Managing the Chaos

- Setting up your Disaster Recovery Plan

It’s a fact: cyber attacks continue to rise.

- 122 records are stolen every **second.**
- Less than **5%** of those records will be encrypted.
- A company is hit with ransomware every **60** seconds.
- For a site outages, **67%** of companies estimate a loss of over **$20k+** for every day of downtime.

Information in Bloom
Management Services

We need to do more than defend.

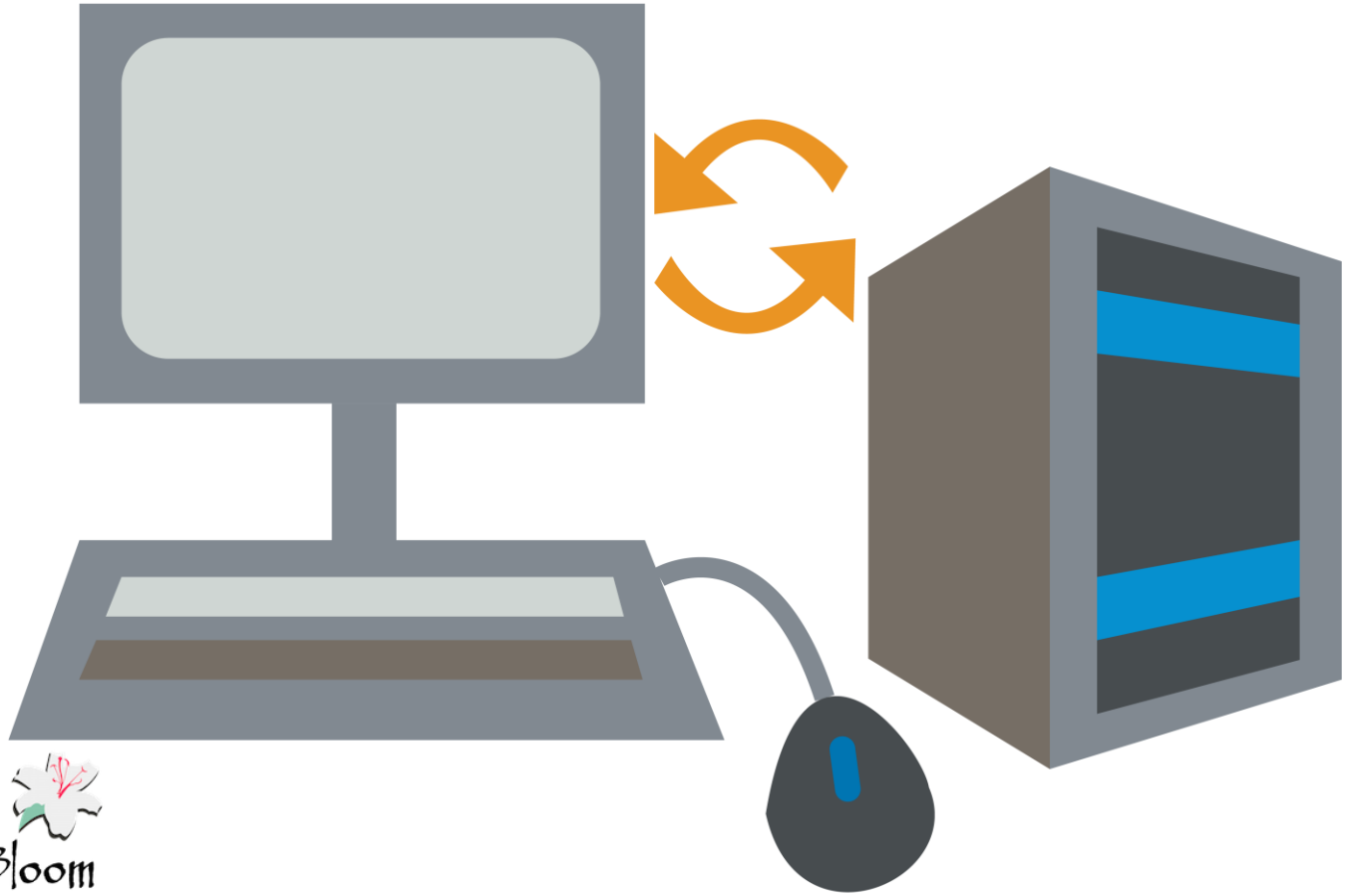
We need to be prepared.

Information in Bloom
Management Services

Enter the Disaster Recovery Plan

Information in Bloom
Management Services

What We Often Think of as Disaster Recovery



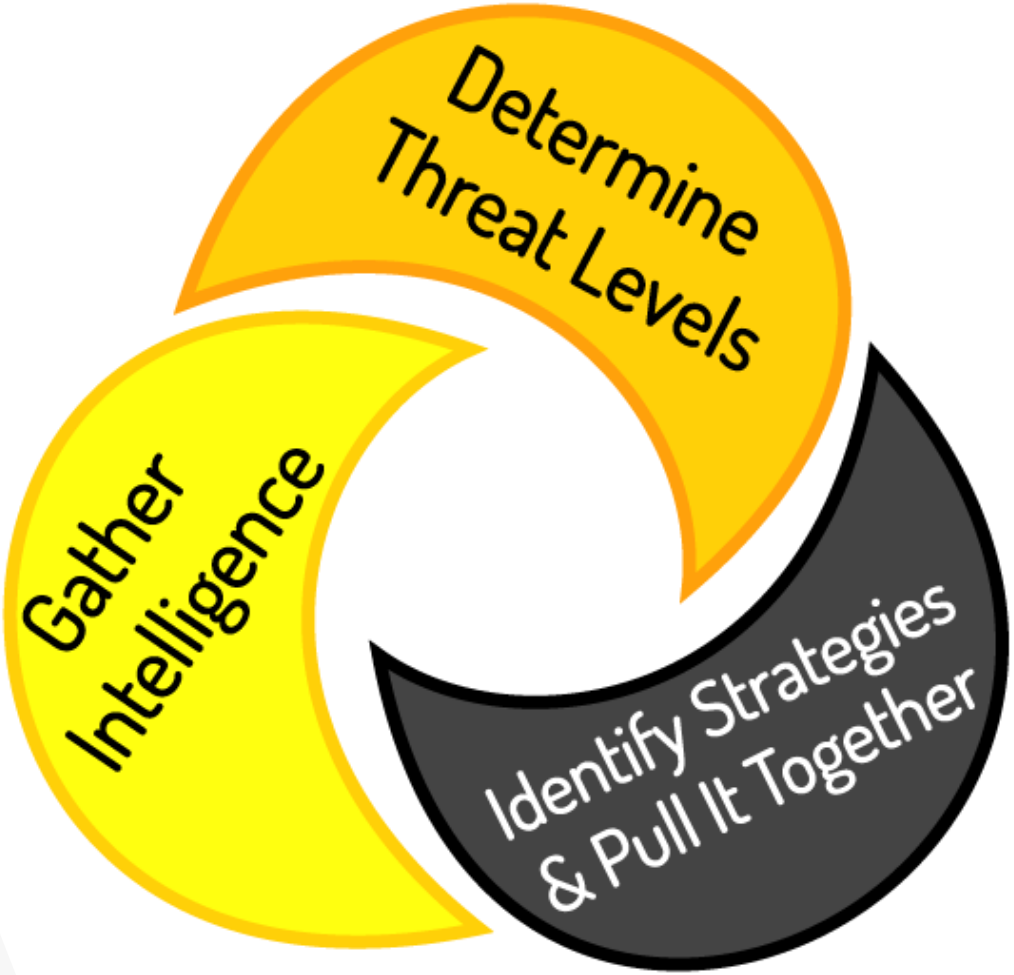
Information in Bloom
Management Services

What is a Disaster Recovery Plan (DRP)?

- **Documented process** for protection and recovery.
- **Prepare** how to put out the fires.
- **Minimize** damage when you get hit.
- Get back up and running **faster**.

Information in Bloom
Management Services

Elements of A Disaster Recovery Plan



Information in Bloom
Management Services

Gather Intelligence

What do we have, what are our safeguards and where’s that Bat-signal?

Information in Bloom
Management Services

Information Auditing and Data Mapping

- Learn the ‘what, where, how, who and why’ of your data.
- Involve stakeholders from all affected units.
- You can’t protect what you don’t know exists.
- Visualize the data’s pathways, partnerships, and processes.

Information in Bloom
Management Services

Identify Existing Safeguards

- What do we have to protect ourselves?

Do we have:

- Administrative safeguards?
- Technical safeguards?
- Physical safeguards?

Information in Bloom
Management Services

Important Contacts

- Who is in charge of responding to the crisis?
- Who needs to be contacted in the event of an attack or disaster?
- Who can do repairs, or supply needed materials?
- Who will speak for the company to victims, clients, employees or the press?
- Who can you call for help?

Information in Bloom
Management Services

Determine Threat Levels

Information in Bloom
Management Services

How Do We Find Our Organizational Threat Level?

Tools of the trade:

- Risk Assessment.
- Business Impact Analysis.
- Privacy Impact Assessment (if collecting personal information).

Information in Bloom
Management Services

Risk Assessment vs. Business Impact Analysis

Risk Assessment

- Threats & vulnerabilities.
- The likelihood and impact of an attack.
- What do we **value** most and how do we **reduce risk**?

Business Impact Analysis

- The effect of interruptions.
- The operational and financial impacts from major disruptions?
- How **fast** do you need to recover, and what can you **afford?**

Information in Bloom
Management Services

Problem Classification

Establish an internal code for identifying the threat level.

Problem	Signs/Symptoms	Risk Level	Time Objective	Class
Ransomware Bad Bunny	Message on screen, data locked	High. Infectious to rest of network.	1 hour	Class A
Database C Downtime	Staff unable to log in.	Low. Rarely used resource.	1/2 day	Class C

Information in Bloom
Management Services

Identify Strategies

Pulling it all together

Information in Bloom
Management Services

Problem Solving: Tactical Response and Recovery

- What response options have been identified?
- Ways you can speed up recovery?
- Map it out:

Threat	Prevention	Response	Recovery

Communications and Public Relations

- A crisis communication strategy is a must!

Should include:

- Holding statements & social media response.
- Is there a time requirement for reporting?
- Who does the talking? Who *doesn't*?

- Consider strategies for a social media PR crisis in your disaster recovery plan.

Information in Bloom
Management Services

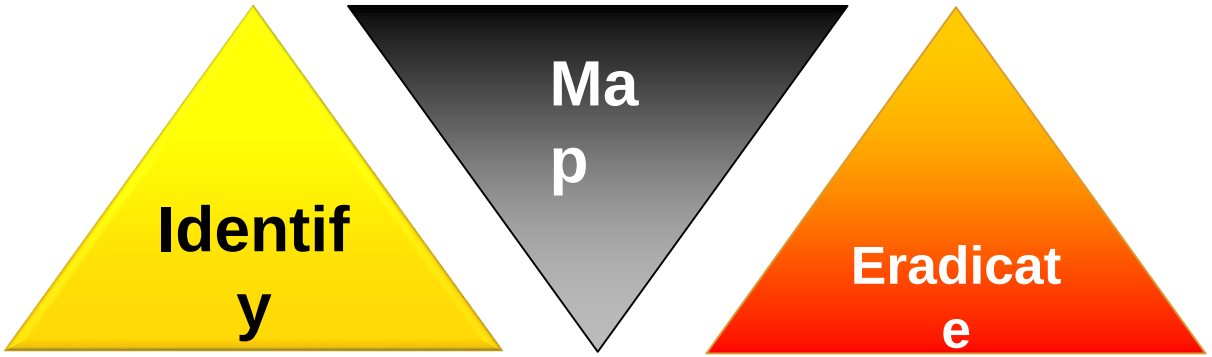
Plan: The Codified, Selected Strategy

- **Make the call**: which strategies and tactics will be used in an emergency.
- Document design: consider checklists, summaries, or spreadsheets.
- How does the information get found **fast**?

Information in Bloom
Management Services

The Importance of Triage on the Cyber Attack Battlefield

- **Triage**: the ability to sort problems and allocate limited resources based on need or benefit.
- Determining the **order** of problem response.
- Komand Blog Method:



Information in Bloom
Management Services

Drills and Updates

- Update your Disaster Recovery Plan on a regular basis.
- Rule of I.T: don’t forget to test!
- Training: does everyone understand their role?

Information in Bloom
Management Services

Need More Help?
Existing Standards and Options

- *U.S. National Institute*: NIST SP 800-34
- *International Organization for Standardization*: ISO/IEC 24762
- *British Standard Institute*: BS 25777

- Disaster Recovery Services are available commercially.
- Be aware: does the DRS cover disaster relief, or data recovery?
- Consider a needs analysis before you outsource.

Information in Bloom
Management Services

Contact

bloom@victoriamcintosh

@vmcntosh

www.victoriamcintosh.com

Information in Bloom
Management Services