Cybersecurity Fire Drills | Incident Response Plans and What Comes Next

Presented by: James Motz, Produced by: Nathan Austin & Stephanie Kingslien, Mytech Partners

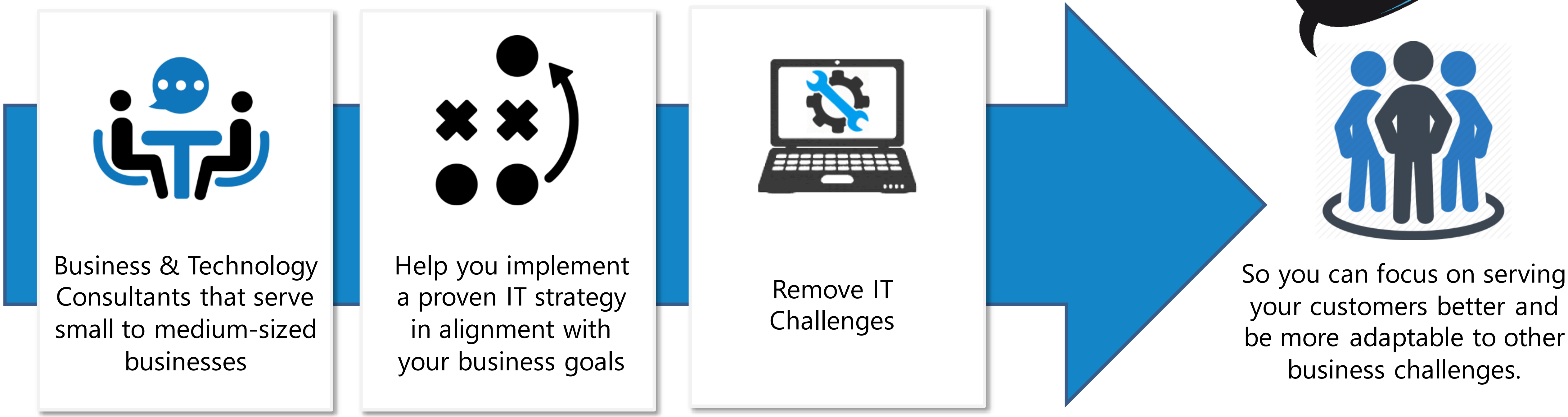
MYTECH PARTNERS

Quick Takes

- *What is an "Incident Response Plan"*
- *What goes into a good plan?*
- *How to make the plan useful*
- *Next steps to build your own plan*

One Minute about Mytech

MAKE I.T. EASY!



Business & Technology Consultants that serve small to medium-sized businesses

Help you implement a proven IT strategy in alignment with your business goals

Remove IT Challenges

So you can focus on serving your customers better and be more adaptable to other business challenges.

Our clients achieve 4x more value and productivity from their IT investments.

Cybersecurity Fire Drills

PURPOSE OF THIS SESSION – LEARNING ABOUT INCIDENT RESPONSE PLANS

REASONS TO HAVE ONE

THINGS TO CONSIDER WHEN PREPARING

Q&A

What it’s like…

- Bad day!
- Your organization owns regulated data
- IT is responding to an Event: unauthorized mailbox access
- Probable data disclosure
- Everyone looks at you for what to do next! ☺

…Without a Plan

- Everyone is looking at you for what to do next!
- Call… someone? The insurance agent!
  - …he's out golfing and not answering his cell
- Ask IT to change everyone's password!
  - They get it half right, and now 50% of your team is locked out
- Tell marketing to warn clients about your breach!
  - Your clients and your staff are now demanding answers

About 3 days later you get started on a low quality response.

…With a Plan

- Everyone begins working on their tasks
- Your team notifies your underwriter's cyber hotline
  - Breach counsel has been assigned
- Your IT team has taken standard containment actions
  - Actively coordinating with cyber response specialists
- Your PR team has created internal and external messaging
  - Clients and staff understand you are acting

You have an understanding of risk within 8 hours – a high quality response.

Practicing Your Fire Drills

- You might pass an inspection on effective *controls*…
  - …but no one knows what to do when they *fail*.

- The controls to prevent are not enough on their own

- The team needs to know what to do
  - And practice it!

Why is this so important now?

“Every organization today is dependent on technology for mission and business success” (Dr. Ron Ross, NIST)

- Risks to that technology must be managed
- Regulation and compliance requirements are only getting stronger
- Someday, something bad WILL happen. What then?

Make your approach **Formal**, **Focused**, and **Coordinated**

Cybersecurity Incident Examples

- Attempt to gain unauthorized access
  - Business email compromise
- Denial of service to information resource
  - DoS attack
- Unauthorized use of information resource
  - Organization website defaced
- Unauthorized modification of information
  - Financial Fraud
- Loss of protected information
  - Disclosure of personal health data

INCIDENT RESPONSE PLAN ELEMENTS

Key elements of an IR Plan:

Who will do what?

How will they do it?

And by **when**?

Key components overview

- Response structure
- Roles and responsibilities
- Resources available
- Communication channels
- Measurements of the response effort
- Documentation and reporting requirements
- Expectations for internal reporting and review

Response Plan Structure

- 1. Preparation
- 2. Detection & Analysis
- 3. Containment, Eradication & Recovery
- 4. Post-Incident Activity

Key components - detailed

Roles and Responsibilities

Who will do What – With Names!

e.g. Incident "commander", computer incident response team, insurance activation

Resources

Include how to locate/activate these resources

e.g. Cyber insurance policy, breach coach, law enforcement

Communication

How will you get the word out?

e.g. Backup numbers, personal email, multiple channels

Key components - detailed

Measurement

Incident response is expensive – manage your costs!

e.g. Categorization, metrics for assessing effectiveness

Documentation & Reporting

Set standards for preserving evidence & reporting properly

e.g. Legal obligations, when to consult

Internal Review

Arguably most important step – LEARN YOUR LESSONS!

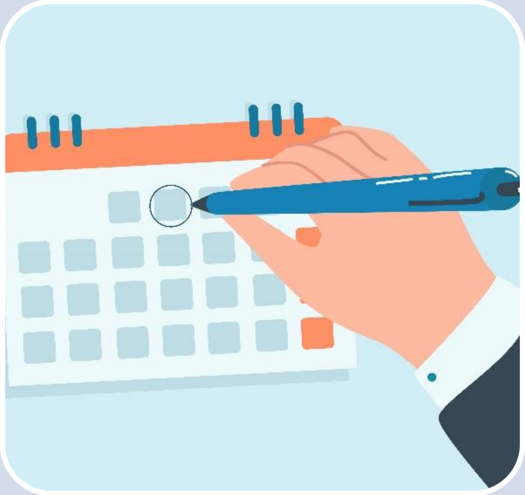
e.g. How to improve controls, how to seek understanding & not blame

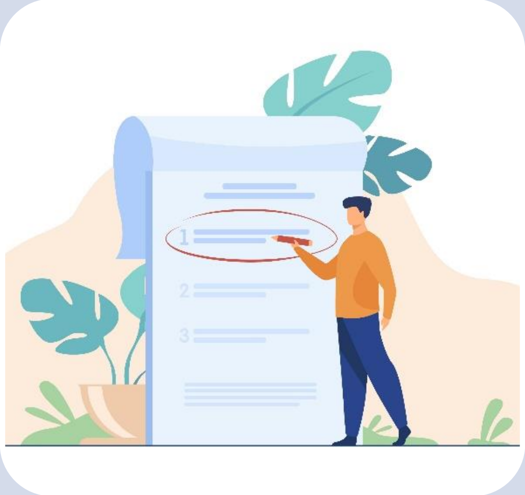
HOW TO PUT TO USE

Available, Updated, and Understood

- Make it Accessible
  - Team can locate
  - Hard copies
- Governance
  - Structures allowing success
  - Establish Due Diligence
- Training
  - Leaders and Responders
  - Run through the plan

Summary





Assemble the Team

- Leaders
- Responders
- External resources

Keep it Current

- Regularly get the plan out
- Update the information

Practice

- Play “What If” collectively
- Train your staff

Lessons Learned

- Review after the fact
- Make improvements

Build Your Incident Response Plan

A guide for a cybersecurity crisis

In-person workshop
October 2022

MYTECH PARTNERS

Join us for Future Events

Please Subscribe to our YouTube Channel or Follow us on LinkedIn

Share these Events with those who can benefit

Join us for in-person October IRP workshops:

Mytech.com/events

Every Other Month Power User Group Sessions

Thank you for Attending!
Open for Questions…

Presented by: James Motz, Produced by Nathan Austin & Stephanie Kingslien, Mytech Partners

MYTECH PARTNERS®