“Demystify Cybersecurity for Small and Medium Sized Manufacturers” Webinar

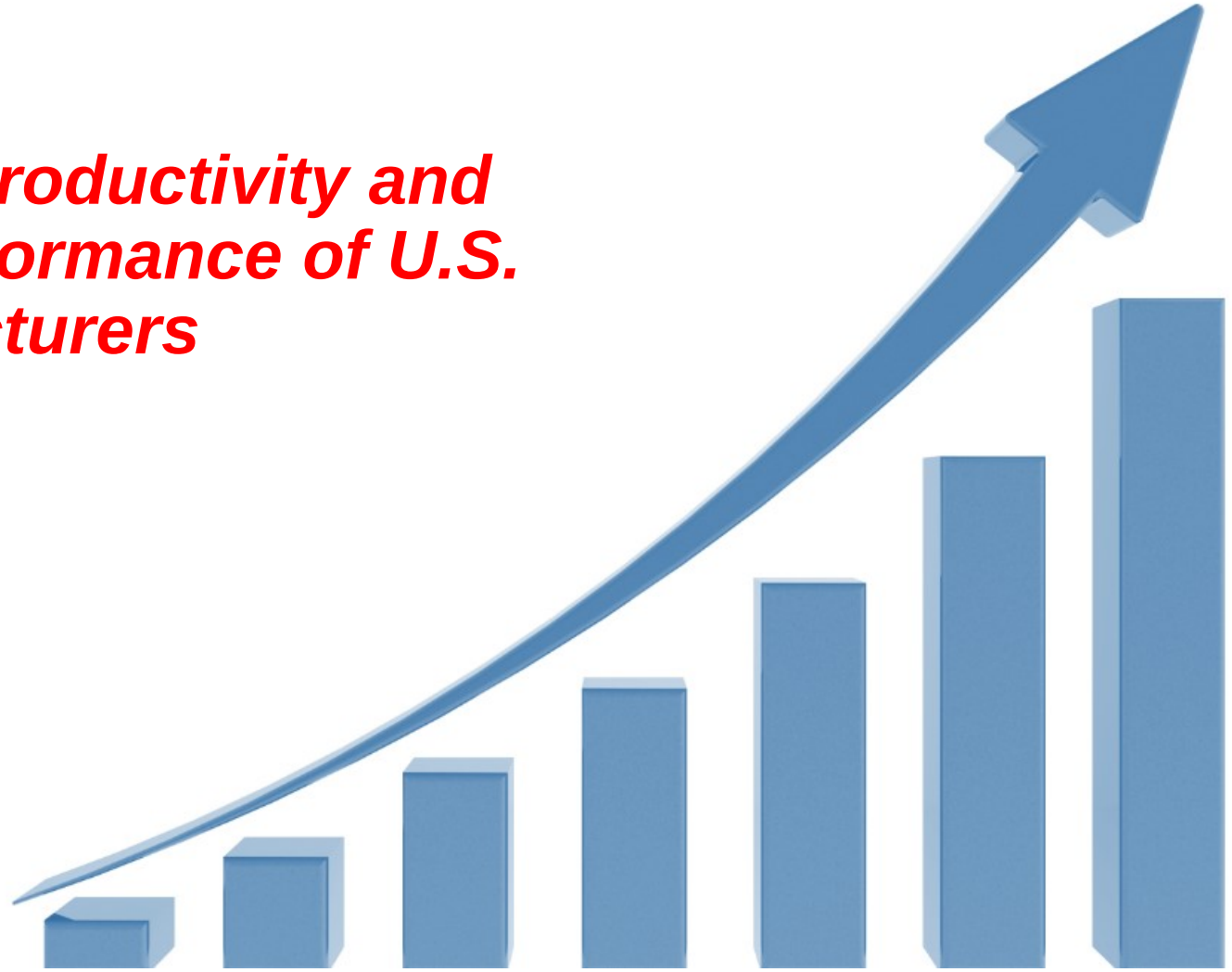
Webinar, September 17, 2020, 12:00-1:00 pm

Webinar Agenda

1. Introductions
2. What is Cybersecurity?
   - Why is it important?
   - Cybersecurity Audit
   - Prepare for CMMC
3. Remediation
   - Importance of Managed Services
4. Funding Opportunities
5. Q&A

Manufacturing Extension Partnership Mission

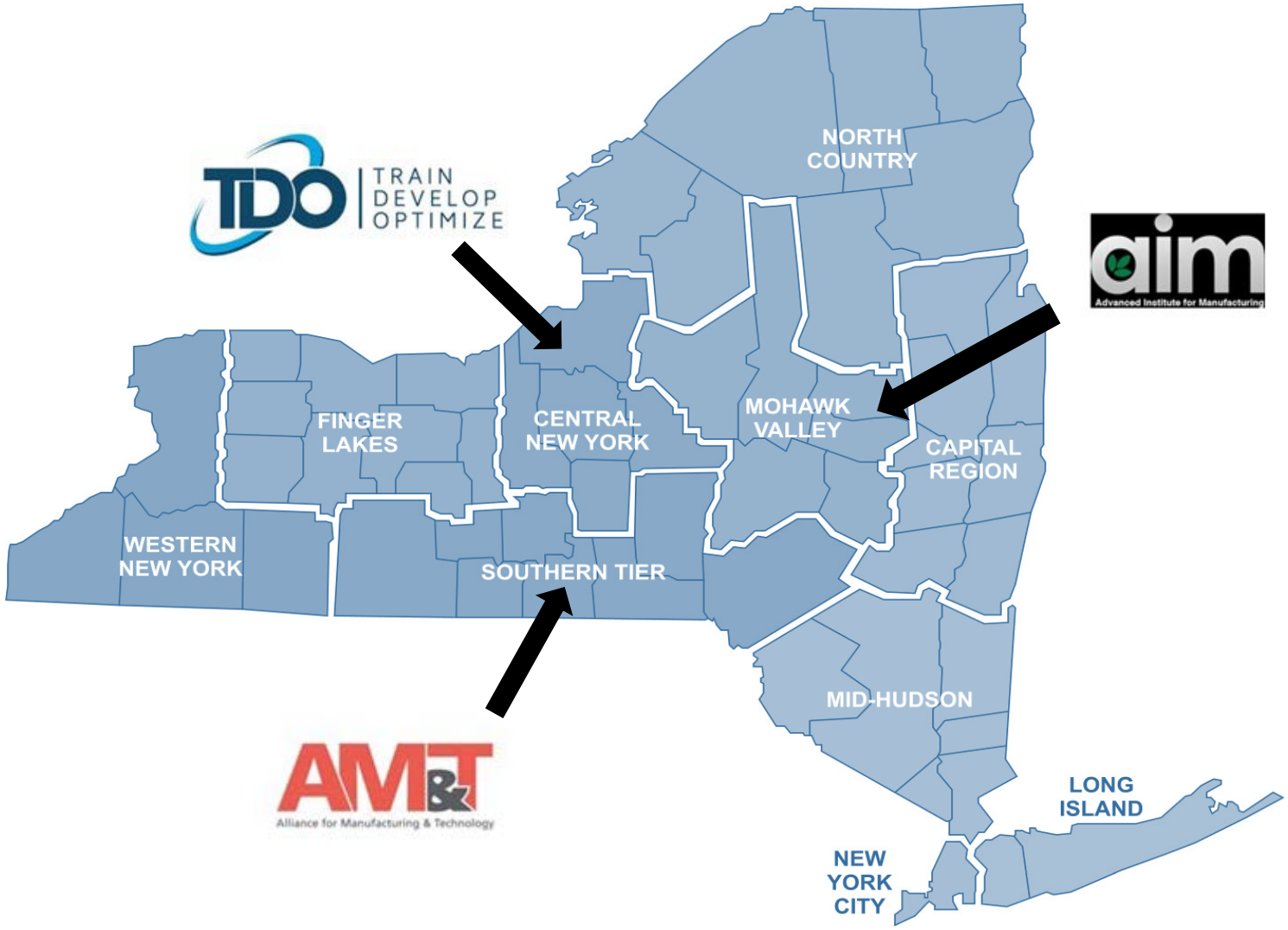
To enhance the productivity and technological performance of U.S. manufacturers



National MEP 2019 Results

The NYMEP System

- 10 Regional Centers
- One State-wide Center, FuzeHub



NY MEP Services Offered

- Growth and Innovation
  - Strategic and Operational Planning
  - Sales & Marketing
  - Export Assistance
  - New Product Development (NPD)
  - Entrepreneur and Start-up Assistance
- People Development
  - Leadership Principles & Coaching
  - Supervisors Training
  - General Workforce Training
- Operational Excellence
  - Quality and Environmental Services: ISO9001, AS9100, ISO14000
  - Lean Enterprise and Six Sigma Programs
  - Information Technology
  - Project Management
- And More…
  - Technology Road Mapping
  - Cybersecurity
  - Safety Programs
  - Grant Assistance

Our Partner Presenters Today

- Paul LaPorte - Cyber Security Coordinator, As an IT professional for 10 years, Paul has provided a variety of IT and Cyber Security solutions and training in the fields of engineering, manufacturing, education, commerce, insurance, and more. Paul has an A.S in Microcomputer Technologies: Technical Support and a B.S. in Network and Computer Security. Prior to joining AIM, Paul was the Interim Director of Information Technology at the Utica School of Commerce.

- Steve Stellwagen - Steve Stellwagen is an IT Solutions Consultant at ComTec Solutions, an ERP and IT managed services provider based in Rochester, New York, that has been serving a diverse range of manufacturers for over 25 years primarily in the Northeastern U.S. Steve specializes in helping business leaders find ways to succeed by leveraging their investments in technology in an efficient and cost effective manner, with a focus on their business objectives first. He has over 20 years of experience in the technology services industry, and has played an integral role in creating meaningful partnerships at ComTec Solutions.

Webinar Agenda

1. Introductions
2. What is Cybersecurity?
   - Why is it important?
   - Cybersecurity Audit
   - Prepare for CMMC
3. Remediation
   - Importance of Managed Services
4. Funding Opportunities
5. Q&A

Advanced Institute for Manufacturing

What is Cybersecurity?

What is Cyber Security?

Definition:

- Cybersecurity is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access. In a computing context, security includes both cybersecurity and physical security.

What is Cyber Security?

- Cybersecurity is the body of technologies, **processes and practices…**

What is Cyber Security?

- Cybersecurity is the body of technologies, **processes and practices…**
- Designed to protect networks, computers, programs **and data…**
- From attack, **damage** or unauthorized access…

What is Cyber Security?

- Cybersecurity is the body of technologies, **processes and practices…**
- Designed to protect networks, computers, programs **and data…**
- From attack, **damage** or unauthorized access…
- In a computing context, security includes both cybersecurity and **physical security**.

What is Cyber Security?

- Why is this important for small/medium manufacturers?
  - “I’m too small to be attacked”
  - “This won’t happen to me”
  - “I have more important things to worry about”

“Do you have insurance?”

Reactive vs. Proactive

- Nearly all businesses have insurance
  - To protect from unlikely but damaging events.
  - Customers will usually remain loyal and return.
  - Can afford to react after disaster

Reactive vs. Proactive

- Cyber attacks can irreparably damage business if one happens
  - Customer will lose trust
  - You've put *their* information at risk
  - Susceptible to litigation up the supply chain
  - Being reactive isn't good enough

- Small and medium manufacturers are one of the most popular targets for cyber attacks because business owners do not give security a high priority.
- Sixty percent of small businesses that are the victim of a cyber attack go out of business within six months of the event.

Reactive vs. Proactive

A strong cyber security plan provides a ***proactive*** solution rather than a ***reactive*** one. Instead of helping to recover from the disaster, it helps prevent the disaster from happening. Saving a business time, money, and preventing their reputation from being negatively affected.

Advanced Institute for Manufacturing

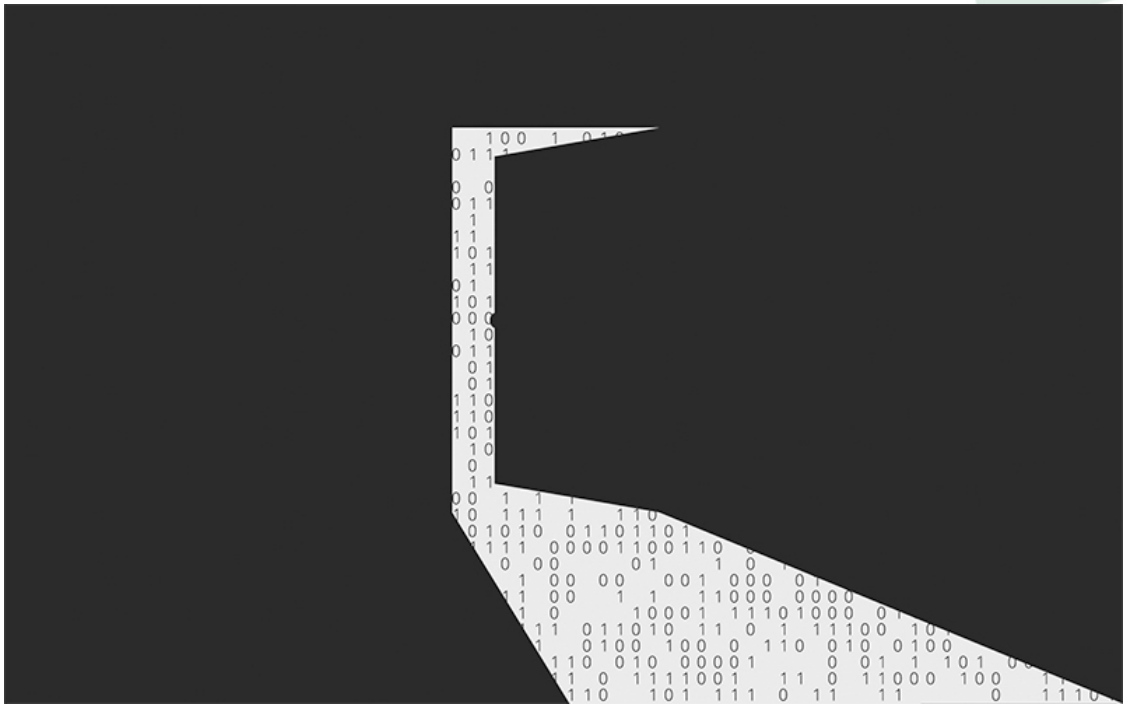
The Chain of Security

The Chain of Security

The areas which, when combined, comprise the majority of concern in regards to data theft and loss

The Chain of Security

- Physical: Can my information be accessed in the real world?



The Chain of Security

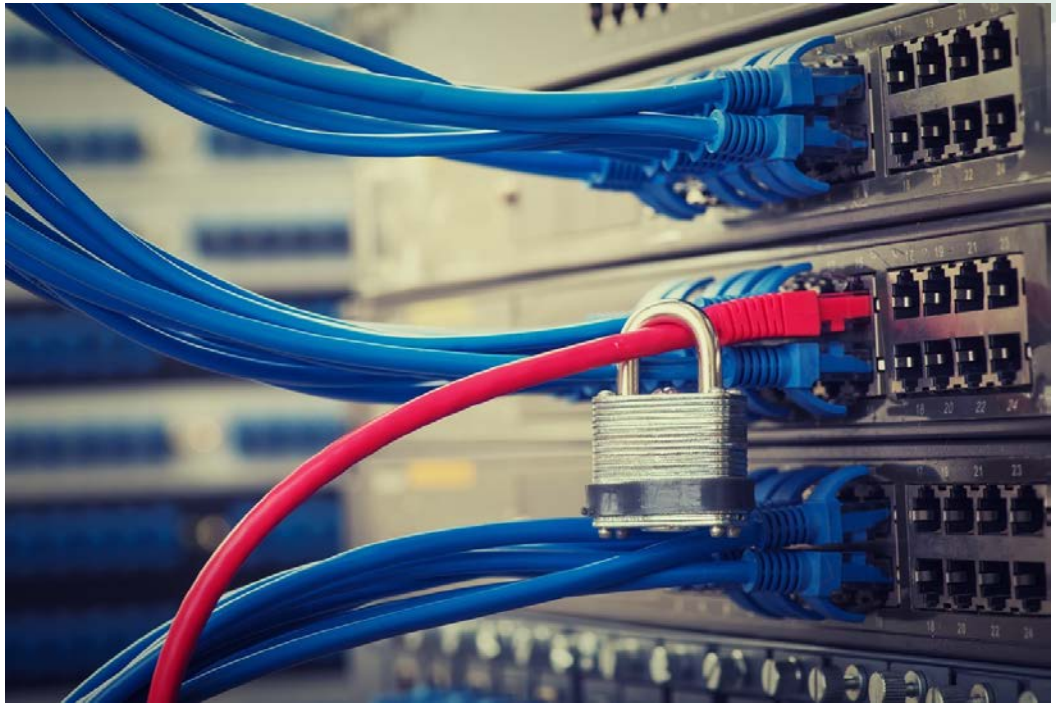
- Physical Security
  - Rarely associated with Cyber Security at all
  - Determines how easy it is for attackers to physically access information or devices

The Chain of Security

- Physical Security Considerations
  - Important equipment stored in secured areas (locked rooms/cabinets)
  - Physical access to building is restricted via locks, keypad/card swipe entry, etc.
  - Non-Employees entering facility have to sign in at reception/security station.
  - Video camera monitor entry points externally/key internal areas.

The Chain of Security

- Network: Can my information be accessed by an outside computer?



The Chain of Security

- Network Security
  - What people traditionally think of when they think “Cyber security”
  - Protects information and devices on network

The Chain of Security

- Network Security Considerations
  - Firewall installed to protect network.
  - User permissions are restricted to necessary duties
  - Anti-virus solution is present and up to date
  - Identity Management System in place
  - Program installation restricted to IT admins
  - Software updated and patched regularly
  - Public facing systems heavily secured and segregated from internal network

The Chain of Security

- Policy: Does my company have policies in place to keep my information safe?

The Chain of Security

- Policy Security
  - Rules set by management to determine how devices and information are handled.
  - Implementation of policies help support other areas of security.

The Chain of Security

- Policy Security Considerations
  - Company policy that clearly dictates usage of IT resources and handling of sensitive information
  - Documented references and restrictions on cell phones, password length, thumb drives, etc.
  - Clearly outline process for reporting IT and security incidents and who to report to
  - Allows information to be communicated uniformly and not through hearsay.

The Chain of Security

- Training: Are my employees properly trained to protect my information?

The Chain of Security

- Employee Training
  - Allows employees to safely and properly handle company devices and information.
  - Helps employees protect themselves and others from cyber security attacks.
  - The more knowledgeable a staff is, the more secure the company will be.

The Chain of Security

- Employee Training Considerations
  - Policy review with new employees upon orientation and existing employees at regular intervals
  - Allows proper communication of any additions to new policies and revisions to existing policies
  - Sound training and policies mean less incidents, reduced impact from incidents that do happen, and can help shift liability from incidents from the company to the employee if policies are violated

The Chain of Security

A chain is only as strong as its weakest link

Advanced Institute for Manufacturing

The Cybersecurity Assessment Process

Step One: Logistical Map

- Physical Walkthrough of the company
  - ID and document each individual device on network
  - Determine environment of IT devices and how they are being used
  - Allows specific questions to be asked about specific devices.
  - Overview of physical site security

Step Two: NIST 800-171 Review

- Review Entire NIST 800-171 Document
  - HR and IT Team involvement
  - 14 Sections, 110 Items
  - Compare company policies to see progress in meeting requirements

- Access Control
- Audit and Accountability
- Awareness and Training
- Configuration Management
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection
- Physical Protection
- Personnel Security
- Risk Assessment
- Security Assessment
- System and Communications Protection
- System and Information Integrity

Step Three: Employee Interviews

- Select five employees per 50-100 IT users
  - Varying departments
  - Varying company experience
  - Varying IT experience
  - General employees/management
- Ask same series of questions
  - Find discrepancies in policy communication/training
  - See what one area may know/believe over another
- NOT for disciplinary purposes

Assessment Report

- Assessment Report/Remediation Plan
  - Lists issues found in assessment
  - Notes compliance/non compliance compared to NIST 800-171
  - Suggested remediation steps for non-compliance
    - Prioritize remediation
      - Critical – Fix immediately
      - Very high – Within 30 days
      - High – Within 60 days
      - Medium – Within 90 days
      - Low – At company discretion

Follow Up Steps

- Post-Remediation Activities
  - Work with company to develop Plan of Action
  - Re-check for compliance with NIST 800-171 standards
  - Looks at trouble/non-compliant areas from previous assessment
  - Provide with revised assessment report showing updated compliance
  - Provide with completion letter if all requirements of NIST 800-171 are met/Plan of Action in place for non-compliant areas

CMMC Preparation

- Cybersecurity Maturity Model Certification (CMMC)
  - Builds on existing 800-171 requirements
  - Official certification that requires full audit
  - 5 Levels of certification
    - Most DoD companies handling CUI will require level 3 certification
  - Certification requirements to be rolled out in contracts over the coming years
  - Manufacturers encouraged to start preparing now

COMTEC SOLUTIONS

Creating the Foundation

Data Theft

43% of cyber attacks target small businesses.

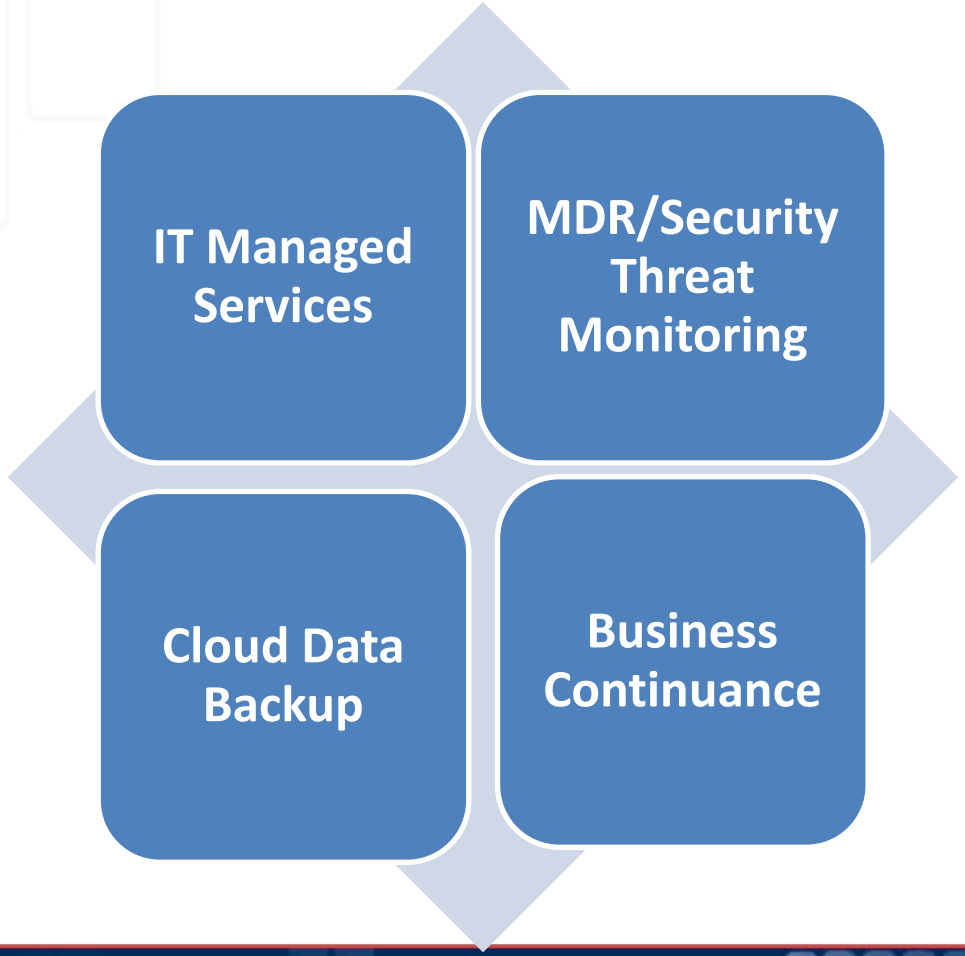
14% of small businesses today have the technology and the ability to mitigate cyber risks.

60% of small companies go out of business within six months of a cyber attack.

48% of data security breaches are caused by acts of malicious intent. Human error or system failure account for the rest.

NIST Framework

IT Services Overview



5 Elements of IT Managed Services

Proactive Monitoring (24x7)

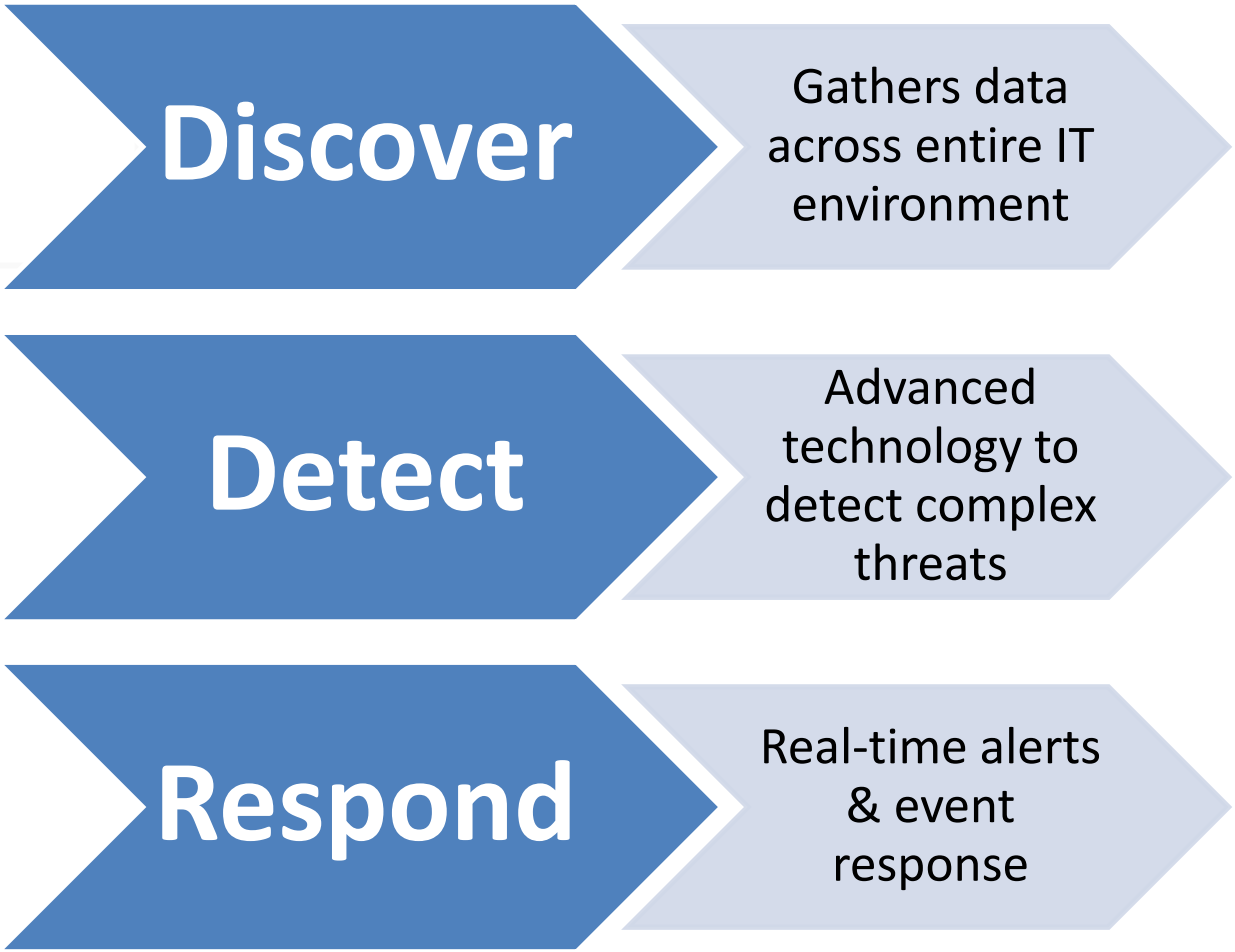
Response – SLA

Software Patching

Reporting/Playbook

Anti-Virus (Traditional vs AI)

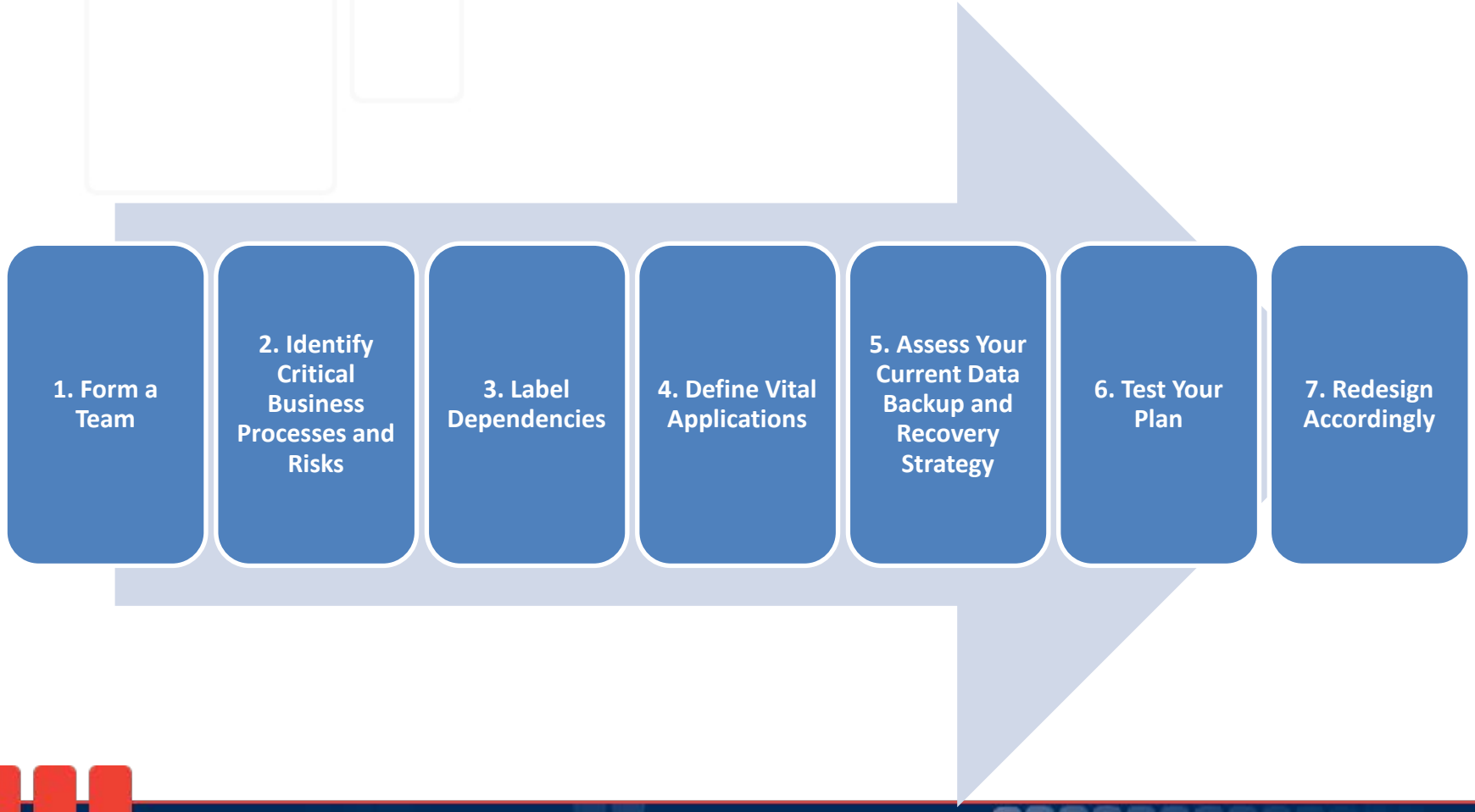
Security Threat Monitoring



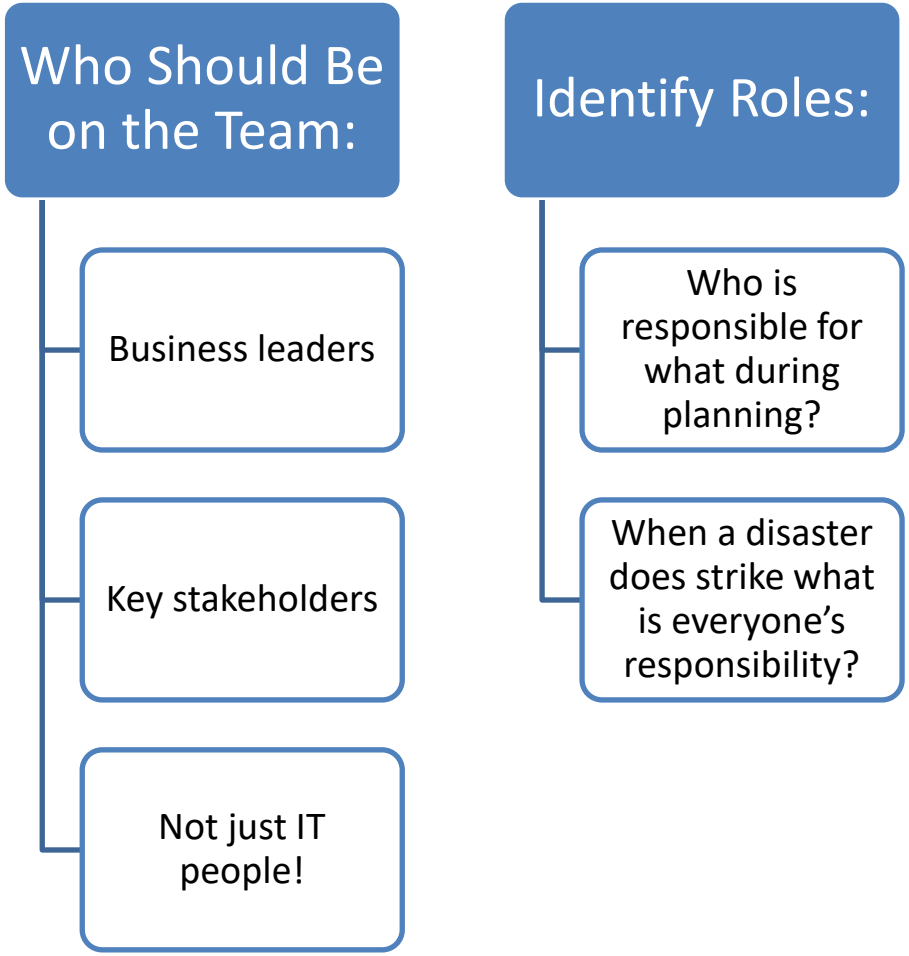
Cloud Data Backup

Reliability	**Automatic healing, validation and restore capabilities**
Compliance Safeguard	**Check for ITAR Compliance**
Automatic Process	**Eliminates the human element**

Creating a DR/Business Continuance Plan



Form a Team



Identify Critical Business Processes & Risks

Email or communication

- What if email is down? How will you communicate to your employees?

Manufacturing

- If we had a physical loss to the building, do we have partnerships where we could resume operations?

Phone system

Physical building considerations

Data in the cloud – how is it backed up?

Label Dependencies

Where is your weakest link?

What single points of failure do you have?

If employees don't have access to your primary business system, what is your Plan B?

Do you have redundant internet connections?

Do you have a generator to power your building?

Define Vital Applications

- Email
- Line of Business (LOB) Applications
- Engineering
- HR Information System (HRIS)
- Website (internally hosted?)
- Cloud based systems

Assess Your Current Data Backup & Recovery Strategy

On Premise

- Tape
- NAS

Cloud

- Where is your data?
- How quickly can you get it back?
- Is it stored in an ITAR compliant facility?

Site to Site

- More cost effective and best of both worlds IF you have that luxury.

Do you have workstations or laptops that are important? Are they being backed up?

Is laptop data stored on the network by default?

Assess Your Current Data Backup & Recovery Strategy

Define Recovery Point Objectives (RPO)

- The time allowed to elapse since the last backup of your data prior to the outage. How much data can you afford to lose?

Establish Recovery Time Objectives (RTO)

- The acceptable amount of time required to recover the business function after an outage. How long can you be down without these applications running?

Make sure your stakeholders agree to these objectives!

Monitor backups to make sure they are completed each day

- Do not rely on humans
- Test restore at least monthly

Test Your Plan

- Walk through your plan at least annually
- Make it part of your year end activities
- A full environment recovery test is expensive and time consuming
- The only way to truly find weaknesses in your plan is to exercise it

Redesign Accordingly

Take the results of your test and adjust as needed

When new critical applications are added to the environment make sure the plan is updated

DR Team may meet quarterly to discuss any changes in your business that would affect the plan

Remember, DR is NOT just an IT function!!

Educating Users

Quick Quiz to send to users

- https://phishingquiz.withgoogle.com/

Discrete Tools

- https://www.sophos.com/en-us/products/phish-threat.aspx
- https://www.knowbe4.com/

Safe Site check

- https://global.sitesafety.trendmicro.com/
- https://mxtoolbox.com/Public/Tools/BrandReputation.aspx
- https://safeweb.norton.com/
- https://transparencyreport.google.com/safe-browsing/search?hl=en

Webinar Agenda

1. Introductions
2. What is Cybersecurity?
   - Why is it important?
   - Cybersecurity Audit
   - Prepare for CMMC
3. Remediation
   - Importance of Managed Services
4. Funding Opportunities
5. Q&A

Funding Opportunities

- NYSEG/RGE/National Grind Manufacturing Accelerator Program (MAP) for Assessments and Remediation for NYSEG Manufacturing Customers
- FuzeHub / NY MEP Cyber Assessment Grant for Manufacturers that are new MEP Clients.
- Mohawk Valley Community College and FuzeHub's 2020 Cybersecurity Assistance Grant for DoD Tier 1 and Supply Chain


Q
A

Thank you for your interest!

For assistance or additional information, please contact:

5 South College Drive
Suite 104
Binghamton, NY 13905
607-774-0022
www.amt-mep.org

Jeff DuBrava
Business Development Manager
607.422.1048
jdubrava@amt-mep.org

Counties: Broome, Chemung, Chenango, Delaware, Schuyler, Steuben, Tioga, and Tompkins

445 Electronics Pkwy Suite 102
Liverpool, NY 13088
T: 315.425.5144
F: 315.233.1259
www.tdo.org

Mike Metzgar
Business Development Manager
(315) 425-5144 x 307
mmetzgar@tdo.org

Counties: Cayuga, Cortland, Madison, Onondaga, and Oswego

310 Broad Street
Utica, NY 13501
315.624.9800
www.aim-mep.org/

Paul LaPorte
Cyber Security Coordinator
315-624-9800
PLaPorte@mvcc.edu

Counties: Fulton, Herkimer, Montgomery, Oneida, Otsego, and Schoharie