MOREnet
Be better connected.

INCIDENT RESPONSE PLANNING

MOREnet Cybersecurity
security@more.net

In coordination with
The Office of Homeland Security
CISA-Cybersecurity & Infrastructure Security Agency

IR/DR/BC

- Incident Response
- Disaster Recovery
- Business Continuity

INCIDENT RESPONSE PLAN

1. Prepare
2. Identify
3. Containment
4. Eradicate
5. Recovery
6. Learn
7. Review, Test, Train & Maintain

Be better connected.

PLANNING OBJECTIVES

DEFINE THE PROBLEM

- State the reason for the plan.
- Keep it simple, covering as many situations as possible.
- Know your budget, planning timeline, technical requirements, and what you are expected to deliver

CYBER RISK INSURANCE

- Review your policy
  - What is Covered?
  - Category-breach, data loss, ransomware, etc.
  - What is considered cyber risk as opposed to normal coverage?

PREPARE

- Build a team
- Risk assessment
- Contingencies
- Tools

BUILDING A TEAM

- Team leader
- Investigator
- Communications
- Documentation
- HR/Legal representation

Create Roles & Responsibilities

BUILDING TEAMS

- Crisis Management
- Emergency Response
- Communications
- Everyone Else

Be better connected.

CHOOSING TEAM MEMBERS

Try to recruit members with the following in mind:

- Organizational placement, who can make decisions
- Technical proficiency
- Existing training and location
- Outside organizations
- Emergency response
- Cross training in case member not available.

Be better connected.

TEAM RESPONSIBILITIES

- Maintain a checklist.
- Confirm priorities have not shifted.
- Expectations of the team
- Communicate milestones reached to the team leader.

DOCUMENT KEY CONTACTS

Contact	Phone
Superintendent	
CIO, CFO, Tech Director	
Communications Director	
General/Legal Counsel	
HR Director	
Insurance Co-Cyber Risk Policy	
Law Enforcement	
Credit Monitoring Services	
Vendors	

Be better connected.

RISK ASSESSMENT

- Policies & procedures
- Infrastructure
- Personnel

- Define the threat & symptoms
  - Attacks
  - Malware, viruses
  - Ransomware
  - Data breach credential theft
  - Phishing
  - Insider threat

Be better connected.

MITIGATION IS RISK MANAGEMENT

1. Analyzing risk
2. Reducing risk

VULNERABILITY ASSESSMENT

- Utilize questionnaires, interviews, document reviews, and research.
- Rate each risk you have identified on a vulnerability scale.
- Now you can assign values to all identified risks.

RISK LEVEL MATRIX (QUALITATIVE)

RED=UNACCEPTABLE YELLOW=HIGH ORANGE=MEDIUM BLUE=LOW

		IMPACT			
LIKELIHOOD	**Catastrophic 5**	**Critical 4**	**Serious 3**	**Minor 2**	**Insignificant 1**
Almost Certain 5	25	20	15	10	5
Likely 4	20	16	12	8	4
Possible 3	15	12	9	6	3
Unlikely 2	10	8	6	4	2
Improbable 1	5	4	3	2	1

Be better connected.

RISK	THREAT	SYMPTOMS	MITIGATION
	MALWARE/VIRUS	POP UPS, SLUGGISH, UNRESPONSIVE	REMOVE FROM NETWORK. ANTI-VIRUS SCAN/CLEAN, REIMAGE. SCAN AGAIN.

THREAT ASSESSMENT APPROACHES

- Quantitative
- Qualitative

OTHER CONSIDERATIONS

RTO VS RPO

- Recovery Time Objective – How quickly you can recover
- Recovery Point Objective – How much data loss can you tolerate to a point of operational functionality

TYPES OF RISK MANAGEMENT STRATEGIES

- Risk Acceptance or the Do-Nothing strategy
- Risk Avoidance
- Risk Limitation
- Risk Transference

RISK MANAGEMENT SUMMARY

- Secure functions as much as possible
- Putting management or stakeholders in a position to make the best decisions possible for business functions.

CONTIGENCIES

- Alternate location
- Phone access
- Alternate personnel
- Access to hardware
- Business continuity

Mitigation Plans

- ✓Understand the users and their needs
- ✓Seek out the experts and use them
- ✓Recognize risks that reoccur
- ✓Determine the scope of an event
- ✓Plan ‘B’

STEPS TO TAKE FOR RECOVERY

- Implement Risk Mitigation
- Outline what it will take for the plan to be activated
  - Minor
  - Intermediate
  - Major
- Outline triggers
- Communication

JUMP BAG
GRAB AND GO

- Switches – New, Old, Stealable
- Cell Phone
- Software-AV, packet sniffer
- Hard drives – spare, external
- Laptops - w/ diagnostics software
- Bootable device, usb,
- Hotspot – Who, what, and where.
- Cables
- Toolbox-screwdrivers, cable crimpers/testers, etc

Copy of IR plan, Journal and contact list

Be better connected.

HOMEWORK

- Identify Team members
  - Assign roles and responsibilities
- Identify key contacts
- Risk assessment
- Compile a jump bag

Be better connected.

QUESTIONS