CYBER INCIDENT RESPONSE EXECUTIVE CHECKLIST.

Cyber security is a harsh taskmaster. You can do everything by the book and still get breached – but it isn't the end of the world and, provided you've planned appropriately, most businesses can recover from a cyber incident.

Having a clear response strategy and incident plan which helps get your business back on track with minimal disruption will lessen the effectiveness of the attack. It may also help you avoid a situation where your organisation is forced to recover data or system access from an untrustworthy cyber-criminal.

This checklist has been developed as a tool to help your organisation refine your own incident response plan, so should the worst happen, you have a good frame of reference and understanding of what factors should be covered.

The specific areas listed below can change depending on each organisation's requirements, but generally speaking this can be used as a good high-level document for your executive team and board to work through.

SETTING UP A "WAR ROOM"

The war room is an essential tool in any incident response (IR). This is the centralised command centre, established to foster collaboration so your team can efficiently work together to fight off cyber security incidents. As part of your IR plan, we recommend setting up dedicated war rooms – both a physical space, as well as online conferencing channels.

INCIDENT CONTROLLER

Appoint an incident controller to lead your response. This could be your internal CISO or security lead, or an external professional experienced in managing a serious cyber incident.

ENLIST THE RIGHT SUPPORT

It's a good idea to ensure you have the right people ready to assist, should you fall victim to a breach or cyber-attack. If you don't have the expertise inhouse to manage any of the activities below, or you are dealing with a major attack that requires specialist support, make sure you set up relationships with relevant agencies and professionals in advance, and discuss the role you'd like them to play in your response plan.

THESE COULD INCLUDE

- PUBLIC RELATIONS AGENCY
- FORENSIC IT ANALYST
- LAW FIRM
- INSURANCE COMPANY
- CYBER SECURITY CONSULTANCY
- EXPERIENCED INCIDENT CONTROLLER

Kordia has supported customers to develop and refine their incident response plans, as well as to mitigate and minimise damage during a crisis. We're on hand to support you before, after and during an incident, with our dedicated Incident Response practice.

GOVERNANCE

□ Reallocate or provide additional resources to other business units during the recovery effort as needed

□ Establish the organisation's stakeholder expectations - board of directors, shareholders, supporters, adversaries, participants, and partners in the value chain

□ Conduct an initial business impact assessment and ongoing assessment of the cyber security incident

□ Set a cadence of periodic debriefing sessions with the incident controller to monitor progress and determine problem areas as the incident progresses or parameters change

□ Assess whether critical business / customer services are impacted, and whether these can be isolated and contained

□ Provide updates to the board

□ Ensure that the following policies and standards are maintained during the recovery effort:

- Financial security and control policies
- Anti-fraud policies
- Information security standards

□ Determine if the severity of the cyber security incident impact requires implementation of the recovery plan. Determine recovery objectives including:

- Priorities
- Recovery strategies
- Action plans
- Assignments

□ Establish clear communication channels between any separate units or personnel that are dealing with different aspects of response or recovery efforts

□ Ensure that the incident controller has a clear, direct line of communication to relate threats in a timely manner to you and to the board

□ Review your organisation's business continuity or disaster recovery plan, as there may be specific requirements and action items mandated to implement BCP or DR plan(s)

□ If you have cyber insurance, call the insurance company to alert them of the incident

LEGAL

In the event of a ransomware attack:

Establish some key facts. Ask your team to confirm the following:

- □ Has communication been made by the attackers?
- □ Has a demand for payment been made?
- □ Evaluate the relevant regulatory and legal guidance for ransomware in your operating environment
- □ Assess risks involved with paying a ransom
- □ Liaise with local law enforcement
- □ Does the organisation need to engage an outside forensics investigation team or ransomware negotiation consultant? (these vendors should be engaged by outside counsel acting on behalf of the company to maintain legal privilege).

- □ Manage all required regulatory notifications

- □ Provide legal counsel for response and recovery operations

- □ Work with legal specialists to identify liabilities and escalate these

- □ Review and approve new contracts acquired as a result of the event, before implementation

- □ Contact the insurance company. Understand their requirements and any specific steps that may need to be taken to protect forensic data or evidence

- □ Coordinate with insurance broker on the preparation and filing of all insurance claims
  - Document proof of losses
  - Submit claims and monitor payments

- □ After consultation with legal counsel and management, determine whether involving law enforcement and/or any regulator is necessary, prudent or valuable

- □ Determine whether legal counsel (in-house or external) should participate in the interviews (individuals involved in discovery and initial investigation of a breach) or be present if law enforcement also requests interviews with relevant personnel.

EXTERNAL COMMUNICATIONS

Ensure to establish key facts for your communications team, including:

- □ How did this happen?
- □ What data did they get?
- □ Have you notified customers?
- □ What are you doing?

□ Create a holding statement

□ Establish key stakeholder and channels to reach (update) them

□ Identify a spokesperson(s)

□ Monitor and log media and social media interest.

□ Ensure all incident responders are reminded of their obligations in regard to comments made externally of the organisation

□ Prepare a media statement

□ Establish a phone number / contact for media inquiries

INTERNAL COMMUNICATIONS

□ Ensure the communications lead is communicating or reiterating the company's rules of disclosure to its employees, especially what should or should not be communicated via public channels like social media, the press, as well as with clients

□ Prepare key messages, Q&A and FAQ's and share with colleagues

□ Establish a central point of information distribution and update

CUSTOMER AND REGULATOR NOTIFICATION

□ Ensure the internal legal team has been engaged if Personal Identified Information (PII) or sensitive information has been impacted

□ Where applicable, NCSC has been notified of the cyber security incident

□ If a Data Breach, Privacy Commissioner's Office has been notified of the details of the Data Breach. Ensure the Data Breach Escalation Procedures are adhered to https://www.privacy.org.nz/responsibilities/privacy-breaches/notify-us/

□ When your organisation becomes aware of an incident of unauthorised access to sensitive customer information, follow notification best practices and notify the affected customer(s) as soon as possible

□ Ensure notification process and procedures are adhered to in line with policy

NOTIFICATION OF THIRD PARTIES / KEY SUPPLIER

□ Remind the communications team to communicate or reiterate the company's rules of disclosure to its Third Parties / Suppliers, and to address what should or should not be communicated via public channels like social media, the press, as well as with clients

□ Set up lines of communication to local authorities and first responders if relevant

HUMAN RESOURCES

□ Coordinate employee communications with corporate communications

□ Coordinate additional or temporary staffing for recovery efforts

□ Put into place response and recovery well-being plans, and provide employee counselling services as required

□ Provide local transportation during response and recovery activities as required, including travel arrangements and accommodations for employees travelling to any remote recovery locations

FINANCE

□ Ensure funds are available for recovery

□ Manage all incident related purchasing

□ Ensure that all recovery expenditures are properly documented

□ Set up a recovery cost centre

□ Estimate the impact of the incident on the company's financial statement

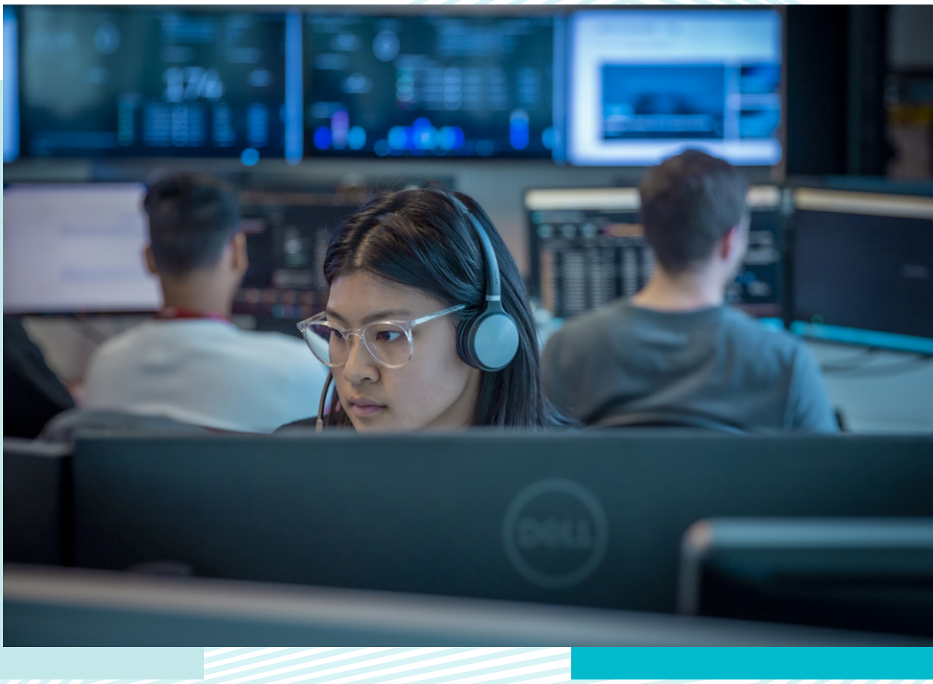
REVIEW

□ Ensure a Post Incident Review (PIR) is conducted to identify lessons learnt across people, process and technology

□ Are there processes, procedures or policies that need to be improved?

□ Ensure action points are assigned to improve the internal security posture

□ Ensure that any backdoors that the adversary introduced are closed and tested



kordia®

For more information on cyber security call

0800 KORDIA | KORDIA.CO.NZ