CYBER INCIDENT RESPONSE PLAN TEMPLATE

TEMPLATE INTRODUCTION:

This template is designed to help you create a basic incident response plan.

The plan may be tailored to your facility/organization.

This plan is broken into two components:

- A 'Quick start guide' at the beginning with key information required to kick off an incident response; many businesses will find this sufficient for handling of most incidents.
- An appendix with additional useful forms and templates.

There are some parts of the plan which need completing, such as relevant contact details of various teams who would assist with incident response.

Incident response:

An incident response plan is a useful document in handling incidents, however good incident response requires more than just a plan. It requires rehearsals, suitable technology and evidence availability (e.g. log data), good backups and system / network documentation, experienced responders (in-house or external) and often input from many teams around the business (from technical to HR, PR, Legal).

You may also want to create playbooks with specific guidance on different types of incident – e.g. data breach, ransomware, unknown malware, and denial of service.

Questions:

If you have any questions or need assistance with your Cyber Incident Response Plan, please reach out to either Dennis O'Connell at doconnell@customonline.com or Dennis Ast at dast@onegroup.com.

CYBER SECURITY INCIDENT RESPONSE PLAN

<Your Company>

<Date>

KEY CONTACT INFORMATION

Team	Typical reason for involvement/contact	Contact details
Computer Security Incident Response Team	Any cyber/computer incident	[EMAIL / PHONE / OTHER]
Incident response vendor	To perform or support technical investigation of a cyber / computer security incident.	[EMAIL / PHONE / OTHER]
IT security	To support investigation and remedial activities	[EMAIL / PHONE / OTHER]
Legal / compliance	Breach of sensitive data and/or when regulators or law enforcement are involved	[EMAIL / PHONE / OTHER]
PR / Communication Team	Incident requires communication with media/public	[EMAIL / PHONE / OTHER]
HR	Employee is suspected of malicious activity; or potentially breach of staff data	[EMAIL / PHONE / OTHER]
Crisis team / Senior mgmt. / Execs	Major incidents (see priority table)	[EMAIL / PHONE / OTHER]
Cyber insurance provider	Should be informed for any incident which may become a claim. Can also offer technical, legal, PR support as required on any incident	[EMAIL / PHONE / OTHER]

Emergency numbers for incident calls:

Name	Conf bridge
	[NUMBER AND CODE]
	[NUMBER AND CODE]

CLASSIFICATION

Classification	Description / Example
Data breach	Data has been leaked or exposed in some way that it is not meant to be and/or data has been accessed by an unauthorised party. This could be anything from someone having emailed data to the wrong person to an attacker stealing data from the network.
Denial of service	An attack which affects service availability – such as website or mobile app being taken down by floods of traffic.
Fraud / scam	Someone has been convinced to make a fraudulent payment or provide information as part of a scam.
Ransom / extortion	There is a demand for payment (or some sort of action but usually payment) to stop some ongoing or imminent attack.
System / data damage	Systems / data are damaged – often making them unusable. The most common cyber event of this type is ransomware.
Malware	Malware has been discovered on the network – potentially spreading / has spread. Should consider whether it is 'common' malware or something more targeted along with the spread and potential motive of the attacker.
Unauthorised access	Some type of unauthorised access has been discovered – this could be to the network in general or to specific data sets. This could also be by an employee or contractor; not necessarily an external party.

PRIORITIZATION:

The incident manager may alter the priority as more information is determined; if unsure raise to the crisis team(s) for review.

Priority	Description / Example
Critical (P1) – **RAISE TO CRISIS TEAM**	Severe impact and often damage increasing rapidly / limited resolution options. • Large number of (>40%) staff unable to work, critical work impacted • Critical business systems are down with no known resolution • Significant volume of sensitive data has been breached • Large number of customers are affected and/or acutely disadvantaged in some way. • The financial impact of the incident is likely to exceed [INSERT VALUE – E.G. $100,000] – consider business interruption as well as costs for handling the incident. • Widespread virus outbreak across all systems causing damage to data and systems • Major reputational damage / significant impact to share price/company value
Medium (P2) – **INFORM CRISIS TEAM**	• Number of (<40%) staff are unable to work (in non-critical roles). • Non-critical systems are down; or critical systems are down but with possible resolution • Some (non-sensitive) data has been breached, or there is a potential, but low, risk that a small amount of sensitive data has been breached. • Small number (<50) of customers are affected and/or disadvantaged in a minor way. • Known virus / malware on several (<10) non critical machines - low risk • The financial impact of the incident is limited, but still of note [E.G. £$0,000]
Low (P3)	• A few staff are impacted / unable to work – e.g. 1-5 people in non-critical roles. • Non-critical systems are down for <1 hour; or critical systems are down for <15 minutes. • Minor virus / malware on 1-2 (non-critical) machines

INCIDENT RECORD FORM:

This form is a simple template for recording key incident information – it can be used as the initial incident notification / record and used for updates or handovers.

For large and complicated incidents it may also be worth mapping out the attack in a diagram and/or creating a timeline of events to understand all aspects of it and ensure nothing is missed.

Incident Ref/title		Start date	
Update date		Author	
Incident still live? Yes/no			
Incident summary:			

Affected systems/users (refer to separate spreadsheet/file if needed)			
System name	**IP address**	**Username**	**Purpose/function/role**
System: mspsrv012	1.2.3.4	NA - all	Internal file server
Unknown	Unknown	jharris	finance

Known indicators of compromise / signatures (refer to separate spreadsheet/file if needed)		
Type	**Name**	**Notes**
File	Bad.exe	Main malware executable
Network account	Adminuser1	Admin account used by attacker

Current status: [What actions have been taken; what is in progress; what is known]
Next steps (any urgent actions / questions): [very important if being used as a handover]

Actions (or refer to action tracker)			
Actions ref	Action	Assigned to	Due date

CHECKLIST

Triage / Start response

- Validate the incident – is it real, what is known?
- Assign an incident manager and assemble team.
- Inform your insurer and engage 3rd parties as required.
- Start incident record – document facts, key decisions etc.

Contain / Mitigate

- Take action to preserve evidence if required (e.g. isolate machine but do not turn it off or start taking action on the system; alternatively this may just be making sure certain logs are not overflowing / overwriting etc.).
- Consider if any immediate action is possible to lower the risks / reduce impact.
- Ensure you consider the risks and benefits of these actions vs others/doing nothing.
- Plan and prioritise before implementing actions if many are required.
- Consider additional logging / monitoring where appropriate.
- Document findings, actions and key decisions, and report upwards as required.

Investigate

- Plan and prioritise tasks
- Assign tasks to relevant people/teams and track progress.
- Regularly review findings and determine:
    - New (or changes to existing) tasks.
    - Further mitigation/containment actions and / or steps for remediation plan.
- Document findings, actions and key decisions, and report to others as required.

Remediate

- Plan remediation actions if required – e.g. if timings are important.
- Ensure monitoring is in place if required while implementing actions.
- Implement remediation actions.
- Confirm remediation success – e.g. monitoring.
- Document findings, actions and key decisions, and report to others as required.

Recover

- Continue with any non-critical investigation actions (e.g. historical activity) if required.
- Restore / recover data or any other action required to return to 'BAU'.
- Document final status and report to others as required.
- Ensure all external reporting is complete where required (e.g. customers, regulators).

Lessons Learned

- Invite all relevant parties to review (may require separate sessions)
- Review incident using the form in the Appendix.
- Assign any actions to relevant people/teams.
- Agree incident close down.

APPENDIX A – CONTACT DETAILS

Internal

Key group contact info:	
Incident Response Team	
Incident conference bridges	
Escalation details – e.g. crisis team /execs	

Incident Managers			
Incident Lead Primary:		Incident Lead Secondary:	
Direct Dial:		Direct Dial:	
Mobile:		Mobile:	
Email:		Email:	

IT			
IT Primary :		IT Secondary :	
Direct Dial:		Direct Dial:	
Mobile:		Mobile:	
Email:		Email:	

Security			
Security Primary:		Security Secondary :	
Direct Dial:		Direct Dial:	
Mobile:		Mobile:	
Email:		Email:	

Legal			
Legal Primary:		Legal Secondary :	
Direct Dial:		Direct Dial:	
Mobile:		Mobile:	
Email:		Email:	

Public Relations			
PR Primary:		PR Secondary :	
Direct Dial:		Direct Dial:	
Mobile:		Mobile:	
Email:		Email:	

Risk and Compliance			
Risk and Compliance Primary:		Risk and Compliance Secondary :	
Direct Dial:		Direct Dial:	
Mobile:		Mobile:	
Email:		Email:	

Human Resources	
HR Primary:	HR Secondary :

Direct Dial:		Direct Dial:	
Mobile:		Mobile:	
Email:		Email:	

Customer Services			
Customer Services Primary:		Customer Services Secondary :	
Direct Dial:		Direct Dial:	
Mobile:		Mobile:	
Email:		Email:	

Internal Audit			
Internal Audit Primary:		Internal Audit Secondary :	
Direct Dial:		Direct Dial:	
Mobile:		Mobile:	
Email:		Email:	

External

Forensics / incident response	
Contact:	Company:
Direct Dial:	
Mobile:	
Email:	

Legal counsel	
Contact:	Company:
Direct Dial:	
Mobile:	
Email:	

Public relations	
Contact:	Company:
Direct Dial:	
Mobile:	
Email:	

Insurance company	
Contact:	Company:
Direct Dial:	
Mobile:	
Email:	

Notification / credit / identity monitoring	
Contact:	Company:
Direct Dial:	
Mobile:	
Email:	

APPENDIX B – FORMS

B.1 Incident record:

This form is a simple template for recording key incident information – it can be used as the initial incident notification / record and used for updates or handovers.

For large and complicated incidents it may also be worth mapping out the attack in a diagram and/or creating a timeline of events to understand all aspects of it and ensure nothing is missed.

Incident Ref/title		Start date	
Update date		Author	

Incident still live? Yes/no

Incident summary:

Affected systems/users (refer to separate spreadsheet/file if needed)

System name	IP address	Username	Purpose/function/role
System: mspsrv012	1.2.3.4	NA - all	Internal file server
Unknown	Unknown	jharris	finance

Known indicators of compromise / signatures (refer to separate spreadsheet/file if needed)

Type	Name	Notes
File	Bad.exe	Main malware executable
Network account	Adminuser1	Admin account used by attacker

Current status:
[What actions have been taken; what is in progress; what is known]

Next steps (any urgent actions / questions):
[very important if being used as a handover]

Actions (or refer to action tracker)

Actions ref	Action	Assigned to	Due date

B.2 Action tracker:

This simple template can be used to track the status of various actions:

Ref	Date created	Action	Priority	Assignee	Due date	Status	Notes
1	1/08/17	Block all access to XXX	High	ABC	2/08/17	Closed	
2	1/08/17	Analyse logs for XXXX	High	DEF	5/08/17	Open	
3	2/08/17	Update staff communications	Medium	GHI	5/08/17	On hold	Awaiting action 2.

B.3 Lessons learned:

The following template can be used to capture lessons learned following the incident response.

Incident Ref/title		Meeting date	
Incident summary:		Attendees:	
Lessons Learned – Incident			
How could the incident have been prevented? (Or should it have been?)			
How could the incident have been detected earlier?			
Are there security improvements that would assist with preventing or detecting this type of incident?			
Lessons Learned – Incident handling			
Could anything have been improved regarding the initial reporting/notification of the incident?			
Was the incident response plan (or any other plan) followed – why not / did it work?			
Were there issues with managing the incident – e.g. anything that could've been done differently?			
Were there any issues with investigation – e.g. missing data for analysis?			
Were there any issues with mitigation/containment/remediation?			
Were there any difficulties with full recovery of systems/data/BAU?			
Is there anything else which could have gone better?			
Actions			

Actions ref	Action	Assigned to	Due date