ADARMA
TOGETHER WE'VE GOT THIS

INCIDENT-READY: What You Should Do Before a Major Cyber Event

Introduction

A significant cyber incident can have severe consequences for any organisation. Financial losses, reputational damage, regulatory penalties, and operational disruptions are just some of the risks businesses face if they are not adequately prepared.

Cyber resilience is no longer a luxury; it is a necessity. The key to minimising the impact of a cyber incident is thorough preparation. This eBook outlines the critical steps an organisation needs to take to prepare for and respond to a cyber incident effectively. From proactive risk management to post-incident recovery, these strategies will help strengthen your cybersecurity posture and ensure a swift, coordinated response to any cyber incident.

Step 1: Establish a Robust Incident Response Plan (IRP)

A well-documented IRP is the foundation of cyber preparedness. This plan should outline roles, responsibilities, and clear steps to take during a security incident.

Key components of an effective IRP:

- **Incident Classification:** Assign and design different levels of security incidents and how they should be handled.
- **Roles and Responsibilities:** Assign clear responsibilities to security teams, IT, legal, communications, and executive leadership.
- **Communication Plan:** Outline internal and external communication protocols to ensure a coordinated response.
- **Incident Escalation Process:** Define when and how an incident is escalated to senior leadership or external cybersecurity experts.
- **Regulatory and Legal Considerations:** Ensure compliance with GDPR, NIST, ISO 27001, and any industry-specific regulations.

Action Step: Regularly review and update your IRP to reflect new threats, technologies, and regulatory changes.

Step 2: Conduct Regular Cyber Crisis Simulations

ADARMA
TOGETHER WE'VE GOT THIS

Cyber crisis simulations are essential to ensure that your teams are ready to respond under pressure. These exercises test your Incident Response (IR) capabilities and help identify vulnerabilities in your current strategy.

Types of crisis simulations:

- **Tabletop Exercises:** Scenario-based discussions involving key stakeholders.
- **Functional Simulations:** Hands-on exercises testing specific response actions.
- **Purple Team Exercises:** Simulated attacks (Red Team) to test defensive (Blue Team) measures in real-time.

Action Step: Conduct cyber crisis simulations at least once a year to refine your response strategy and improve team coordination.

Step 3: Implement Proactive Threat Detection and Monitoring

Early detection of cyber threats can prevent an incident from escalating. Organisations must deploy advanced threat detection and monitoring tools to identify and respond to attacks in real-time.

Key measures include:

- **Security Information and Event Management (SIEM):** Aggregates and analyses security logs to detect anomalies.
- **Extended Detection and Response (XDR):** Provides deeper visibility across endpoints, networks, and cloud environments.
- **Threat Intelligence Integration:** Uses real-time intelligence to stay ahead of evolving threats.
- **Vulnerability Management:** Continuously scans for security weaknesses and prioritises patching efforts.

Action Step: Ensure your Security Operations Centre (SOC) is equipped with the latest monitoring capabilities to detect and respond to threats proactively.

Step 4: Implement Strong Access Controls and Data Protection

Data breaches often occur due to weak access controls and inadequate data protection measures. Strengthening security at these levels can significantly reduce the risk of a cyber incident.

Best practices for access control:

- **Multi-Factor Authentication (MFA):** Enforce MFA across all critical and personal systems.
- **Zero Trust Security Model:** Grant users the minimum necessary access based on need-to-know principles.
- **Privileged Access Management:** Secure accounts with elevated permissions to prevent misuse.

Best practices for data protection:

- **Regular Data Backups:** Ensure that backups are encrypted, stored securely, and tested regularly.
- **Data Encryption:** Protect sensitive data at rest and in transit using encryption protocols.
- **Endpoint Security:** Deploy endpoint protection solutions to safeguard devices against malware and ransomware.

Action Step: Regularly review user access permissions, enforce strict security controls for sensitive data and use MFA wherever possible.

Step 5: Ensure Effective Communication During an Incident

Clear communication is essential to managing a cyber crisis effectively. Miscommunication or delayed response can worsen the situation and lead to increased financial and reputational damage.

Essential elements of a cyber incident communication plan:

- **Internal Communication:** Ensure key stakeholders are informed and aware of their roles. Establish a contingency plan for communicating both online and offline in the event normal communication channels are impacted by the incident.
- **External Communication:** Prepare predefined messages for customers, partners, and regulatory bodies.
- **Media Handling:** Train spokespersons to address the media and mitigate reputational risks.

Action Step: Develop a crisis communication playbook to ensure consistent messaging during a cyber incident.

Step 6: Establish a Post-Incident Recovery and Learning Process

ADARMA
TOGETHER WE'VE GOT THIS

Once an incident is contained, recovery and learning from the event are crucial. A structured post-incident review ensures that mistakes are not repeated and defences are strengthened.

Key post-incident activities:

- **Problem Management:** Identify how the breach occurred and take corrective actions to prevent the incident from materialising again.
- **Update IR Playbooks:** Refine response strategies based on lessons learned.
- **Strengthen Security Controls:** Implement additional security measures to reduce risk of future incidents.
- **Educate and Train Employees:** Improve awareness and conduct regular training exercises based on learnings.

Action Step: Conduct a formal post-mortem after every major incident to improve your security posture.

The Role of Adarma in Cyber Incident Preparedness

ADARMA
TOGETHER WE'VE GOT THIS

At Adarma, we help organisations enhance their incident preparedness and response capabilities through expert-led assessments, crisis simulations, and tailored security strategies.

Our services include:

- Cyber Crisis Simulations: Stress-testing your organisation's response in real-world scenarios.
- IRP Planning: Ensuring you have a structured plan to minimise the impact of cyber incidents.
- SOC Maturity Assessments: Evaluating and improving your SOC's detection and response capabilities.

How Adarma Can Help

Cyber incidents are inevitable, but how well an organisation responds determines the severity of the impact. By taking proactive steps to prepare, businesses can minimise damage, recover faster, and maintain trust with customers and stakeholders. Partner with Adarma to develop a tailored incident preparedness strategy that aligns with your business needs and risk profile.

From establishing an IR plan and conducting cyber crisis simulations to strengthening security controls and improving communication, organisations must take an integrated approach to cybersecurity preparedness.

Let Adarma help you build resilience and prepare for the unexpected. Contact us today to learn how our expertise in cyber crisis management can protect your organisation's future.

Get in touch

If you would like to speak to an Adarma consultant about any issue, please contact us at **hello@adarma.com**.

ADARMA

TOGETHER WE'VE GOT THIS

hello@adarma .com

www.adarma.com