THE CYBER FIRST AID KIT

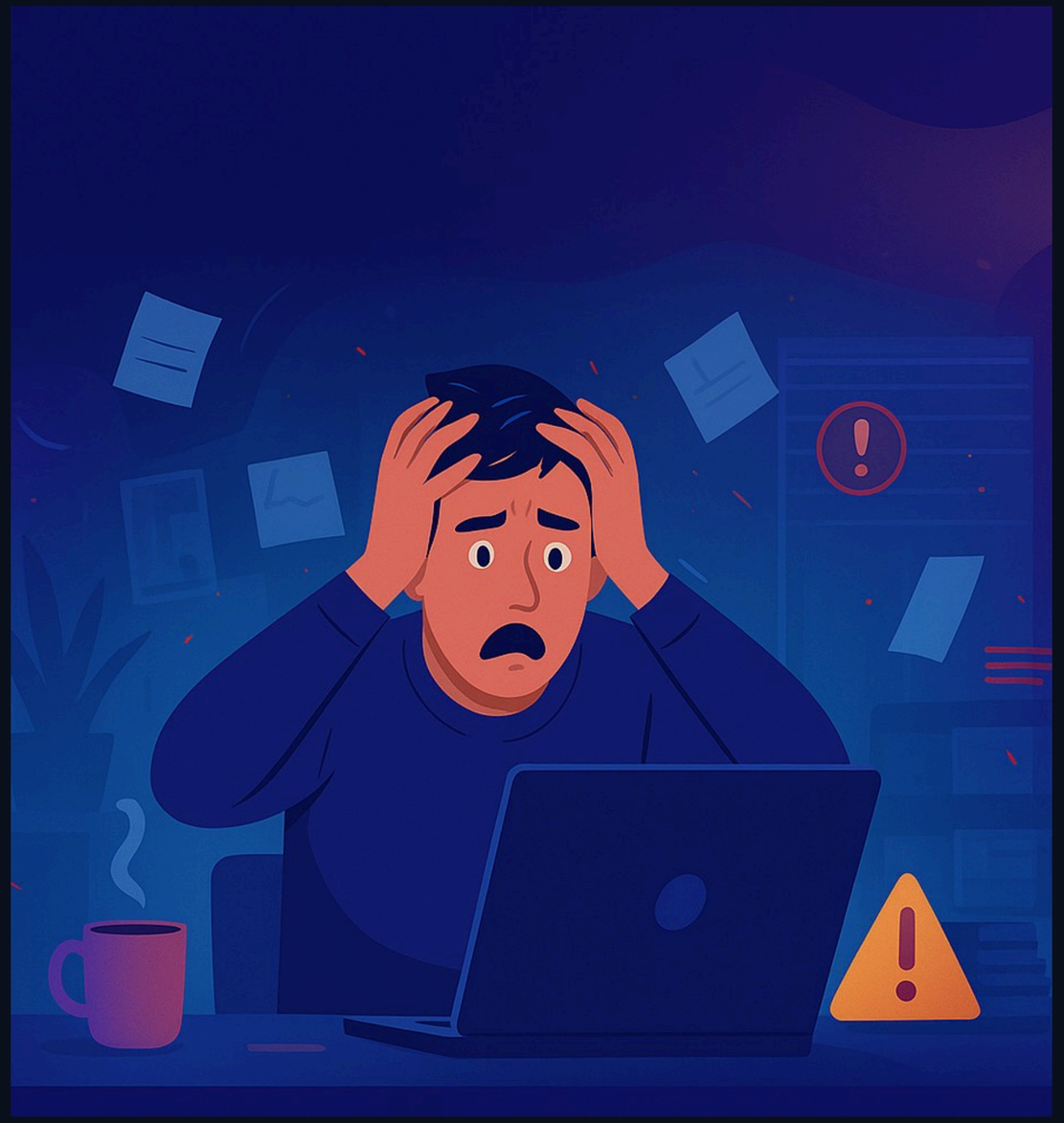
BY NELSON SAMUEL

REALITY

When it comes to Cyber incidents, its not a matter of *if* but *when.* Many organizations lack a tested incident response plan increasing recovery costs by as much as 40%. With 63% of businesses worldwide reporting to have been affected by a cyber attack the need for prevention and incident response teams rises each day.

PURPOSE

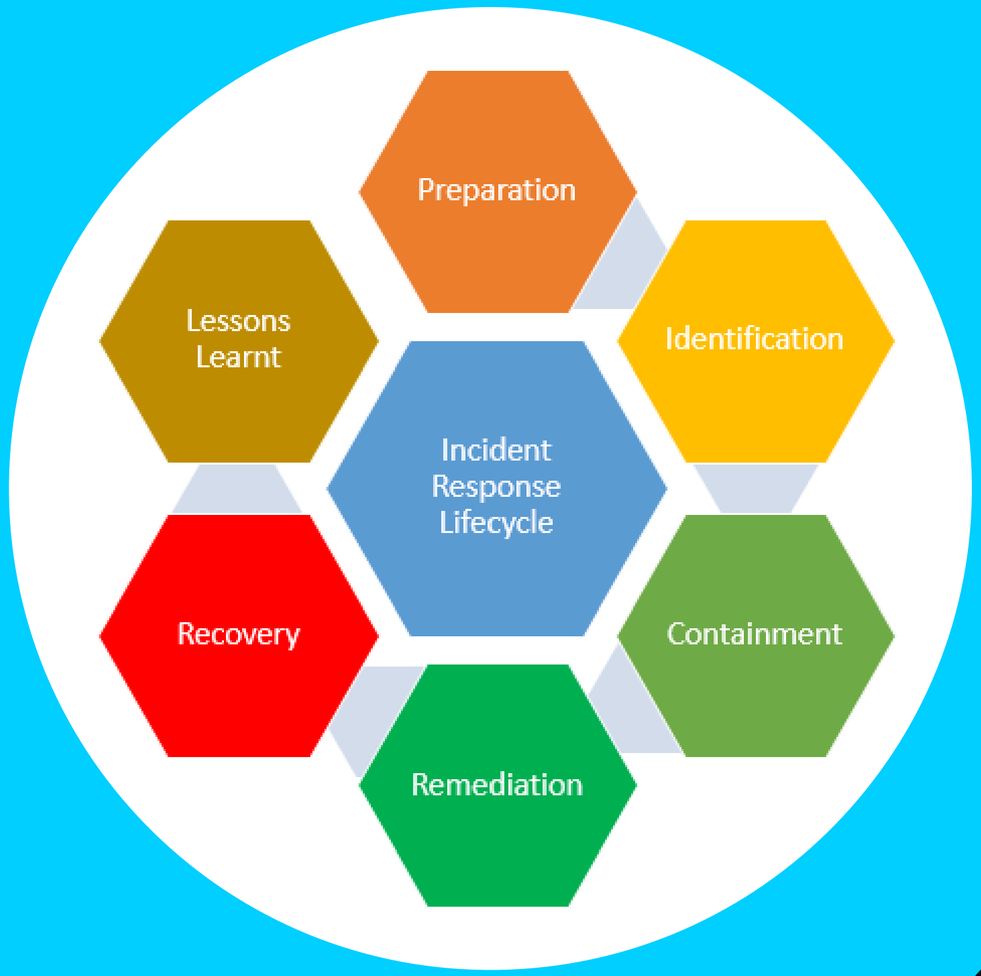
This playbook is about fast, structured and business-focused recovery. It gives a preview of what incident response entails and the *Dos* and *Donts* when hit with a cyber attack.



WHAT IS INCIDENT RESPONSE (IR)

- Incident response is like having a fire drill for your business but instead of smoke and flames it’s hackers, malware, and data leaks.
- In formal terms, IR is a structured methodology for handling cyber security incidents and breaches with an aim to recover from attacks while minimizing damage and desruption

THE INCIDENT RESPONSE LIFECYCLE



1. PREPARATION: Involves defining clear policies,acquiring the right tools and training.
2. IDENTIFICATION: Confirming whether and event is a cyber attack and evaluating its intensity.
3. CONTAINMENT: Isolating the affected systems to prevent further damage.
4. ERADICATION: Investigating the root cause of the incident and eradicating any threats.
5. RECOVERY: Restore affected systems to the pre-incident state and restore operations.
6. LESSONS LEARNT: Review,document everything that occured and monitor continuously.

COMMON CYBER INCIDENTS BUSINESSES FACE

- Phishing and Business Email Compromise
- Ransomware and Data Encryption
- Insider Threats (Malicious Employees)
- Cloud Service Breaches
- Distributed Denial of Service attacks (DDoS)

The impact of these incidents; loss of data, downtime, legal exposure. Yeah, you do not want that ⚠️

DOS AND DONTS WHEN HIT WITH A BREACH

DO	DON'T
• Stay calm and try not to panic. Panic spreads faster than malware clouding your judgement.	• Don't ignore it. That weird tone on your HR's email might actually be a phishing attempt. Follow up and consult with IT.
• Notify the Incident Response team immediately about the alleged issue.	• Don't try to fix it yourself, you might worsen it.
• Disconnect compromised systems from the network. DO NOT SHUT THEM DOWN.	• Again I repeat, Don't shut down any affected system as this might make forensics harder.
• Document and keep notes of every detail happening including timelines.	• Finally, Don't spread the word especially on public places and platforms without approval.

BEST PRACTICES

- Invest in an Incident Response Team
- Have an Incident Response Plan
- Backup your data regularly
- Keep systems updated
- Offer awareness and training for employees
- Regular security reviews including IT audits.
- Use Multi-factor Authentication

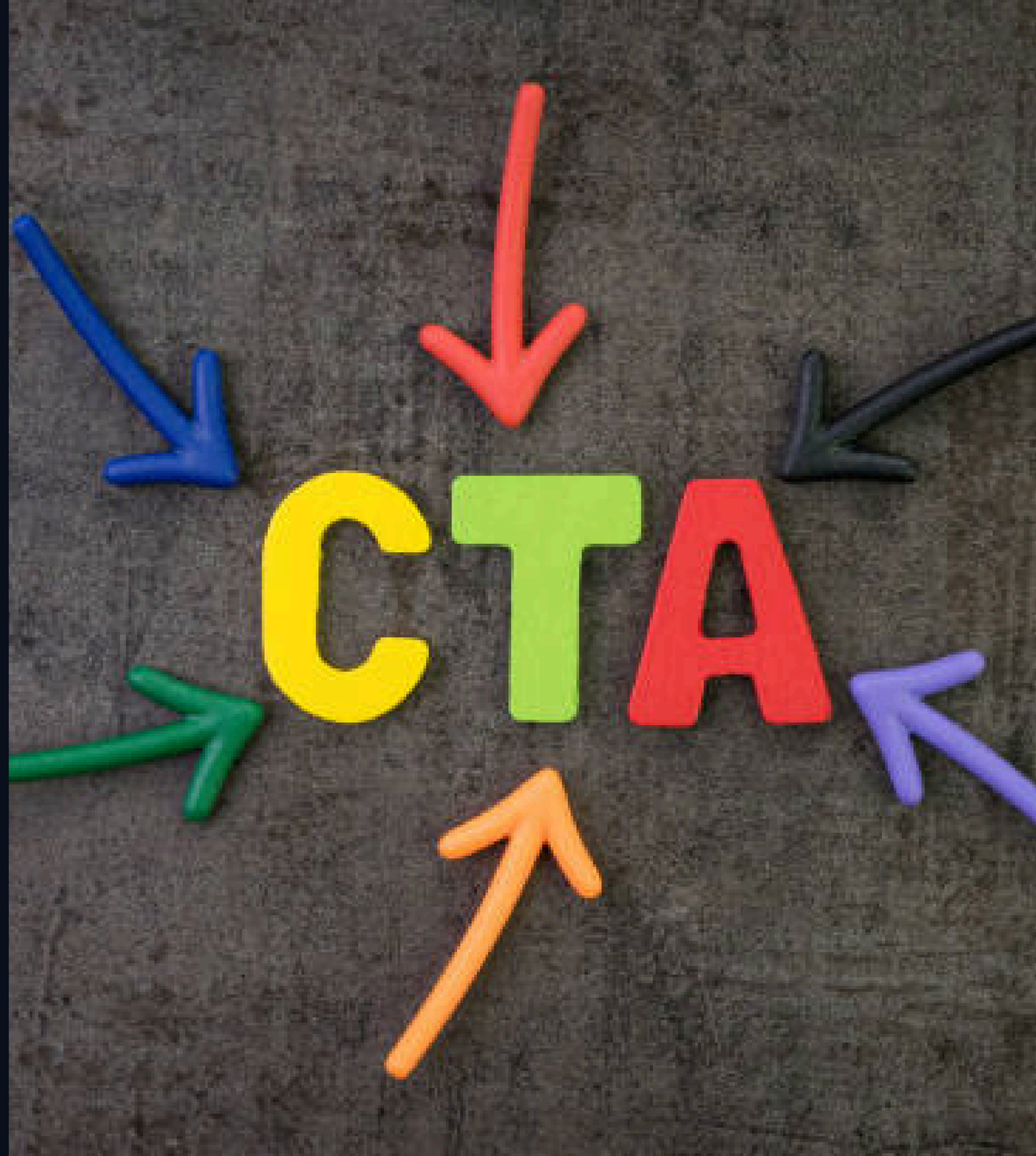
This is Jane. Jane’s organization has been hit by a ransomware. Jane does not have an IR team or plan. Jane is in super panic. Business operations have halted. DON’T BE LIKE JANE.

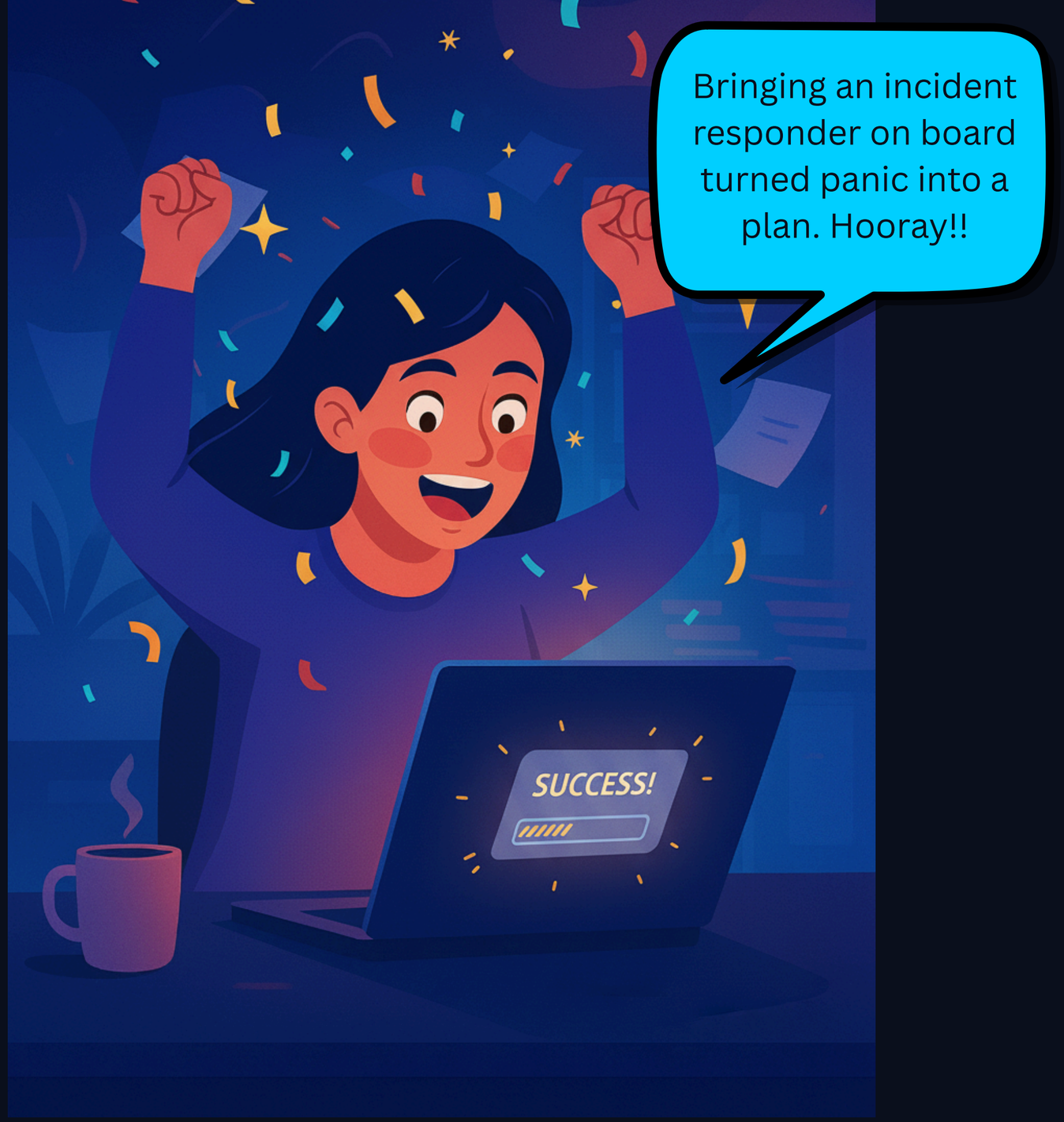
CALL TO ACTION

- Remember that this playbook is a preview. A real IR plan is customized to your business.

Book a 30 min Cybersecurity Readiness Consultation

Contact: +254 746 392 370
Connect with me on:
https://www.linkedin.com/in/nelson-samuel-0164792b5




Bringing an incident responder on board turned panic into a plan. Hooray!!
SUCCESS!

THANK YOU

Thank you for taking the time to explore this playbook Remember that cybersecurity is about readiness, resilience and response. When a breach happens every second matters and that’s when you need a Digital First Responder.

Nelson Samuel
Digital First Responder