also now important that where relevant an SLO is associated with each process and service enumerated in those same asset inventories. The office of the CISO will take responsibility for conducting audits to ensure that a sane SLO is associated with all processes and services and will hold asset owners accountable for a failure to establish one. We anticipate this also serving as a useful exercise for rooting out assets that do not in fact have clear ownership, an even more serious issue.

How asset owners choose to ensure their SLOs are not breached we feel should be left up to them. However, we are keen to push for a culture of creating, maintaining, and using runbooks as the goto way to support products and services.

Important Notes and Philosophy:

On discretion:

As mentioned elsewhere in this document, knowledge about incidents should be disseminated during an incident on a need-to-know basis. This is for three reasons:

- In the case of a security incident, to mitigate the possibility that a threat actor has compromised our internal communications systems and is alerted to the fact that we are aware of them.
- To minimise the workload for the person serving as comms operator. Their role will likely be difficult enough as is. The more people that are being given a partially complete picture of the incident the more questions they will be flooded with from concerned parties.
- Controlling the narrative. Any incident can escalate and spiral in severity. In this event, the more that people outside the immediate room where the incident is being managed from know the harder it becomes for the team to control the narrative of the situation. A failure to control the narrative can have serious implications for the company from a reputational standpoint as a picture could be painted in the media of an organisation that is not in control of the situation.

Mitigating the incident vs. solving the incident:

There is no point in attempting to rebuild a house that is still on fire. The highest calling of an incident response function is to sustain the business and protect it's profitability. In real terms this means restoring service. This matters much more than understanding the issue in the moment or pursuing a solution to the root cause of the problem. Solutions should be pursued, but only after mitigation.

On flexibility:

The progression of an incident is often non-linear. It is often inherently chaotic even if it does not end up qualifying as a crisis. It generally defies efforts to create comprehensive plans to cover all scenarios. Therefore another item to be stressed in this procedure is flexibility. The team should be flexible, it's hierarchy should be flexible, the number of people working the incident and the precise roles they have can be flexible. As long as the authority of the incident commander is respected, all else is at their discretion. This document serves to guide them through a chaotic and unpredictable sequence of events, but it would be a mistake to try and precisely prescribe what their team should look like.

Bias to action:

Proactivity is everything. The timeline of events recorded by the scribe will hold the team to account, so the record had better look good. An incident response team cannot be seen resting on its laurels. There is always more that can be done to gather more data, provide stakeholders with more up to date or accurate information, and to research the situation to better understand it. The timeline and data collection efforts will ideally show this, and with any luck the time to mitigation will reflect it.

Plans are worthless, people are key:

As stated before, the real crux of this strategy is to do the utmost to prepare incident responders through training and simulation, so that they will be as able as possible to react that to the many bizarre scenarios that a prescriptive incident response plan could never hope to enumerate.

References

[1] IETF. Guidelines for Evidence Collection and Archiving. https://tools.ietf.org/html/rfc3227/, 2024.

[2] NIST. Incident Definition. https://csrc.nist.gov/glossary/term/incident/, 2024.