INSERT ORGANIZATION LOGO

BUSINESS CYBER DISRUPTION PLANNING WORKBOOK

for

[Organization Name]

CONTENTS

INTRODUCTION

The word 'Cyber', as used in this document, is intended as a collective term to include all information technology systems (IT, computers), applications (software), and data networks (Internet, private leased, internal)

Every day there are increasing reports of cyber-attacks being committed against companies, small and large, across the United States. The cause and effect of these cyber events vary from theft of sensitive data (credit cards, healthcare, etc.) to losing control of automated devices (manufacturing, environmental, etc.) to ransomware (extortion)! Yet, even as the volume and scope of these events continue to grow, often with devastating consequences, many small to medium sized companies are not preparing for the impact of such situations.

This planning workbook is offered as a simple facilitation framework for your company to begin exploring and preparing for response and recovery from a *Cyber Disruption*.

A *Cyber Disruption* is any event that may interrupt or prevent critical business functions and services across your business operation(s) by impairing the confidentiality, integrity, or availability, of electronic information, information systems, services, or networks.

A *Cyber Disruption* may be a simple but prolonged loss of connectivity with your Internet Service Provider, or a malicious software attack (virus or ransomware), or a cybercrime event, or it may even be a cyber-attack on a national scale meant to damage the United States infrastructure.

The bottom line is that every business that depends on information technology, even those that may not connect directly to the Internet, should develop a *Cyber Disruption Plan* —before a cyber event prevents you from conducting business!

BACKGROUND

Traditionally, experienced businesses have relied on well-developed Business Continuity and Disaster Recovery Plans (BCDRP) for response and recovery to significant emergencies. Most often, events triggering a BCDRP situation have been those events denying a business access to a physical location, such as might be caused by floods or fires.

Nevertheless, over the last several years as dependence on information technology and Internet connectivity has grown, many businesses have been lax in understanding their *cyber footprint*. With that in mind, consider a situation where the loss of cyber assets might so cripple your organization that relocation to a new physical location is of no value or is simply impractical. For example, several recent ransomware attacks have resulted in businesses losing *all* of their essential data.

In one instance, the loss was of critical operating information collected over 30 years and relied on for day-to-day operations. The victim was a law firm. With literally all of their information controlled by a cybercriminal demanding a substantial ransom, it became impossible for business to continue. And, even after paying the ransom, they were ultimately denied access and lost all of their information.

In another example, a large manufacturing enterprise had literally thousands of computer-hard drives running onboard critical machinery become simultaneously unusable and unrepairable. This victim was an energy industry giant. They relied on each of these machines spread over a large geographic area to help them control their daily operations. In fact, as a result of this automation enhancement they reduced their workforce believing there would be no future need for those employees. Then, disaster struck when they were the object of an attack that was not as much about hurting them as it was about making a political statement. Can you imagine the difficulty with ordering ten thousand computer hard-drives at one time? What happens until those replacements arrive?

As reliance on information technology grows, it is inevitable that traditional emergency management and cyber security events will overlap from some common exposure, these are known as *converged events*. For example, as with all businesses rushing to embrace technology as a path towards efficiency and cost savings, the environmental controls (HVAC, power, water, etc.) industry has done the same. This means that your building environmental controls are likely vulnerable to the same or similar threats as your business' information technology!

Consider, if your building environmental systems were to become degraded or inoperable as a result of a cyber event not directed at your business but at the controls manufacturer, you might likely find yourself placed in an emergency management situation requiring an immediate response in order to remain operational. While you might not be the target, an attack on vulnerabilities within the automated systems controlling your building's environmental systems resulted in you becoming a collateral victim. Do you have a plan to respond and recover from that type of event?

Examples of "*Cyber Disruptions*" that might affect your business are:

- a hurricane, flood, tornado, earthquake, or other natural disaster that impairs or destroys a key data communications infrastructure resource (**3rd party provider**) that results in **loss of data communications connectivity**;
- destruction or damage to a data center (**cloud provider**) which results in a loss of connectivity or loss of data access;
- a cyber-attack on the power grid leading to loss of power;
- a cyber-attack on water treatment and delivery leading to a loss of water supply;
- cyber-attacks on financial management, healthcare providers, transportation partners;
- a cyber-attack on network capabilities leading to loss of communications (aka DDOS).

PLANNING FOR BAD THINGS

A *Business Cyber Disruption Plan* is intended to be used **in conjunction** with your *Emergency Preparedness and Response Plan* and your *Business Continuity and Recovery Plan.* In fact, it should be an integral part of both of these plans. Some key components of these plans are:

Emergency Preparedness and Response Plan

Emergency Preparedness and Response Plans identify and prioritize the dangers that may affect business operations, and subsequently lay out preparedness and mitigation activities. Accordingly, these plans may also include operational procedures designed to respond to an *incident*. The goal of the *Emergency Preparedness and Response Plan* is to direct life and safety requirements in response to a disaster.

Typically, these plans include information such as:

- Preparedness
- Hazard identification and assessment
- Employee education and training
- Drills and exercises timelines and plans for your business
- First aid kits
- Disaster supply kits
- Response
- Evacuation procedures
- Fire procedures
- Shelter-in-place procedures
- Staff notification
- Information gathering procedures
- Incident management

Business Continuity and Recovery Plan

Business Continuity and Recovery Plans are developed for response to a calamity, *once* life and safety have been assured. Accordingly, these plans identify key resources and needs necessary for the business to continue, even in a limited capacity, or it may direct how the business intends to fully recover should the disaster be *catastrophic*.

Typically, these plans include information such as:

- Critical assets
- Critical operations
- Key suppliers and contractors
- Alternate business location

Business Cyber Disruption Plan

Business Cyber Disruption Plans are documented methods for controlling critical information security activities. This effort represents the ***knowledge and planning*** intersection of recognizing a cyber event that triggers business continuity and/or emergency management issues. Therefore, cyber disruption requires three areas of focus surrounding information security:

- Prevention and Protection
- Detection and Analysis
- Response and Recovery

Working to Create a Business Cyber Disruption Plan:

Your Plans should be living documents that require routine maintenance and modifications based on your organization's changing business focus and technology implementations. Create YOUR document to fit YOUR need.

Start the planning process by answering the questions below. These questions will lead you through a discovery process that, if done diligently, will provide the necessary background to conduct a meaningful analysis involving your business. Finally, your analysis should lead you to conclusive plans that, once documented, provide your organization with a roadmap by which to recognize and respond to a cyber disruption.

Phase I, Discovery

Step 1: Document Your Business

Some facts around your business are simple and straight forward, others are not. Consider carefully what might need to be known in an emergency, especially a long disruptive event with limited communications.

Primary Business Location	Additional Business Location
Business Name:	Business Name:
Street Address:	Street Address:

City, State, Zip Code:	City, State, Zip Code:
Telephone Number:	Telephone Number:
Type and State of Incorporation:	Federal Tax ID:
Location and Specialty Licenses:	Primary Bank or Financial Institution:
PRIMARY POINT OF CONTACT	**ALTERNATE POINT OF CONTACT**
Primary Emergency Contact:	Alternate Emergency Contact:
Telephone Number:	Telephone Number:
Alternate Telephone Number:	Alternate Telephone Number:
E-mail Address:	E-mail Address:
EMERGENCY CONTACT INFORMATION	
Non-emergency Police:	Electricity Provider:

Non-emergency Fire:	Gas Provider:
Insurance Provider:	Water Provider:
Other (e.g., equipment manufacturer):	Other (e.g., property management):
Other (e.g., HazMat Spill Clean-Up):	Other (e.g., property security):
Other (e.g., IT support contractor):	Other:
Other:	Other:
Other:	Other:

Step 2: Identify Your Business Continuity and Recovery Planning Team

Select a 'team' of employees to participate in ***Business Continuity and Recovery Planning***. Why? For the simple reason that it takes more than one person to run your business, it stands to reason not everyone knows or understands all functional areas of your business. Who handles finance, IT, HR, sales, operations?

NAME	POSITION	EMAIL

Coordination with Others:

The following people from *neighboring businesses* and our *building management* will coordinate with us on ***Emergency Planning***.

NAME	BUSINESS	EMAIL

Step 3: Identify Critical Resources

Ask, "if these resources were taken away, would it drastically affect your business or cause a major disruption to your business"?

PEOPLE (EMPLOYEES, CUSTOMERS, ETC.)	
Name	**Location & Purpose**
BUILDING (PHYSICAL STRUCTURE, STORAGE UNIT, WAREHOUSE, MAIN OFFICE, ETC.)	
Name	**Location & Purpose**
EQUIPMENT (NON-IT SUCH AS SPECIALTY/MANUFACTURING TOOLS, COPIERS, FURNITURE, ETC.)	
Name	**Location & Purpose**
BUSINESS DATA (DOCUMENTS, PAYROLL, FILES, , ETC.)	
Name	**Location & Purpose**

SUPPLIES	
Name	**Location & Purpose**
BUSINESS FUNCTIONS (ACCOUNTS RECEIVABLE/PAYABLE, PAYROLL, MANUFACTURING, MAIL ROOM, ETC.)	
Name	**Location & Purpose**

Specify Key Suppliers, Vendors, and Contractors

BUSINESS NAME:		
Street Address:		Contact Name:
City, State, Zip Code:		Contact Telephone Number:
Telephone Number:	Fax Number:	Contact Email:
Emergency Telephone:	Website:	Does this business have a continuity plan?

Material/Service Provided:
If this company experiences a disaster, we will obtain materials/services from the following:

BUSINESS NAME:		
Street Address:		Contact Name:
City, State, Zip Code:		Contact Telephone Number:
Telephone Number:	Fax Number:	Contact Email:
Emergency Telephone:	Website:	Does this business have a continuity plan?
Material/Service Provided:		
If this company experiences a disaster, we will obtain materials/services from the following:		

Step 4: Identify Critical Operations

What operations are necessary to fulfill legal and financial obligations? Which are necessary to maintain cash flow and reputation? Which are NOT critical? (what's left must therefore be critical)

OPERATION:	
Staff in Charge (Position):	Staff in Charge (Name):
Key Supplies/Equipment:	Key Suppliers/Contractors:

OPERATION:	
Staff in Charge (Position):	Staff in Charge (Name):
Key Supplies/Equipment:	Key Suppliers/Contractors:

OPERATION:	
Staff in Charge (Position):	Staff in Charge (Name):
Key Supplies/Equipment:	Key Suppliers/Contractors:

Step 5: Identify Business Information Types and Format(s)

Identify all information used in the normal course of business, whether it is stored within your business files or information systems or at a third-party provider.

Check All as Appropriate	Information Type	Description (Number of Records & Storage Location)
☐	Personally Identifiable Information (Name, Address, Phone Number, etc.) and Social Security Number	Electronic: Paper: Other:
☐	Individual Health Information	Electronic: Paper: Other:
☐	Individual or Business Financial Information	Electronic: Paper: Other:
☐	Credit Card Information	Electronic: Paper: Other:
☐	Information deemed Sensitive or Confidential by Policy or Law	Electronic: Paper: Other:
☐	Trade Secrets or Proprietary Information	Electronic: Paper: Other:

BUSINESS INFORMATION					
Employees	**Customer/Clients**	**Financial**	**Intellectual Property**	**Inventory**	**Contracts**
Format & Location	Format & Location	Format & Location	Format & Location	Format & Location	Format & Location

REGULATED INFORMATION			
Credit Card Data (PCI)	**Personal Health Information (PCI)**	**Personally Identifiable Information (PII)**	**Other**
Format & Location	Format & Location	Format & Location	Format & Location

Step 6: Identify Information Technology Assets

What company provides Internet access to your organization? What company provides network management for your organization?

HARDWARE INVENTORY					
Hardware (CPU, Monitor, Printer, etc.)	Model	Serial Number	Date Purchased	Purchased or Leased from?	Cost

SOFTWARE INVENTORY					
Name of Software	Version	Serial / Key Number	Disc or Download	Date Purchased	Cost

OTHER DEVICE INVENTORY					
Hardware	Model	Serial Number	Date Purchased	Purchased or Leased from?	Cost

Step 7: Identify Alternate/Temporary Business Location

Assuming it makes sense to set up an alternate or temporary business location if your primary site is unavailable, identify where that location should be. Consider whether work can be done virtually? What pre-agreements would be needed?

ALTERNATE BUSINESS LOCATION	**SECOND ALTERNATE BUSINESS LOCATION**
Street Address:	Street Address:
City, State, Zip Code:	City, State, Zip Code:

Telephone Number:		Telephone Number:	
Is there a pre-agreement in place?		Is there a pre-agreement in place?	
Point of Contact		**Point of Contact**	
Contact Name:		Contact Name:	
Telephone Number:	Alternate Number:	Telephone Number:	Alternate Number:
E-mail Address:		E-mail Address:	
Site Assessment		**Site Assessment**	
Number and type of staff to work here:		Number and type of staff to work here:	
Supplies already in place:		Supplies already in place:	
Supplies that would be needed:		Supplies that would be needed:	
Time to set up operations:		Time to set up operations:	
Length of time to stay in this site:		Length of time to stay in this site:	
Possible hazards in the area:		Possible hazards in the area:	
Notes:		Notes:	

Step 8: Identify Potential Threats

Each part of the country has naturally occurring threats that all businesses should anticipate. Others, however, have unique natural threats that should be considered based on geography. On the other hand, don't discount natural threats just because they've not occurred in recent years.

NATURALLY OCCURRING EVENTS: EARTHQUAKE, FIRE, FLOOD, PANDEMIC

MAN MADE EVENTS: SOFTWARE FAILURE, HARDWARE FAILURE, DISGRUNTLED EMPLOYEE, CRIME, ETC

Step 9: Identify Current Business Insurance Coverage

Most all businesses have some type of business insurance at a minimum. Others have a variety of policies intended to protect the insured based on unique aspects for their business. If you depend on computers at any level, do you have cyber insurance?

INSURANCE AGENT:		
Street Address:		Contact Name:
City, State, Zip Code:		Contact Telephone Number:
Telephone Number:	Fax Number:	Contact Emergency Telephone:
Emergency Telephone:	Website:	Contact Email:

INSURANCE POLICY INFORMATION				
Type of Insurance	Policy Number	Policy Limits	Deductibles/SIR	Coverage (General Description)

RELATED INSURANCE QUESTIONS	
Do you need Flood Insurance? □ Yes □ No	What perils or causes of loss does my policy cover?
Do you need Earthquake Insurance? □ Yes □ No	How will my property be valued?

<table>
<tr><td>Do you need Business Income and Extra Expense Insurance? □ Yes □ No</td><td>Does my policy cover the cost of required upgrades to code? □ Yes □ No</td></tr>
<tr><td>How much insurance am I required to carry by third parties?</td><td>What does my policy require me to do in the event of a loss?</td></tr>
<tr><td>What types of records and documentation will my insurance company want to see?</td><td rowspan="2">Am I covered for lost income in the event of business interruption because of a loss? Do I have enough coverage? For how long is coverage provided? How long is my coverage for lost income if my business is closed by order of a civil authority?</td></tr>
<tr><td>If cyber insurance is purchased, then am I required to get the insurer's prior written consent before engaging third-party service providers, including legal and forensics?</td></tr>
<tr><td>To what extent am I covered for loss due to interruption of power? Is coverage provided for both on- and off-premises power interruption?</td><td>To what extent am I covered for reduced income due to customers' not all immediately coming back once the business reopens?</td></tr>
<tr><td colspan="2">Notes:</td></tr>
</table>

Phase II, Analysis & Conclusion(s)

An Approach to Planning

Strategic planning is a process of defining strategy or direction for long term intentions, and making consequential decisions about allocating resources in pursuit of that strategy. Consequently, while there are many approaches to strategic planning, one of the approaches for you to consider is a simple three-step process commonly referred to as the "*STP Method*".

STP is summarized as:

- **Situation** - analyze the current situation in comparison with an accepted standard or "best practice", and then determine proper alignment
- **Target** – from conclusion(s) reached in the previous step, define specific goals and/or objectives (sometimes called ideal state) to reach the desired condition
- **Path** – to reach the desired condition, map a realistic route to the goals/objectives

Accordingly, as you must consider carefully the potential impacts and desired outcomes regarding information security controls around your organization's people, processes, and technology.

Step 1, Analyze Your Current Situation

Key 'Big Picture' Questions to Ask

1) Is there appropriate support for creating, sustaining and maturing a cyber disruption plan?

2) What messaging is required to gain the necessary support for creating, sustaining and maturing a cyber disruption plan?

3) Who are key executive sponsors critical to the success of a cyber disruption plan?

4) Who are key stakeholders and partners that should be included in my cyber security disruption plan network?

5) What critical infrastructure providers should be included?

6) What manufacturers and distributors should be included?

7) What backup communications capabilities are in place to maintain communication locally, regionally and nationally?

8) What are key assets and roles that must be available at the various stages of a cyber disruption event?

9) What are the priority assets and a backup/recovery strategy for these assets?

10) Do we have appropriate interoperability between cyber incident response and emergency management functions?

11) Are key roles and resources mapped to a cross functional process that clearly describes how they will interact and be deployed at various threat levels?

12) When was a cyber disruption simulation last tested through a tabletop exercise?

13) How long might it take for our local government/infrastructure to restore the delivery of power, water, natural gas, internet, sewage treatment, transportation?

14) What training is currently in place for existing cyber security staff?

15) What new training should be added to shore up capabilities to support a cyber disruption plan?

Cyber Security Specifics

1) Do you have a formal information security policy? (published to all employees)

2) Specifically, who is responsible for developing and maintaining the information security policy?

3) Which functional group (or individual) enforces the policy?

4) Are there other policies associated with security? If so, what are they?

5) How often is the policy updated and reviewed?

6) How many employees are dedicated to security (both physical and information)?

7) Where are these employees placed within the organization? (refer to organizational chart)

8) How do you distinguish the various levels of data sensitivity within the organization? (ie, markings)

9) What are some of your recent information security-related education initiatives?

10) What methods do your use to protect the physical assets of your company?

11) Who determines the importance of assets?

12) What methods are used to protect mobile devices? (PDAs, cell phones, Laptop Computers)

13) Do you keep a formal inventory of assets? If so, are information systems included?

14) Does your organization have procedures or guidelines for labeling and handling data?

15) Are procedures for hiring new personnel documented?

16) Who contacts references or otherwise vets new hires?

17) Examine your employee termination procedure as it relates to the terminated employee having access to the organizations information and information technology.

18) Do you require all employees sign a confidentiality agreement that includes limitations on the disclosure of information? (Non-Disclosure Agreement)

19) Describe new employee training regarding information security

20) Does the organization have dedicated security guards? (employees or contract)

21) What type of controls do you have for protecting physical access to your information systems?

22) Do you use video surveillance? If so, how long are images retained?

23) Describe your policy, processes, and procedures for disposing of old or unwanted information systems, magnetic media, and paper

24) Does the company have an Internet presence and how is its security managed? (web site)

25) Describe your process for backing up data, and how often is it tested to ensure accuracy?

26) Do you use an offsite storage facility to store your backups? If so, do you use a vendor/service?

27) Do you formally segregate duties for information technology support? (ie., is there a dedicated IT administrator or is it a collateral duty for a specific employee)

28) How is access to sensitive data within the organization accomplished?

29) How are employees identified within the company (individual logins for systems, display badges for physical access)?

30) Is encryption used to protect certain data? If so, is there a documented procedure?

31) How is remote access to your business network accomplished?

32) Are **all** changes to the organization's software and hardware documented? If so, please describe how

33) Describe your process for applying patches (security and maintenance) to information systems.

34) Is 'test' data different from 'live' data? Do you distinguish 'test data' from live data?

35) How do you ensure your organization follows applicable 'information' related regulations?

36) Is there a dedicated contractual review process for technology support? If so, does the contract review include specific references to information security?

37) How do you safeguard organizational records?

38) Describe your process for the collection of evidence in event of a breach.

Step 2, Define Your Target Strategy for Cyber Disruption Events

Considering the analysis conducted in Step 1 above, you should now be well versed in what your company is doing and not doing around cyber security and business continuity. The next step is to take into consideration what, if any, information security related regulation or standards requirements apply to your business and within that context, design a strategy around cyber disruption that considers:

1) Prevention and Protection
2) Detection and Analysis
3) Response and Recovery

Prevention and Protection

Based on everything known to this point, what additional information security and protection efforts should be undertaken to reasonably assure your cyber capabilities are not disrupted easily?

Detection and Analysis

Based on everything known to this point, what additional cyber security efforts should be undertaken to detect and analyze cyber events in order to reach well-reasoned risk conclusions that will in turn allow effective management decisions?

Response and Recovery

Based on everything known to this point, what processes must be established and documented to allow for a methodical and escalating response to varying cyber threats? And, should these threats rise to become a disruption, what recovery processes do not exist today?

Phase III, Path to Building a Cyber Disruption Plan

Concept of Operations for Cyber Disruption Plan

- *Near-Term (24 hours)*

  Specific Cyber Response Tasks

  - Data Backup
  - Disaster Recovery / Business Continuity Plan
  - Equipment Shutdown
  - Log File Recovery
  - Communication (Include Media, Executives, etc.)
  - Cyber Disruption Response Plan Activation
  - Other

- *Medium Term (7-10 days)*

  Specific Cyber Response Tasks

  - Data Backup
  - Disaster Recovery / Business Continuity Plan
  - Equipment Shutdown
  - Log File Recovery

- Communication (Include Media, Executives, etc.)
- Cyber Disruption Response Plan Activation
- Other

- *Long Term (10 days – weeks)*

  Specific Cyber Response Tasks

  - Data Backup
  - Disaster Recovery / Business Continuity Plan
  - Equipment Shutdown
  - Log File Recovery
  - Communication (Include Media, Executives, etc.)
  - Cyber Disruption Response Plan Activation
  - Other

Critical Considerations

- *Continuity of Management*

Given the nature of the cyber disruptions, it should be assumed that not every person identified in your plan will be available to respond as expected. Expect that not every key person will be available either virtually or physically to help respond to the emergency. Therefore, it is critical to ensure that recovery decisions can be made without undue delay. That means everything must be documented at the most elementary detail. And, don't forget to consult your legal department regarding laws and corporate bylaws governing continuity of management.

Establish procedures for:

- Assuring there is a chain of command
- Maintaining lines of succession for key personnel
- Ensure all employees are aware

POLICY STATEMENT REGARDING CONTINUITY OF MANAGEMENT:

- *Staff Notification*

Staff should be regularly updated on business operational status including whether they should report to work, what work conditions are like, alternate work sites and plans, etc.

<table>
<tr><th colspan="3">NOTIFICATION</th></tr>
<tr><td rowspan="3">Staff will be notified by:

Phone Tree:

Automatic Notification System:

Email Blast:

Other:</td><td colspan="2">Staff member responsible for notification:</td></tr>
<tr><td>Telephone Number:</td><td>Email:</td></tr>
<tr><td colspan="2"></td></tr>
</table>

- *Key Business Contact Notification*

Customers, vendors, and other key business contacts should be regularly updated on business operational status such open hours, orders in progress, etc.

<table>
<tr><th colspan="2">NOTIFICATION</th></tr>
<tr><td>Key business contacts will be notified by:

Website:</td><td>Staff member responsible for notification:</td></tr>
<tr><td>Automatic Notification System:

Email Blast:</td><td>Telephone Number:</td></tr>
<tr><td>Signage:

Other:</td><td>Email:</td></tr>
</table>

PLAN DEVELOPMENT SUMMARY

- Identify all partners to build a network of stakeholders that might be affected by a cyber disruption; don't forget business interactions with government at the local, state, and federal levels; share ideas

- Enhance relationships with stakeholders through frequent non-crisis interaction; In that way, when a cyber disruption event does occur the relationship is prepared for the crisis

- Integrate cyber disruption planning with emergency management and business continuity planning; Cyber Disruption Plan core component, not a standalone effort

- Establish a priority for activities based on near-term, medium term and long term time lines

- Create a meaningful information technology vulnerability assessment process; but, consider information risk across the entire business enterprise

- Develop a strategy for communications with clients, partners, and others; especially addressing the loss of telecommunications including internet and wireless networks

- Develop contingency plans, alternative action plans considering secondary effects of regional emergencies and secondary effects of cyber disruptions

- Carefully examine supply chains, particularly those that are relied upon by all partners; If the supply chain is broken for one partner, it may be the same circumstance for other partners

- Develop test plans and execute those test plans on a regular basis

- Carefully examine supply chains, particularly those that are relied upon by all partners. If the supply chain is broken for one partner, that is most likely the circumstance for other partners