HODGSON
CONSULTING & SOLUTIONS

## IT MANAGER'S MASTERCLASS

# Step By Step Disaster Recovery Framework

## How You Can Protect Your Company From Being Held Hostage, Lost Profits, And Irreparable Reputation Damage

### Abstract

This interactive webinar series is for IT Managers or IT leaders of organizations who want to enhance their knowledge and skills, enabling them to better protect their organizations from potential threats, minimize the impact of incidents on business operations, and successfully recover from an IT disaster.

## PART 1

# PRACTICAL STRATEGIES FOR ASSESSING RISK IN IT

Mitigate The IT Risks That Could Negatively Impact Your Organization.

# HOMEWORK

**IT Infrastructure Risk Assessment Activity**

Objective: To enable IT managers to identify, profile, and estimate potential risks to their IT infrastructure.

Instructions: Follow the instructions listed under each step.

## Step 1: IDENTIFICATION OF TOP 5 ASSETS AT RISK

Instructions: List the top 5 assets in your organization that are most critical to business operations and have potential vulnerabilities. Consider the impact on your business if these assets were compromised.

1. Asset 1: ______________________________

   Asset Description: ______________________________

2. Asset 2: ______________________________

   Asset Description: ______________________________

3. Asset 3: ______________________________

   Asset Description: ______________________________

4. Asset 4: ______________________________

   Asset Description: ______________________________

5. Asset 5: ______________________________

   Asset Description: ______________________________

# Step 2: THREAT PROFILING

Instructions: For each of the identified assets, answer the following questions related to different aspects of potential threats:

**Asset 1** ______________________________________________________________

### Cybersecurity:

- What are the current cybersecurity measures in place for this asset?

- Have there been any recent attempts to breach the security of this asset?

### Data Backup and Recovery:

- Is there a robust data backup and recovery system in place for this asset?

- How often are backups tested for successful restoration?

### Software/Hardware Vulnerabilities:

- Are there any known software or hardware vulnerabilities associated with this asset?

- Is there a process to regularly update and patch these vulnerabilities?

### Cloud Infrastructure:

- If this asset is hosted on the cloud, what are the security measures in place to protect it?
- What is the cloud provider's history of security incidents?

### Unauthorized Device Access:

- Can this asset be accessed by unauthorized devices?
- Are there measures in place to detect and prevent unauthorized access?

### Training of IT Security Personnel:

- Is the IT security team trained to handle potential threats to this asset?
- Are there regular training sessions to keep the team updated on the latest threats and best practices?

## Asset 2 ________________________________________________

### Cybersecurity:

- What are the current cybersecurity measures in place for this asset?
- Have there been any recent attempts to breach the security of this asset?

### Data Backup and Recovery:

- Is there a robust data backup and recovery system in place for this asset?
- How often are backups tested for successful restoration?

### Software/Hardware Vulnerabilities:

- Are there any known software or hardware vulnerabilities associated with this asset?
- Is there a process to regularly update and patch these vulnerabilities?

### Cloud Infrastructure:

- If this asset is hosted on the cloud, what are the security measures in place to protect it?
- What is the cloud provider's history of security incidents?

### Unauthorized Device Access:

- Can this asset be accessed by unauthorized devices?

- Are there measures in place to detect and prevent unauthorized access?

### Training of IT Security Personnel:

- Is the IT security team trained to handle potential threats to this asset?

- Are there regular training sessions to keep the team updated on the latest threats and best practices?

**Asset 3** ____________________________________________

### Cybersecurity:

- What are the current cybersecurity measures in place for this asset?
- Have there been any recent attempts to breach the security of this asset?

### Data Backup and Recovery:

- Is there a robust data backup and recovery system in place for this asset?
- How often are backups tested for successful restoration?

### Software/Hardware Vulnerabilities:

- Are there any known software or hardware vulnerabilities associated with this asset?
- Is there a process to regularly update and patch these vulnerabilities?

### Cloud Infrastructure:

- If this asset is hosted on the cloud, what are the security measures in place to protect it?
- What is the cloud provider’s history of security incidents?

### Unauthorized Device Access:

- Can this asset be accessed by unauthorized devices?

- Are there measures in place to detect and prevent unauthorized access?

### Training of IT Security Personnel:

- Is the IT security team trained to handle potential threats to this asset?

- Are there regular training sessions to keep the team updated on the latest threats and best practices?

**Asset 4** ____________________________________________

### Cybersecurity:

- What are the current cybersecurity measures in place for this asset?
- Have there been any recent attempts to breach the security of this asset?

### Data Backup and Recovery:

- Is there a robust data backup and recovery system in place for this asset?
- How often are backups tested for successful restoration?

### Software/Hardware Vulnerabilities:

- Are there any known software or hardware vulnerabilities associated with this asset?
- Is there a process to regularly update and patch these vulnerabilities?

### Cloud Infrastructure:

- If this asset is hosted on the cloud, what are the security measures in place to protect it?
- What is the cloud provider’s history of security incidents?

### Unauthorized Device Access:

- Can this asset be accessed by unauthorized devices?
- Are there measures in place to detect and prevent unauthorized access?

### Training of IT Security Personnel:

- Is the IT security team trained to handle potential threats to this asset?
- Are there regular training sessions to keep the team updated on the latest threats and best practices?

## Asset 5 ______________________________________________

### Cybersecurity:

- What are the current cybersecurity measures in place for this asset?
- Have there been any recent attempts to breach the security of this asset?

### Data Backup and Recovery:

- Is there a robust data backup and recovery system in place for this asset?
- How often are backups tested for successful restoration?

### Software/Hardware Vulnerabilities:

- Are there any known software or hardware vulnerabilities associated with this asset?
- Is there a process to regularly update and patch these vulnerabilities?

### Cloud Infrastructure:

- If this asset is hosted on the cloud, what are the security measures in place to protect it?
- What is the cloud provider's history of security incidents?

### Unauthorized Device Access:

- Can this asset be accessed by unauthorized devices?
- Are there measures in place to detect and prevent unauthorized access?

### Training of IT Security Personnel:

- Is the IT security team trained to handle potential threats to this asset?
- Are there regular training sessions to keep the team updated on the latest threats and best practices?

# Step 3: RISK ESTIMATION

Instructions: For each asset, consider hypothetical situations such as data breaches, ransomware attacks, and malicious threats. Estimate the likelihood and potential impact of these situations on a scale of Low, Medium, and High (for details, see the Definitions section on pages 15-16). Use the Risk Matrix on page 15 to determine the Risk Rating.

**Asset 1** ______________________________________________

| | Threats | Likelihood | Impact | Risk Rating |
|---|---|---|---|---|
| 1 | | - | - | |
| 2 | | - | - | |
| 3 | | - | - | |
| 4 | | - | - | |
| 5 | | - | - | |

**Asset 2** ______________________________________________

| | Threats | Likelihood | Impact | Risk Rating |
|---|---|---|---|---|
| 1 | | - | - | |
| 2 | | - | - | |
| 3 | | - | - | |
| 4 | | - | - | |
| 5 | | - | - | |

**Asset 3** ______________________________________________

| | Threats | Likelihood | Impact | Risk Rating |
|---|---|---|---|---|
| 1 | | - | - | |
| 2 | | - | - | |
| 3 | | - | - | |
| 4 | | - | - | |
| 5 | | - | - | |

**Asset 4** ______________________________________________

| | Threats | Likelihood | Impact | Risk Rating |
|---|---|---|---|---|
| 1 | | - | - | |
| 2 | | - | - | |
| 3 | | - | - | |
| 4 | | - | - | |
| 5 | | - | - | |

**Asset 5** ______________________________________________

| | Threats | Likelihood | Impact | Risk Rating |
|---|---|---|---|---|
| 1 | | - | - | |
| 2 | | - | - | |
| 3 | | - | - | |
| 4 | | - | - | |
| 5 | | - | - | |

# RISK MATRIX

| | | | | |
|---|---|---|---|---|
| IMPACT | High | Medium | High | High |
| | Medium | Low | Medium | High |
| | Low | Low | Low | Medium |
| | | Low | Medium | High |
| | | | LIKELIHOOD | |

# DEFINITIONS

## Impact Scale

**Low Impact:** Low impact risks in IT risk assessments are those that may cause only minor disruption or damage to the infrastructure, such as a temporary outage or minor data loss. These risks tend to have limited exposure and require relatively simple and low cost solutions. Examples of low impact risks include hardware failure, software bugs, employee errors, and natural disasters.

**Medium Impact:** Medium impact risks in IT risk assessments are those that may cause significant disruption or damage to the infrastructure, such as data loss, system shutdowns, and financial losses. These risks tend to require more complex solutions and have a higher cost associated with their mitigation. Examples of medium impact risks include malicious attacks, unauthorized access to critical systems.

**High Impact:** High impact risks in IT risk assessments are those that may cause severe disruption or damage to the infrastructure, such as permanent data loss, system failure, or operational downtime. These risks tend to have extensive exposure and require complex solutions with a high cost associated with their mitigation. Examples of high impact risks include data breaches, ransomware attacks.

## Likelihood Scale

**Low Likelihood** in IT risk assessment refers to risks that are unlikely to occur, but still exist and should be considered. These risks may have serious or catastrophic consequences if they do occur, so they must be assessed carefully. Low likelihood risks can include natural disasters, new security threats, technology failure, or malware attacks.

**Medium Likelihood** in IT risk assessment refers to risks that are moderately likely to occur and should be considered. These risks may have serious or catastrophic consequences if they do occur, so they must be assessed carefully. Medium likelihood risks can include a wide range of events and activities, such as cyberattacks, insider threats, malicious software attacks, or data breaches.

**High Likelihood** in IT risk assessment refers to risks that are highly likely to occur and should be taken seriously. These risks may have serious or catastrophic consequences if they do occur, so they must be assessed carefully. High likelihood risks can include common software vulnerabilities, human errors, misconfigured systems, phishing attacks, and other security threats. Additionally, they can also include natural disasters, such as floods, fires, or storms.

## PART 2

# PROTECT YOUR BUSINESS ASSETS

An Essential Webinar For IT Managers
On Incident Management & Response.

# TABLETOP EXERCISE

## RANSOMWARE

I know it's something no one wants to experience.
And I see so many vulnerable networks after auditing hundreds of companies.

While your network's susceptibility to malicious attackers is something always top of mind, another worrisome piece to the whole ransomware puzzle is how to recover from an event.

**Nearly every company I've spoken with has had trouble communicating to me their recovery plan.**

They might say they have backups or that their cloud solution handles it, but hardly anyone has actually been able to walk me though steps to validate that they're doing enough on the recovery side that they actually have disaster recovery handled. Their plan might have been well-thought (that is when they have one in the first place), but after years of neglect, many are unable to satisfy a critical requirement.

They've put off testing their plans (and updating them) though tabletop exercises to make sure they will actually work.

I want to walk through setting up and executing a tabletop exercise that will test your plan.

### First, What Is A Tabletop Exercise?

Your tabletop exercise should be a way to further test and facilitate discussion around concrete plans that will manage and mitigate any sort of disaster—ransomware to Mother Nature and beyond. You are probably thinking the main test will be to evaluate your business continuity and disaster recovery plans.

Most often, your team will help define a couple of scenarios most likely to occur and test (in theory) the efficacy of your plans step by step.

What you should take away from your tabletop exercise is insights into how well your plan will likely perform in a real-life scenario and identify weaknesses to correct before an event actually develops.

### What Happens In A Tabletop Exercise?

Your tabletop exercise should be a discussion- based session where your team informally meets to discuss their roles during an emergency. You will have a facilitator that takes ownership of guiding participants through resolving issues from various scenarios.

If you already have a response plan in place, one of these exercises might only eat up a couple of hours—simply validating that your current approach is effectively addressing all issues coming up in the incident and figuring out any ways to improve.

## Essentially, most tabletop exercises should follow this type of schema:

☑ Set goals

☑ Select functions or plans to be tested

☑ Choose participants from each department

☑ Establish ground rules

☑ Develop a disaster scenario, related to your local environment

☑ Confirm assumptions involving available resources, such as phone, internet and staffing

☑ Conduct the exercise

☑ Determine whether the exercise is tied to any key vendors

☑ Document and discuss the results

*After you're done with an exercise, evaluate whether your goals and objectives were met and receive any feedback to improve the meeting.*

***If you're interested in actually improving your disaster response plan, here are a few things you should consider:***

### Identify Your Stakeholders

who will be involved in the event? Consider who core members of your crisis team are. I would think of the main processes for your business and make sure to include each of the process owners (they all will be involved at some level in the recovery). Also note that different scenarios will likely require different stakeholders, so when you are planning out your event, make sure to identify what parts of your company and what expertise you will need on hand to help participate.

### Understand What You Will Talk About

inviting a whole bunch of people to the meeting is one thing, but providing them with a sound business justification for why they'd want to think about imaginary hackers is an entirely different beast. Until you've communicated your WHY, you might not have buy-in from leaders on your team as to why they should be spending (or in their minds, wasting) their time on the exercise.

### Identify Your Business Impact

when running through each scenario, understand what mission-critical applications or data will be impacted by the event? Will you be able to operate (at least getting the mission-critical stuff done)? What would your output look like? Review the impact by major department within your company and focus on where the problems will arise from that scenario.

### Execute Your Tabletop Exercise

begin mapping the malware attack (or other disaster), along with its damage. As you move through the attack, you will probably uncover steps and details you will have to act on. Make sure to ask questions like: will it be feasible to restore? Can we restore from backup at this point? Who will get notified? When to inform the leadership team?

# THE TABLETOP EXERCISE

A tabletop exercise or simply a "tabletop," is a staged event where management and/or staff meet in an open forum to discuss actions for response to a specific emergency scenario. The informal format facilitates participation and is structured to explore emergency procedures, recovery plan details, standard operating procedures and personnel resources to recover critical functions.

**A tabletop exercise simulates a disaster without interrupting normal organization operations.** At the beginning of the exercise, a scenario is presented to participants by a facilitator, who guides participants in a verbal "walk through" of their organization's emergency plan. The length of a tabletop exercise is typically one to three hours.

While only one of many ways to exercise a organization's emergency plan, a tabletop has a number of advantages. The tabletop can have a broad or narrow focus, is economical and flexible, and most importantly, it presents a very real scenario in a non-threatening format. Tabletop exercises are used to:

- Determine if participants can realistically "talk through" their critical functions during an emergency;
- Help participants become more aware of possible weaknesses and gaps in the plan;
- Thoroughly acquaint participants with the contents of their organization's plan.

A tabletop is flexible because the scenario can be structured to exercise particular sections of a organization's emergency plan or the entire plan. If an organization has multiple departments or locations, the disaster scenario can target specific departmental functions or locations. The purpose is to allow for the discovery of weaknesses during a non-threatening exercise rather than during a real disaster.

## KEY ROLES IN A TABLETOP EXERCISE:

- **The Exercise Facilitator** presents the scenario, facilitates group problem solving, controls the pace and flow of the exercise and stimulates discussion using injects (problem statements) that occur on a timeline appropriate to the exercise scenario.

- **Exercise Players** (participants) are organization staff and invitees who address the goals and objectives of the exercise and participate in the facilitated discussion.

- **The Exercise Evaluator** does not participate in the exercise, but takes notes during the exercise, making observations about what happens during the exercise specifically related to the group's ability to achieve the stated objectives. The evaluator may also note "Action Items" that should be considered to addresses weaknesses/gaps revealed during the exercise.

- **An Exercise Observer** is an optional role. Some exercise planners may appoint observers, perhaps from other disciplines or external partners, to observe the exercise and provide feedback.

# Designing a tabletop exercise: Step-by-step

Follow the steps below and the sample Tabletop Exercise Planning Worksheet on the following pages to design your own tabletop exercise.

## Step 1:

**Assess your organization's needs.** Has your organization had to activate its plan? If so, use that experience to help identify areas of need. What are the training needs of new staff? Review the training logs for your organization – where are the gaps? For each need, identify the corresponding section(s) of your organization's Emergency Plan to which it is related.

## Step 2:

**Prioritize the needs and determine the scope of the exercise.** Based on your assessment (step 1), prioritize the training needs and determine what should be exercised first. Will it be a focused exercise (a power outage) or will it involve external partners? For example, a test of the viability of your transportation contracts might include external partners. Does the function being tested involve multiple departments?

## Step 3:

**Write a goal (purpose statement) for the exercise.** What are you trying to improve/establish? A tabletop exercise can include more than one goal, but keep the one to three hours timeframe in mind when planning goals and objectives for a single exercise. Also, always tie the goal/ purpose to the organization's written emergency plan. See the following pages for sample goals and objectives.

## Step 4:

**Write specific objectives for the goal.** What are the ideal outcomes for the exercise and how will you know if you have achieved them? For example, if the exercise purpose is to test the access staff have to the emergency contact list, objectives would be both the access that staff had to the list (could they locate it?) and the accuracy of the list (did it contain up-to-date information?). See the following pages for sample goals and objectives.

## Step 5:

**Select or create an emergency scenario.** Every tabletop exercise revolves around a specific emergency scenario – wildfires in the area, hurricane warning/watch, nearby chemical spill. Planners can use the sample hurricane scenario provided in this Guide or create a unique scenario appropriate for their organization. Write specific "injects" (problem statements) to go along with the scenario to be introduced by the facilitator at specific times to direct the discussion. See the following pages for a sample scenario and injects.

## Step 6:

**Identify exercise participants.** The scope of your exercise will contribute to the selection of participants. Which organization staff should participate? Should external partners be included, such as the local emergency management office, county health department, law enforcement, fire department, or others? If so, will they be players (participants) or observers? Also, remember to appoint an evaluator to observe and provide written comments.

## Step 7:

**Determine date/time/place.** A tabletop exercise generally takes 1 to 4 hours to conduct, but can be longer. It should be conducted at a location conducive to the exercise goals and objectives.

## Step 8:

**Invite players (participants) and any external partners if appropriate.** Be sure to give plenty of advance notice so that participants can make arrangements in their work schedules to attend.

## Step 9:

**Prepare materials.** Provide a Situation Manual to each participant at the beginning of the tabletop exercise. A Situation Manual is the participant handbook for discussion-based exercises. It provides background information on the scope, schedule, and objectives for the exercise. It also presents the scenario narrative for participant discussions during the exercise. The Situation Manual gives players in discussion-based exercises the background information about the exercise they will need to fully participate, as well as the scenario narrative which they will be discussing. The exercise facilitator will also need the injects (problem statements) to direct and stimulate discussion. The evaluator will need a copy of the Situation Manual and a form to record their observations and notes. See the following pages for examples.

## Step 10:

**Conduct the exercise.** Convene the tabletop exercise, giving each player a Situation Manual. The facilitator presents the first scenario and continues to facilitate the exercise using the injects prepared by the planning team. The appointed evaluator observes and takes notes. At the designated time, the facilitator concludes the exercise.

## Step 11:

**Evaluate the exercise.** Immediately following the tabletop, the planning team leader may choose to conduct a debrief of the exercise, providing an opportunity for all participants to discuss the exercise and identify concerns and issues to be addressed in the After-Action Report. The debrief process answers these questions:

- What went well?
- What didn't go so well, and what might be the root causes of any concerns?
- What were the surprises, if any?
- Were the exercise goals and objectives met? If not, why not?
- Are the reaction items for follow-up in an improvement plan?

***Tabletop Exercise Planning Worksheet and Examples***

A two-page Tabletop Planning Worksheet and directions for its use follow.

***Worksheet & Examples***

# Tabletop Exercise: Planning Worksheet

***Tabletop Exercise Title:*** ______________________________

***Emergency Plan Being Exercised:*** ______________________________

*State the specific section of your emergency plan related to the exercise goals/objectives*

## EXERCISE GOALS & OBJECTIVES

***Goal 1:*** *Write a concise goal that describes what you want to achieve by exercising this section of your Emergency Management Plan. Each goal must have separate measurable objective(s).*

***Objectives for Goal #1:*** *Write at least one objective for the goal to measure its achievement. Multiple objectives are often helpful.*

## EVALUATOR NOTES

***Leave this column blank.*** *The exercise evaluator will use this space to record his/her observations about the exercise and comments about the achievement of the stated goals and objectives.*

## ACTION ITEMS FOR FOLLOW-UP

***Leave this section blank.*** *This section is used by the evaluator to describe actions that need to be taken to correct areas identified as needing improvement during the exercise. This section may also be completed by observers, the organization's risk manager or others. It might also be completed post-exercise, after reviewing the evaluator and/or observers notes and discussing the exercise experience with others whose input might be needed to write the improvement plan section of the exercise's After-Action Report.*

## SCENARIO & INJECTS

### *Problem Statements*

*Injects are used to help direct the discussion about the scenario presented for the exercise.*

### INJECT/MESSAGE

*In chronological order, write the injects (messages) that should be given to participants necessary to meet the goals and objectives for the exercise. The inject(s) may be presented verbally, or in other ways to simulate how it might be received during an actual event (e.g., telephone, TV).*

*You may want to create several injects to ensure that all objectives can be met by the exercise.*

*Remember to list the injects in the order that you intend for them to be presented by the facilitator during the exercise.*

### EXERCISE GOAL & OBJECTIVE #

*Write the objective # that correlates to the message you have written.*

### TIME ISSUED

***Leave this column blank.*** *The evaluator will use this column during the exercise to record the time when each inject is presented to the participants.*

## SCENARIO & INJECTS

### *Tuesday, 11:00am: One of the staff members gets phished.*

*They clicked on a link in an email, later realizing that they had fallen for an attack.
They report the incident to the helpdesk. What do we do?*

### INJECT#1: 2:00PM

*Identify by name and title, the person in charge during the emergency and one alternate, should that person be unable to serve in that capacity.*

### INJECT#2: 2:05PM

*What documentation do you have to verify your response?*

### INJECT#3: 2:10PM

*Are there any other threats from this event that could impact the organization, beyond the one machine?*

### INJECT#4: 2:15PM

### INJECT#5: 2:20PM

### *The attackers gain access to the employee's email.*

*They then proceed to email all the contacts in the user's account with a message containing a link with an executable.*

**INJECT#1: 2:35PM**

**INJECT#2: 2:40PM**

**INJECT#3: 2:45PM**

**INJECT#4: 2:50PM**

**INJECT#5: 2:55PM**

## PART 3

# PLAN AHEAD, PREPARE NOW

How To Create An Effective IT Disaster Recovery Plan.

# DISASTER RECOVERY PLAN
# Table of Contents

5. **Restoration of Normal Operations** (Details on how backups are created, where they're stored, and how they can be used to restore systems and data)
    a. Criteria for Restoration
    b. Process of Restoration

6. **Training and Awareness** (Guides, manuals, and other materials used to train staff on disaster recovery procedures)
    a. Training Programs
    b. Testing and Drills

7. **Plan Maintenance**
    a. Schedule for Review and Update
    b. Change Management Process

8. **Appendices**
    a. IT Inventory (A detailed inventory of all IT assets, including hardware, software, data, and network elements. This helps in understanding what resources are at risk and need to be recovered)

    b. Vendor Contact Information (A list of all vendors and third-party contacts that can provide support during a disaster recovery process)

    c. Backup Site Details (An alternate hot site plan should provide for an alternative (backup) site. The alternate site has a backup system for temporary use while the home site is being reestablished.

    d. Relevant Documentations

# KEY CONTACT FORM

HODGSON
CONSULTING & SOLUTIONS

Define people (name, role, contact information) the function is dependant upon.
*Include internal and external key contacts (business, IT, IT suppliers, vendors, etc.).

| Business Process/Function | Critical Employee's Role | Employee's Name | Employee's Emergency Contact # | Employee's E-mail | Critical Vendor's Role (IT, Technical Support, Equipment Support, etc. | Vendor's Name | Vendor's Emergency Contact # | Vendor's E-mail | Critical Supplier's Role (Parts, Materials, Labor, etc.) | Supplier's Name | Supplier's Emergency Contact # | Supplier's E-mail | Notes |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Sales Quote Application | Sales Manager | Joe Smith | 333-333-3333 | jsmith@company.com | IT | Quotewerks | 333-222-2222 | support@queotewerks.com | | | | | |
| Company Hardware | Purchaser | Mary Joe | 111-111-1111 | mjoe@company.com | IT Equipment | Amazon | 888-888-8888 | support@amazon.com | Parts | Lenovo | 321-321-32111 | support@lenovo.com | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |
| | | | | | | | | | | | | | |

HODGSON
CONSULTING & SOLUTIONS

1110 W. Lake Cook Rd, Suite 235
Buffalo Grove, IL 60089
www.hodgsonconsulting.com
847-906-5005