CRITICAL INCIDENT MANAGEMENT PLAN
Business Cyber Attack

Incident:

- Business Cyber Attack

Guiding principles:

- Critical Incidents take precedence
- Delegate functions and duties
- Put people first
- Always be professional and ethical
- Work logically through your Critical Incident Plan
- Be proactive, not reactive
- Deal only in the facts, keep an open mind, never assume anything
- Document everything, including time, date, place
- Consider preservation of your brand

Immediate Response Action (1 – 2 hours)

- **Goal:** stop the situation getting worse, preserve evidence, get the right people involved quickly
- Do not try to "fix" the problem by deleting files, rebooting affected systems, or paying any ransom demand
- Disconnect affected devices from the network (unplug ethernet, turn off Wi-Fi). **Do not power them off** – (this preserves evidence for forensic review)
- Notify the Incident Controller immediately, in person or by phone (not email, which may be compromised)
- Incident Controller activates this plan and assembles the response roles listed
- Change passwords for any accounts that are still accessible, especially banking, payroll, and admin/email accounts, starting with the most critical
- Enable multi-factor authentication wherever it is not already on
- Contact the bank's fraud team immediately if there is any chance banking or payment systems have been accessed, to freeze or monitor accounts
- Contact your cyber insurance provider before engaging external IT/forensic help, if you hold a policy

Copyright 2026 © by Mastercraft Services (NZ) Ltd

- Report the incident to CERT NZ via Own Your Online (0800 CERT NZ / www.ownyouronline.govt.nz) for triage and guidance
- Start the incident log below immediately - record every action, time, and decision

Incident Response Roles

Having clear ownership of each area prevents confusion and duplicated effort during a stressful event.

Role	Suggested Owner	Core Responsibilities
Incident Controller	Owner / General Manager	Overall decision-making authority. Activates the plan, approves communications, decides on ransom/payment questions, liaises with insurer and legal counsel, declares the incident over.
IT/Technical Lead	External IT provider / internal IT-capable manager	Technical triage, isolates affected systems, works with forensic specialists, manages restoration from backups, confirms systems are safe before reconnecting.
Communications Lead	Office Manager / Senior Admin	Manages staff, customer, and supplier communications. Drafts holding statements. Single point of contact for media if required.
Finance & Payroll Lead	Accounts Manager	Engages bank/payment providers to halt suspicious transactions, arranges manual/backup payroll, liaises with accountant.
HR & Staff Welfare	Office Manager / People Lead	Keeps staff informed, manages wellbeing concerns, coordinates manual timesheets and any stand-down arrangements.
Production Lead	Workshop/Production Manager	Manages physical production continuity, prioritises jobs that can proceed without digital files, liaises with site teams and installers on current jobs.

- One person may hold more than one role

Copyright 2026 © by Mastercraft Services (NZ) Ltd

Containment and Assessment (first 24 hours)

- **Goal:** understand the scope of the attack, stop it spreading further, decide on next steps
- External IT provider or IT/Technical Lead assesses which systems are affected, isolates them, and checks whether backups are intact and uncompromised
- Identify what data may have been accessed, copied, or encrypted - importantly any personal information about staff, clients, or suppliers (names, addresses, bank details, ID numbers)
- Incident Controller decides whether specialist forensic/incident-response support is needed. For a significant attack, contact the NCSC (www.ncsc.govt.nz) in addition to CERT NZ
- If a ransom demand has been made, contact NZ Police
- Do not negotiate with or pay attackers without Police and legal advice — payment does not guarantee data return
- Finance & Payroll Lead arranges an alternative way to pay staff if payroll is inaccessible
- Communications Lead prepares a communication for staff and begins assessing whether customers or suppliers need to be told anything at this stage
- Brief lawyer and ask for advice specifically on Privacy Act 2020 notification obligations

Legal and Regulatory Obligations

- Under the Privacy Act 2020, a privacy breach becomes notifiable if it is reasonable to believe the breach has caused, or is likely to cause, serious harm to affected individuals
- A breach includes unauthorised access, disclosure, loss, or any action that prevents the business from accessing personal information, which includes a ransomware-style attack that locks staff, client, or supplier data
- **Assess harm:** consider the sensitivity of the data involved (e.g. bank account details, ID numbers, and health information rate higher than general contact details), and what could realistically happen to affected individuals as a result
- **Notify the Privacy Commissioner:** if the breach is assessed as notifiable, notify the Office of the Privacy Commissioner as soon as practicable and within 72 hours via the NotifyUs tool (www.privacy.org.nz/notifyus).
- **Notify affected individuals:** staff, clients, or suppliers whose personal information was involved must also be told as soon as practicable
- **Penalties:** Failing to notify a notifiable breach without reasonable excuse is an offence carrying fines of up to $10,000

Copyright 2026 © by Mastercraft Services (NZ) Ltd

Business Continuity Workarounds

- **Email and Communication**

  Set up a temporary free webmail account (e.g. via a personal or backup domain) known in advance to all managers, purely for emergency use - agree this in advance, not during the incident
- Use phone calls and SMS/text as the default communication method while email is unavailable
- Designate a single staff WhatsApp/messaging group (set up in advance) for fast, verified updates that does not depend on company infrastructure
- **Payroll**
- Keep an offline, regularly updated copy of core payroll data (staff names, bank account numbers, standard hours/pay rates) in a secure, access-controlled location separate from the main network - e.g. encrypted USB drive in a locked safe, updated monthly
- Confirm with your bank in advance whether manual/bulk payment files can be processed over the phone or in-branch if online banking is unavailable
- If payroll cannot be run on time, communicate proactively with staff about the delay and revised payment date - this matters significantly for staff trust and is a common source of complaint after cyber incidents
- **Production Files and Designs**
- Maintain printed or offline-saved copies of current, in-progress job files (designs, specifications) for active jobs at any given time - even a weekly export to an offline drive significantly reduces disruption
- Prioritise jobs already on the production floor with physical materials and paperwork - these can often continue without digital file access.
- Contact clients with upcoming on-site appointments or installation dates proactively if any delay is likely
- **Data Storage and Backups**
- Maintain backups that are both offsite and offline (or otherwise isolated from the main network) - many ransomware attacks specifically target connected backup systems, so a backup that is reachable from the infected network may also be encrypted or deleted
- Test backup restoration periodically (not just backup creation) — an untested backup is not a reliable backup
- Confirm with your IT provider in advance how long a full restoration is expected to take, so realistic timeframes can be communicated to staff and customers during a real incident

Copyright 2026 © by Mastercraft Services (NZ) Ltd

Communication Templates

- Internal Staff Communication

  "We are currently experiencing a technical issue affecting our email, computer systems, and [payroll/files as applicable]. We are working with our IT provider to resolve this as quickly as possible. In the meantime, please [use phone/text for urgent matters / report to your manager directly / await further instructions]. We will update you by [method] as soon as we know more. Please do not discuss details externally or on social media while this is being investigated."

- Customer/Supplier Communication

  "We are currently experiencing a temporary technical issue that may affect our response times for emails and orders. We are treating this as a priority and expect to be back to normal shortly. If your matter is urgent, please contact us by phone on [number]. We appreciate your patience."

- If Personal Information Is Confirmed Affected

  Any notification to affected individuals should include what happened, what information was involved, what the business is doing in response, what the individual can do to protect themselves (e.g. monitoring bank accounts, changing passwords), and a contact point for questions. Have this reviewed by legal counsel before sending, even under time pressure

Copyright 2026 © by Mastercraft Services (NZ) Ltd

Incident Log Template

Use this log from the moment the incident is identified. It supports insurance claims, regulatory notification, and post-incident review.

Date/Time	Action Taken	Details	By Whom	Follow-up Needed

Copyright 2026 © by Mastercraft Services (NZ) Ltd

Key Contacts Directory

Complete missing details in this form and keep current. Store a printed copy off-line.

Contact	Details	When to Use
CERT NZ / Own Your Online (report a cyber incident)	www.ownyouronline.govt.nz | 0800 CERT NZ (0800 2378 69)	First call for triage, guidance, and referral to other agencies
National Cyber Security Centre (NCSC) — significant/large-scale incidents	www.ncsc.govt.nz	For high-impact incidents needing specialist response support
NZ Police (if fraud, extortion, or theft is involved)	105 (non-emergency) or 111 if immediate danger	Required for any ransom demand, extortion, or theft of funds
Office of the Privacy Commissioner — NotifyUs	www.privacy.org.nz/notifyus	Mandatory if personal information is involved and serious harm is likely — notify within 72 hours of becoming aware
Cyber insurance provider (if held)	[Insert policy number and 24/7 claims line]	Notify immediately — many policies require notification before engaging IT/forensic responders to remain valid
External IT / Managed Service Provider	[Insert provider name and emergency contact]	Technical lead support, system isolation, restoration
Banking provider — fraud team	[Insert bank fraud hotline]	To freeze accounts or halt payments if banking access is compromised
Legal counsel	[Insert firm and contact]	Advice on notification obligations, contracts, liability
Domain/website host and email provider	[Insert provider and support contact]	To regain control of email and website if compromised

Copyright 2026 © by Mastercraft Services (NZ) Ltd