Prepare for the Worst, Rather Than Hope for the Best

Preparing to Recover From Major Cyber Security Incidents

Anne Coull
College of Science and Engineering
Flinders University
Sydney, Australia
email: anne.coull@proton.me

***Abstract*—As the threat landscape continues to escalate, organisational leaders are realising that they cannot prevent every cyber incident. The cyber security lens is shifting its focus toward the need for resilience, and the ability to recover from Major Cyber Security Incidents. Cyber incident recovery differs from every day IT incident recovery. The threat actors will have been in the systems domain establishing a foothold, installing malware, and exfiltrating data prior to their presence being noticed. Following the standard IT recovery playbooks will exacerbate the situation, causing confusion and delays. Preparation is the key to cyber incident and recovery readiness. This paper outlines a practical approach for IT and cyber operational teams to apply that will prepare them for major cyber events so that in the heat of an incident, they have the tools at hand, the confidence, and the capability to deal with the situation and the ability to recover within resilience appetite and tolerance.**

Keywords-cyber resilience; recovery; major cyber security incident; playbook.

I. INTRODUCTION

Cyber Security resilience describes the ability to protect against, respond to, and recover from cyber threats [16]. The preceding decade has seen significant focus and uplift in cyber security protection investment in Australian critical infrastructure. And as organisations realise that they cannot expect to prevent 100% of cyber incidents, they are shifting their attention toward preparing for them. This paper provides guidance on how organisations can move to a position where they can recover from significant cyber incidents, and that they are able do so within a reasonable timeframe. Cyber security is different from IT disaster recovery. Prior to the incident being raised, the cyber threat actor has already made-ready, ensuring they can maintain access even when discovered, finding and stealing valuable information assets, and compromising data, backups, configuration files, and applications throughout the environment. All this is achieved well before anything as visible as ransomware is triggered. Applying normal IT recovery processes will only exacerbate the problem, and extend the recovery times. In addition, cyber incident recovery necessitates teams from different areas to work together towards a shared outcome [19].

Preparation is the key [6][16]. Endeavouring to address system and environmental shortcomings whilst attempting to recover business critical systems in the heat of a major incident is not ideal. This will further delay, and may even inhibit the ability to recover. Well before the incident is experienced, the environment needs to be remediated to limit exposure of critical systems, slow lateral movement, close vulnerabilities, correct misconfigurations, tighten privileged user access, and reduce the blast radius of the incident. Section II outlines how cyber security incident recovery differs from normal IT recovery. Section III walks through the five elements that need to be addressed when developing the ability to recover from a Major Cyber Security Incident. Section IV explains the top six threat scenarios that teams should be prepared to recover from. Section V focuses on recovery testing and continuous improvement. Section VI addresses the organisational challenges of cyber resilience readiness. Section VII discusses the metrics use to uplift response performance, and the conclusion reiterates the need for early preparation, and closes the article.

II. CYBER RECOVERY IS DIFFERENT

It is common for the Information Technology (IT) technical support teams to assume that the approach for recovering from cyber security incidents is the same as that used for every-day incidents. This introduces the risk of the intended recovery actions actually making the situation worse and causing further delays. The difference with cyber security incidents is that, prior to being discovered the cyber threat actors have escalated their access privileges, established backdoors, moved laterally across the systems domain, deployed malware to compromise systems and data, altered configuration files and applications across the environment, exfiltrated valuable data and compromised or deleted backups. Their goal is to inflict the most damage on their victim, remove any opportunity of recovery, and maximise the likelihood that their target will be willing to pay, in the instance of ransomware, for example [2].

This means that cyber incident recovery differs. Backups are likely to be deleted or compromised over a period of time. The standard recovery approach exacerbates the situation by reinstalling the malware into the production environment; Restoring a backup compromised with

ISBN: 978-1-68558-186-2

malware will restart the attack process and further extend the recovery times [7].

A. *The Cyber Recovery Process*

NIST's Cyber Incident Response Lifecycle, NIST 800-61r3, incorporates the steps needed to prepare for and recover from a cyber incident (Figure 1) [16].

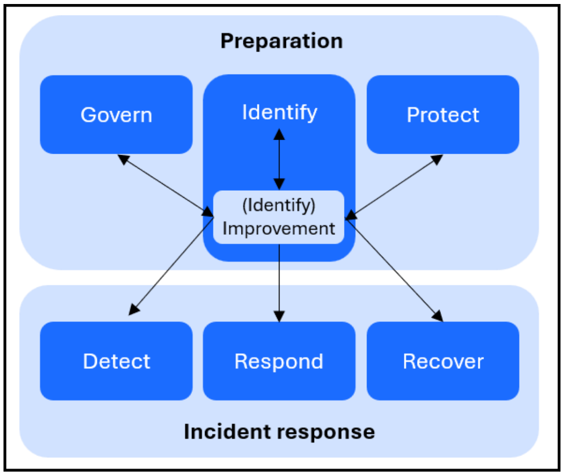


Figure 1. Incident response lifecycle model based on CSF 2.0 Functions [15][16].

In addition to the normal IT recovery steps, cyber recovery incorporates containment and eradication.

1) *Containment*

The purpose of containment is to prevent the threat spreading further across the environment, to reduce the extent of the immediate damage and the opportunity for further exfiltration. If third-parties are needed to help co-ordinate the recovery, or to provide technical guidance or hands-on-keyboard for the recovery actions, now is the time to engage them.

2) *Eradication*

During eradication, the Cyber Security Operations Centre (CSOC) and IT technical support teams work together to ascertain scale of the threat, and assess the extent of the damage or potential damage. Prior to deleting or rebuilding, snapshots of impacted systems, devices, and files need to be taken for the forensic analysts to review [7]. They may be able to map these against known threat actor Tactics, Techniques, and Procedures (TTPs), which will enable the recovery team to predict likely methods and next steps for the attacker. Compromised user accounts are disabled and credentials reset, any malware installed by the threat actor is erased, and vulnerabilities that were exploited during the attack are closed. Immutable backups are scanned to identify any missing or compromised components. Once a clean set of backups are identified, the recovery teams need to establish a clean recovery environment. The unspoiled backups are restored into this secure, clean environment, assured and tested to ensure production readiness. If preparation has not provided secured baseline configuration system-state backup from which to rebuild from, there may be a need to rebuild, reinstall and reconfigure platforms and environments from scratch. Once this has been achieved, patches will need to be installed, passwords updated, and security controls overlayed [16][18].

3) *Recovery*

Only when production readiness is assured, and the team are confident the threat has been contained and eradicated will they be ready to recover the system fully by switch it over to Production [16].

III. Preparing to Recover Rrom a Major Cyber Security Incident

A. *Pre-work*

Prior to working with any specific technology teams or systems, the first step, when preparing to recover from a Major Cyber Security Incident (MCSI), is to understand the organisation's resilience appetite and its tolerance for outages impacting customers [17]. This will provide the basis for system prioritisation, and targets for acceptable recovery times. The second step is to identify the critical IT systems that, if compromised, would have significant impact on the organisation's ability to continue to deliver services. These include access and identification control systems, such as Microsoft's Active Directory, connectivity products, such as VPN & Citrix Netscaler, and data storage, such as private and public cloud.

The IT teams supporting these critical systems will need to be heavily involved in preparing for cyber incident recovery, as they know these systems best. Support from their leaders is essential to ensuring resilience is a priority for these teams, amongst their usual workload. Top-down leader engagement is the most effective approach: Educating leaders and then their teams, ensuring objections are handled, resilience is prioritised, and skilled Subject Matter Expert (SME) resources are made available. Resilience and recovery preparation activities will need to be prioritised and incorporated into the teams' delivery plans or backlogs, to be appropriately allocated to sprints or epics, in line with other priorities in the team's backlogs.

B. *Elements contributing to recover-ability*

There are five elements to be addressed when developing the ability to recover efficiently from a MCSI impacting one or more of company's critical IT systems, in order to meet the organisation's resilience appetite and impact tolerance [17]. These are:

1) *Environmental Remediation*

Work with the IT support team, the cyber red team, and the cyber risk and controls' assurance teams to identify and prioritise environment remediation requirements, such as: vulnerabilities and control gaps;

risks and issues; insecure configurations and misconfigurations; lack of network, system and access segregations; excessive and inappropriate use of privileged access; and poor password management practices. Vendors may be able to provide scanning scripts and threat simulation capabilities to assist with identifying these remediation opportunities. But the platform support teams will have a list of items they know should be fixed. Capture and prioritise all these remediation items. Develop a plan to group them, map them to existing uplift and re-platforming projects and allocate resources to close them. This will significantly lower the initial risk of a cyber incident, slow down the threat actors' transgressions, reduce the blast radius, and streamline recovery. Funding will need to be considered for the big-ticket items, such as retiering or major platform upgrades.

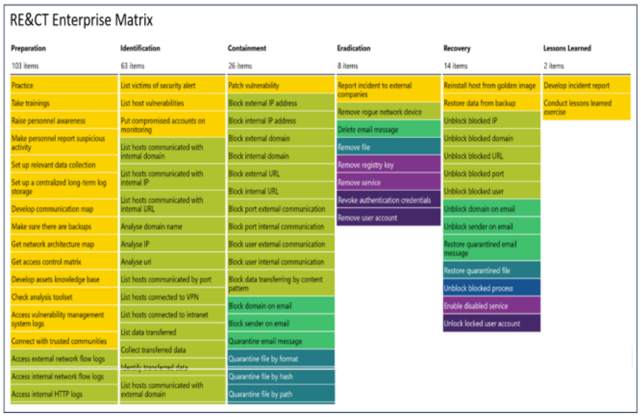
2) Recovery Preparation based on RE&CT

GitHub's RE&CT Enterprise Matrix provides comprehensive guidelines on how to prepare for efficient recovery from cyber security incidents. Based on the MITRE ATT&CK and D3FEND MATRICES, the GitHub RE&CT Enterprise Matrix outlines actions for all stages of the Cyber Incident Response Lifecycle [6][11]-[13][16]. Exhaustive examples are provided for multiple attack sequences in the RE&ACT Enterprise Matrix. They include practical actions that expose assumptions and facilitate comprehensive and complete preparation of capabilities to enable accelerated response. These include basic, but essential items, such as:

i) taking a system-state (golden) image; a snapshot of the baselevel system configuration on critical systems, and storing a clean copy of this in a secure offsite and offline location. This simple mitigation ensures the recovery team won't ever need to rebuild the entire system from scratch, by establishing immutable backups that will be accessible only to those who need them in times of crisis.

ii) building the capability to trigger bulk access revocation and re-enablement, and bulk password resets for compromised accounts, user groups and suppliers' accounts (Figure 2) [3][6].

Use the RE&CT Matrix as a guideline by reviewing each item listed, first determining if this item is relevant to the platform under review, and then assessing whether this has already been addressed, or needs to be actioned. All action items are added to the remediation list to be tracked through to completion.



RE&CT Enterprise Matrix

Preparation	Identification	Containment	Eradication	Recovery	Lessons Learned
103 items	63 items	26 items	8 items	14 items	2 items
Practice	List victims of security alert	Patch vulnerability	Report incident to external companies	Reinstall host from golden image	Develop incident report
Take trainings	List host vulnerabilities	Block external IP address	Remove rogue network device	Restore data from backup	Conduct lessons learned exercise
Raise personnel awareness	Put compromised accounts on monitoring	Block internal IP address	Delete email message	Unblock blocked IP	
Make personnel report suspicious activity	List hosts communicated with internal domain	Block external domain	Remove file	Unblock blocked domain	
Set up relevant data collection	List hosts communicated with internal IP	Block internal domain	Remove registry key	Unblock blocked URL	
Set up a centralized long-term log storage	List hosts communicated with internal URL	Block external URL	Remove service	Unblock blocked port	
Develop communication map	Analyse domain name	Block internal URL	Revoke authentication credentials	Unblock blocked user	
Make sure there are backups	Analyse IP	Block port external communication	Remove user account	Unblock domain on email	
Get network architecture map	Analyse uri	Block port internal communication		Unblock sender on email	
Get access control matrix	List hosts communicated by port	Block user external communication		Restore quarantined email message	
Develop assets knowledge base	List hosts connected to VPN	Block user internal communication		Restore quarantined file	
Check analysis toolset	List hosts connected to intranet	Block data transferring by content pattern		Unblock blocked process	
Access vulnerability management system logs	List data transferred	Block domain on email		Enable disabled service	
Connect with trusted communities	Collect transferred data	Block sender on email		Unlock locked user account	
Access external network flow logs	Identify transferred data	Quarantine email message			
Access internal network flow logs	List hosts communicated with external domain	Quarantine file by format			
Access internal HTTP logs		Quarantine file by hash			
		Quarantine file by path			

Figure 2. RE&CT Enterprise Matrix extract [6].

3) Response-Recovery Scenarios, including who does what.

Validated and assured recovery plans build capability and confidence for swift recovery.

a) Prepare cyber-specific response plans for the most common, and highest impacting threat scenarios.

The IT support teams understand the technology best and as such are major contributors to determining the most streamlined and comprehensive recovery process [16]. The playbooks need to be composed for the average person in the support team to follow, not the most knowledgeable or experienced SME. GitHub's RE&CT site and some vendor sites provides standard recovery playbooks for the common cyber incidents, such as ransomware [6][8]. Complete recovery plans and playbooks are developed by the cyber and IT teams walking through and documenting each cyber scenarios, identifying each step in the recovery process, who is doing that action, and what additional information and/ or materials are needed.

Together, the playbooks will provide end-to-end concise and easy to follow instructions for the team members to follow in the heat of a major incident. When dependencies are identified and accountabilities span more than one team, all the respective specialists need to be involved in developing the complete set of playbooks.

b) Table-top Test

Completeness is assessed through tabletop testing where the CSOC and IT support teams all work together, walking through the playbooks for the chosen scenario, with each person practicing performing their role in the playbook. Testing the set of playbooks end-to-end in conjunction with the CSOC will quickly highlight omissions and refinements needed. Tabletop testing should be repeated until all parties are willing to sign-off on the complete set of playbooks for that scenario.

4) *Vendor engagement to assist with MCSIM.*

Vendor involvement in cyber incidents will depend upon the organisation's sourcing strategy, previous agreements and contractual arrangements. Specialist IT vendors, advisory, and cyber insurance companies offer services to assist with coordinating Major Cyber Security Incident Management (MCSIM) during the event. This will only be effective if they have a clear understanding of the environment, and/ or up-to-date architectural documentation, and recovery playbooks available [16]. Capacity to manage the situation during the event will be heavily reliant on the amount of preparation performed across all the relevant teams prior to the incident.

When vendors are active in supporting the applications and infrastructure, they will have a hands-on-key board role to play during the recovery preparation and incident recovery. In this instance, it is imperative that these personnel participate in the preparation and testing activities, and that arrangements are made during the preparation phase to ensure this assistance will be made available when it is needed. The supplier contracts may need to be updated to include this requirement.

5) *Full MCSI Simulation(s)*

Complex to plan and organise, but well worth the effort, full MCSI simulations enable teams to practice MCSIM and recovery in near-real circumstances. This builds confidence for both the participants as well as the stakeholders observing, and exposes gaps in the preparation plans and playbooks that would otherwise only be discovered during a real incident.

Early engagement with the Crisis Management Teams to garner support and establish communications and co-ordination plans will ensure the simulation is as near to real as it can be.

6) *Post Incident Review*

Whether a simulation or a real event, a Post Incident Review (PIR) provides opportunity for those involved to debrief, capture lessons learned, and apply these to improve the process for next time. The focus is on what worked well, what was needed that wasn't easily available. Aspects to be addressed for next time should all be captured and actioned appropriately to ensure readiness improves with each instance.

IV. Recovery Scenarios

A practical, structured approach to building the recovery plans and playbooks will ensure greatest benefit for least effort.

A. Focus on common scenarios

Rather than attempt to develop playbooks that address every attack sequence, organisations can be prepared for the majority of potential situations by focusing on the most likely, largest scale and biggest impacting MCSI threat scenarios they will need to be able to recover efficiently from. By preparing for these scenarios, incident management and recovery teams will be in a strong position to recovery from most:

1) *Nation State Actor*

The cyber security intelligence team will be able to provide insight into the likely nation state threat actors and their typical TTPs. As an example, the People's Republic of China's (PRC) Volt Typhoon has been active since at least 2021. This group has been observed targeting critical infrastructure organisations where it has been actively performing information gathering and espionage. More recently Volt Typhoon has been attributed as the cause of critical infrastructure outages across the United States. The Volt Typhoon TTPs are based around "stealth in operations using web shells, Living-Off-The-Land (LOTL) binaries, hands on keyboard activities, and stolen credentials" [12].

2) *Ransomware*

Ransomware is highly visible and noisy due to its direct impact on the business users. By the time the threat actor has triggered the ransom message, files will have been exfiltrated, encrypted, backups deleted or compromised, configuration files, applications and data sets across the domain infected with malware. This can take moments or weeks, but the recovery team can safely assume that they are dealing with a broadly compromised environment. Two-way communication with the impacted users will help ascertain the extent of the impact as well as providing confidence to the users that their data will be recovered, in some form.

Recovery steps will need to address every aspect of the infection in order to contain and eradicate it, including and well beyond the encrypted files and backups. Depending on the extent of the infection, systems may need to be recreated. Preparation will include implementing regular immutable system-state backups along with clean, secure recovery environments for the recovery of critical systems.

3) *Dormant Threat (Prestaging)*

Dormant threat is very similar to ransomware in the early phases. This is when the threat actor is discovered before they trigger the blast. Malware payloads will have been deployed across the environment, including backups. The recovery team can expect that data, systems, and configuration files are already compromised. Containment will be similar to ransomware, without the need to replace encrypted files or the corresponding noise from the impacted users.

4) *Third Party*

Ahead of the event, the recovery team will need to generate a list of critical third-party suppliers, to understand the services they provide and their methods for access. In the situation when a supplier is compromised, the recovery team needs to be able to remove connectivity between the organisations swiftly and completely. Access accounts will need to be disabled in a seamless and timely manner while the supplier focuses on containing the threat in their environment. Business processes will need to be pre-prepared to ensure they can function independently through this period.

Detection testing should determine if the infection has spread from the suppliers into the primary organisation's environment, and appropriate containment actions taken if it has. When the supplier can confirm they have completely eradicated and recovered from the threat, only then should the connection between the two organsations be re-established, and the vendor's user accounts re-enabled.

5) *Zero Day – No patch available*

When a critical system is vulnerable to a threat actively exploiting an unpatchable zero day, then compensating controls need to be implement to protect the critical system. The simplest mitigation is to take the platform offline, but this may not be possible for key systems used by the business so alternatives need to be investigated and tested.

6) *Supply Chain*

The organisation needs to be prepared for when the operating system or software update has already been infected, as was the case in the SolarWinds compromise [10]. Preparing for a supply chain compromise involves a full review of the software deployment strategies to ensure software is always deployed in stages and tested prior to full deployment. This will ensure only limited platforms/ devices are impacted. Additionally, all deployments will need to have a rollback strategy. This may be a straight-forward as uninstalling the update, or may involve taking a backup prior to deployment to enable an immediate restore if/ when it is needed.

B. *Building recovery plans and playbooks*

In the heat of a major incident, the recovery teams will have limited capacity to guess the next step or make-it-up on the fly. They will need to have a complete set of logically structured recovery plans with comprehensive playbooks to address all the interdependencies and actions to be performed by each of the teams involved. Teams include the Crisis management team, to co-ordinate external communications and business continuity, the CSOC, who typically co-ordinate cyber incident response and recovery activities, the relevant IT support teams, any vendors involved as incident co-ordinators or extended support team members with hands-on-keyboards, business and technology leaders, communications specialists etc.

In addition to the playbooks, the recovery plans include fundamentals, such as: lists of responsible personnel for each system with contact details, and rosters for extended outagess; pre-established communications plans and virtual war-rooms and bridges for keeping the resolver teams and other stakeholders up to date; data capture methods for later forensics activities; and handover procedures to ensure progress continues smoothy for outages spanning more than twelve hours [16].

While basic playbooks can be sourced online through CISA [3] Microsoft [8], for example, these are very generic and do not relate to the specific environment in the organisation. Hence, their value is limited. Alternatively, if the organisation has engaged a vendor to lead their critical incident management, then this vendor may be leaned upon to provide the CSOC playbooks for the IT playbooks to plug into.

V. Recovery Testing and Continuous Improvement

Recovery plans are initially table-top tested with each person walking through their role in the playbook. Each IT team and the CSOC team bring and use their respective playbooks to ensure they fit together, end-to-end. Regular reviews, every 6-12 months, ensure the approach is continuously improved throughout the process. Once complete, these recovery plans need to be reviewed and updated, as part of operational readiness, whenever there is a change.

Once a set of recovery play books has been completed, a full MCSI simulation, with each person performing their role, is the most effective way to test the plans and identify any gaps ahead of the real event. If the MCSI simulation identifies significant gaps and delays, these need to be addressed and retested within 3 months. Once these simulations run more smoothly, MCSI simulation should be run every 6 months to ensure everyone knows their role in the event of a major incident, or cyber-initiated crisis. The cyber security intelligence team can provide guidance on suitable scenarios for MCSI simulations, based on what they are observing in the cyber threat landscape.

When an organisation has been significantly compromised, access to operational document storage systems may be hampered. It is recommended that an alternative site is established in which to store crisis management and MCSIM documentation. This will ensure these essential instructions are available when they are needed.

VI. Organisational Challenges

A. *Resistance and avoidance*

Both the CSOC and the IT personnel will be busy dealing with their day-to-day response and support activities. Leader intervention will be needed to direct them to prioritise these MCSI preparation activities. Fear of failure and lack of cyber awareness may trigger resistance in those who should be involved. Resistance comes in many forms. The most common is avoidance: "don't understand the ask," "don't have capacity to get involved" or "too busy". These will need to be actively and persistently addressed by leadership.

B. *Lack of cyber knowledge*

It cannot be assumed that the IT personnel have any understanding of cyber security, or any of the additional considerations and actions required when recovering from a cyber incident. This is best taught early during or before the preparation phase, rather than in the heat of a major incident. Education sessions need to start with the very basics. With explanations of how cyber attacks work, the fundamentals of TTPs, and the types of systems and data being targeted [9]. Compromise scenarios should be explained in detail so these IT professionals begin to understand what they will be facing in the event, and how they can be prepared.

VII. Metrics

Two sets of metrics need to be considered. Those relating to recovery readiness, and those that relate to the recovery times.

1) Recovery readiness

Recovery readiness is just that. How ready are the teams to recover from a MCSI. Readiness can be assessed by tracking the completeness and effectiveness of the preparation products outlined: Cyber incident recovery plans complete, end-to-end, for the top six cyber scenarios; Table-top testing completed within the last 6 months, and all shortcomings addressed; Remediation items addressed; Control gaps closed; React matrix preparation steps completed. Full crisis simulation testing completed within the previous 2 years for this technology platform; and Contact lists maintained.

2) Recovery times

MCSI are less frequent than IT major incidents. This limits the value of measuring Mean Time To Recover (MTTR) for a MCSI, but it does not detract from the ability to measure recovery times for full crisis simulations. By setting targets to reduce MTTR, teams identify and address delays, with the ultimate objective of aligning recovery times with the organisation's resilience appetite and impact tolerance.

VIII. Conclusion

Compromise of critical systems can cripple an organisation. Preparation will mean the difference between taking minutes or hours to recover from a MCSI rather than days, weeks or even months. A structured approach to prepare for and practice managing such incidents will build corporate capability and confidence in those responsible. This paper outlined a practical approach that organisations can apply when bringing together their IT and CSOC team to prepare for the worst, rather than hope for the best.

References

[1] ASD, "Essential eight maturity model," Australian Signals Directorate, Australian Cyber Security Centre, Available from: https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model, accessed 24 Aug 2024.

[2] M. Benmalek, "Ransomware on cyber-physical systems Taxonomies, case studies, security gaps, and open challenges," [p.1, p.190, 2023], Available from: https://www.researchgate.net/publication/377211197_Ransomware_on_cyber-physical_systems_Taxonomies_case_studies_security_gaps_and_open_challenges, accessed 24 August 2024.

[3] CISA, "Federal Government Cybersecurity Incident & Vulnerability Response Playbooks," 2024, Available from: https://www.cisa.gov/sites/default/files/2024-03/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf, accessed 15 July 2024.

[4] CISC, "Security of Critical Infrastructure Act 2018 (SOCI)," Available from: https://www.cisc.gov.au/legislation-regulation-and-compliance/soci-act-2018, accessed February 2024.

[5] J. Ford and H. S. Berry, "Leveling Up Survey of How Nation States Leverage Cyber Operations to Even the Playing Field," 2023, Available from: https://www.researchgate.net/ publication/371084176_Leveling_Up_Survey_of_How_Nation_States_Leverage_Cyber_Operations_to_Even_the_Playing_Field, accessed July 2024.

[6] Github, "RE&CT Enterprise Matrix, MITRE ATT&CK® Navigator v2.3.2," Available from: https://atc-project.github.io/react-navigator/, accessed June 2024.

[7] G. Johansen, "Digital Forensics and Incident Response: Incident response tools and techniques for effective cyber threat response, " Packt Publishing, 2022.

[8] Microsoft Learn 2022, "Incident response in the Microsoft Defender portal - Microsoft Defender XDR," Available from: https://learn.microsoft.com/en-us/defender-xdr/incidents-overview#incident-response-workflow-example-in-the-microsoft-defender-portal, accessed 15 July 2024.

[9] Mandiant, "APT1: Exposing One of China's Cyber Espionage Units," Available from: https://www.mandiant.com/resources/reports/apt1-exposing-one-chinas-cyber-espionage-units, accessed July 2024.

[10] MITRE ATT&CK^1, "SolarWinds compromise, campaign C0024," Available from: https://attack.mitre.org/campaigns/C0024/, accessed February 2024.

[11] MITRE ATT&CK^2, "Matrix - Enterprise," Available from: https://attack.mitre.org/matrices/enterprise/, accessed February 2024.

[12] MITRE ATT&CK^3, "Volt Typhoon, BRONZE SILHOUETTE, Group G1017," Available from: https://attack.mitre.org/groups/G1017/, accessed April 2024.

[13] MITRE D3FEND 2023, "D3FEND Matrix," Available from: https://d3fend.mitre.org/, accessed July 2024.

[14] NIST^1, "Security and Privacy Controls for Information Systems and Organizations (nist.gov)," Available from: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf, accessed April 2024.

[15] NIST^2, "The NIST Cybersecurity Framework (CSF) 2.0," [p.15], Available from: https://nvlpubs.nist.gov/ nistpubs/CSWP/NIST.CSWP.29.pdf, accessed February 2024.

[16] NIST^3, "NIST SP 800-61r3 initial public draft, Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile," [p.1, p.10. p.22], Available from: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.ipd.pdf, accessed 24 August 2024.

[17] PWC, "Operational resilience: hoe to set and test impact tolerances," Available from: white-paper-on-impact-tolerances-feb-2020.pdf (pwc.co.uk), accessed 27 August 2024.

[18] D. Schlette, M. Caselli and G. Pernul, "A Comparative Study on Cyber Threat Intelligence: The Security Incident Response Perspective" in IEEE Communications Surveys & Tutorials,

Copyright (c) IARIA, 2024. ISBN: 978-1-68558-186-2

vol. 23, no. 4, pp. 2525-2556, Fourthquarter 2021, doi: 10.1109/COMST.2021.3117338. Available from: https://ieeexplore.ieee.org/document/9557787, accessed 24 August 2024.

[19] J. Steinke, B. Bolunmez, L. Fletcher, V. Wang, A. J. Tomassetti, K. M. Repchick, S. J. Zaccaro, R. S. Dalal, and L. E. Tetrick, “Improving cybersecurity incident response team effectiveness using teams-based research,” 2015, IEEE Security & Privacy, vol. 13, no. 4, pp. 20-29, July-Aug. 2015, doi: 10.1109/MSP.2015.71, Available from: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7180274, accessed 24 August 2024.

ISBN: 978-1-68558-186-2