

MEET YOUR PRESENTERS



Christina Wade, Area Vice-President

Born and raised in Lorain, Ohio, Christina has never met a stranger. As a member of the Lorain County Chamber of Commerce, she serves on the Membership Committee, extending a warm welcome to all new members. Additionally, she is an active member of Manufacturing Works Cleveland and Lorain County Manufacturing Sector Partnership engaging in networking activities and fostering connections within the community.



Leroy Ladyzhensky, Principal

Leroy is co- owner of Integrated Network Concepts, an IT services firm based in Avon Lake, Ohio. With two decades of leadership in a company established in 1991, he specializes in IT networking, security, and disaster recovery, helping organizations build resilient and secure technology infrastructures. Leroy combines technical depth with an approachable, executive presence, guiding clients through complex challenges while ensuring reliable business continuity. His longstanding commitment to IT excellence has supported the growth and stability of numerous businesses across the region.

Cybersecurity 101:

Understanding the Risks, Protect Your Data



Presented by Integrated Network Concepts
Avon Lake, OH



CYBERSECURITY IN THE NEWS

Jaguar Land Rover Sales Plunge Following Cyberattack

- THE WALL STREET JOURNAL, Oct. 7, 2025

Cyberattacks hit 91% of universities and 43% of businesses in last 12 months in the UK — survey suggests more than 600,000 businesses, 61,000 charities affected

- tom's HARDWARE, Oct. 6, 2025

Major local hospital network faces system-wide tech outage due to cybersecurity attack

- LOCAL 12 WKRC, May 20, 2025

5.4 million hit in major healthcare data breach — names, emails, SSNs and more exposed

- tom's guide, July 14, 2025

Almost 1 billion Salesforce records stolen, hacker group claims

- Reuters, Oct. 3, 2025

A Cyberattack on Jaguar Land Rover Is Causing a Supply Chain Disaster

- WIRED, Sept. 22, 2025

NEW
AT 10:00



CBS NEWS CHICAGO

36°

HEADLINES

MAN CHARGED WITH ATTEMPTED MURDER IN HALLOWEEN PARTY MASS SHOOTING C

Headlines: Is Cybersecurity really needed?

Small businesses being
targeted by hackers:



Quick Poll

Enter into the chat...

**On a scale of 1-10
how confident you
are in your current
cybersecurity
practices?**



Myths of Cybersecurity

Attacks are rare.

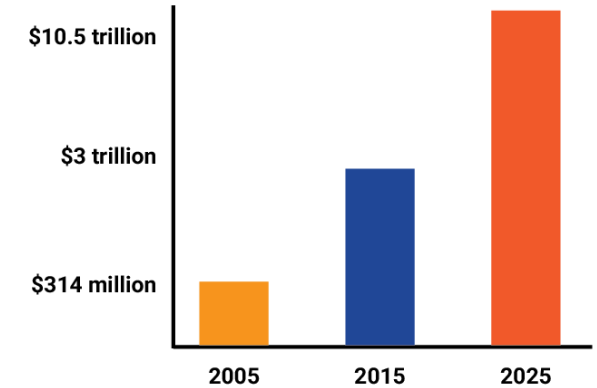
My business is small.

My business doesn't have time to prioritize cybersecurity.

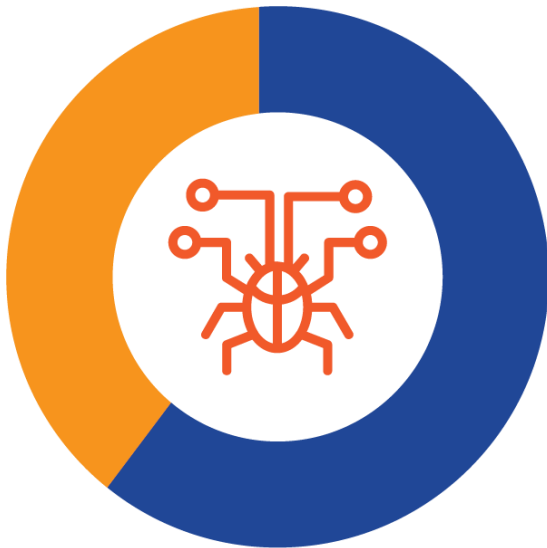
We don't collect sensitive information.

CYBERSECURITY IN NUMBERS

\$10.5 TRILLION *estimated global cost of cybercrime by 2025*



61%



**of small businesses
report at least one
cyberattack in the
past year**

43%



**of cyberattacks
target small &
medium sized
businesses**

Small Businesses in the U.S.

99.7% of US employer firms are small business

1 - 500 employees

49.2% of private sector employment

Have valuable information that cybercriminals can leverage, but often lack the security infrastructure to protect it



Quick Poll

Enter into the chat...

**Have you or someone
you know had a
business affected by
a cyber incident?**

Understanding the Risk

Cybersecurity Risk

Privacy Risk

Legal Risk

Understanding the Risk



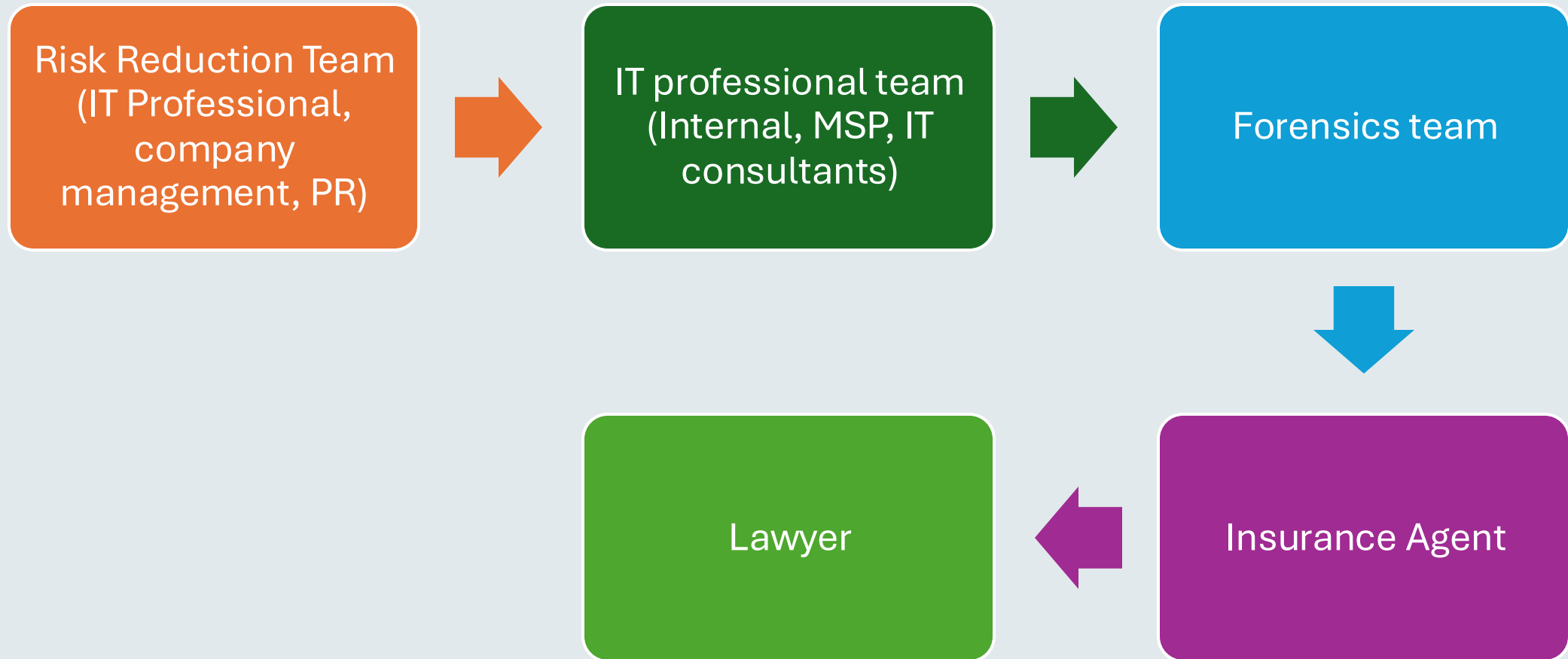
Financial Risk

Operational Risk

Reputational Risk

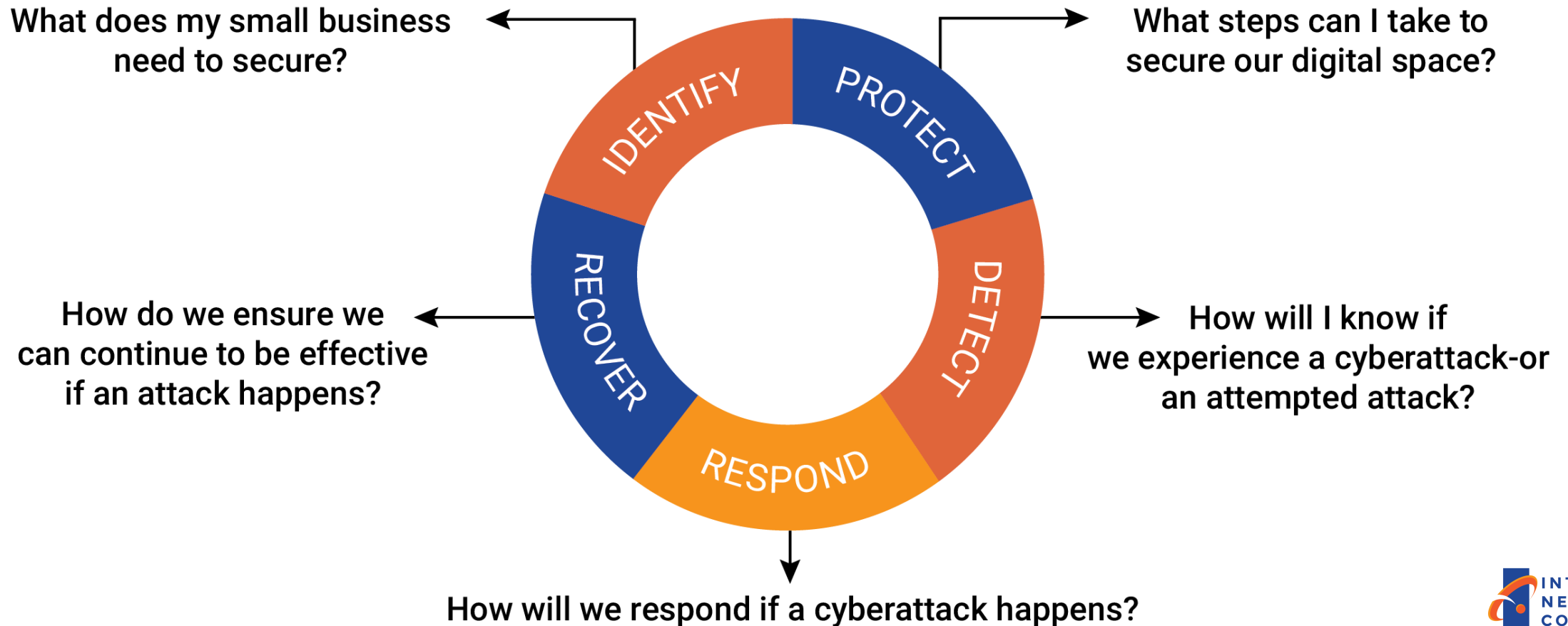
BUILD SUPPORT TEAM FOR PREVENTION

(order of engagement)



MANAGING RISK -Lifecycle for managing risk

National Institute of Standards and Technology recommends companies Identify, Protect, Detect, Respond and Recover



TYPES OF CYBER THREATS

Attacks happen in 2 ways - Systems OR People

Malware Threats

malicious software that is deliberately designed to cause damage to a computer, server, client or computer network. It can include viruses and ransomware.

Ability to spread from one computer to another

Locks victim out of computer or encrypts target data until ransom is paid





Email Threats

Phishing is a type of social engineering attack that uses email or malicious websites to infect machine.

Phishing emails appear as they are coming from a legitimate organization or known person

Often entice user to click on link or open attachment

**FBI Internet Crimes
Complaint Center released
an annual report in April of 2025**

**21,442 complaints of business email
compromise reporting over \$2 BILLION in losses.**



Quick Poll

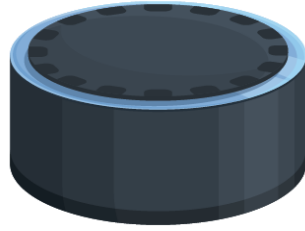
Enter into the chat...

**What is harder for
your team:
Creating strong
passwords or
remembering them?**

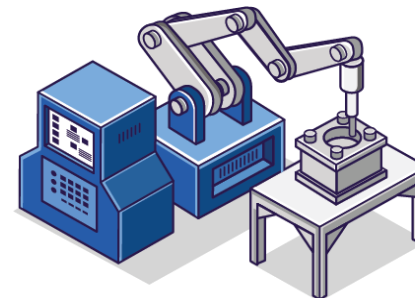
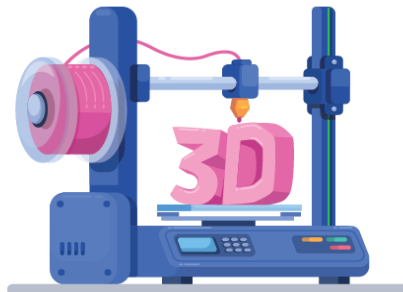
THE LAYERED APPROACH TO PROTECT SYSTEMS AND PEOPLE

- Firewall
- Segregated network
- Patch system
- Antivirus
- Employee training





ENTRY POINTS OF ATTACK





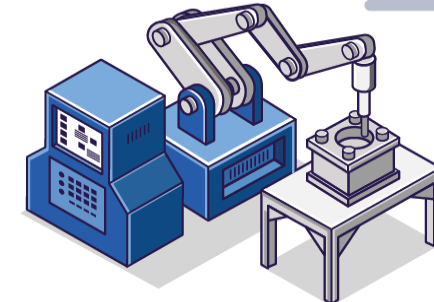
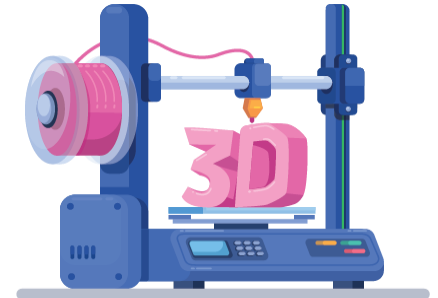
Quick Poll

Enter into the chat...

**Do you have
equipment that runs
on out-of-date
software?**

AGING EQUIPMENT, Modern Threats

- Runs outdated software
- Too costly to replace
- Limited or no security updates
- Vulnerable to cyber attacks
- Not compatible with modern backups
- **Solution:** Separate, secured network



VULNERABILITIES

- Poor password practices
- Clicking on malicious links in phishing emails
- Browsing unsafe websites
- Downloading malicious files
- Failure to take prescribed steps to protect sensitive data
- Failure to keep systems updated and patched



Quick Poll

Enter into the chat...

TRUE or FALSE

**I don't need back ups
because everything I do is
on the cloud or because
it's on Office 365.**

TRUE COST OF RANSOM ATTACK

Average Ransome typically **\$400,000**

Typical legal fees **\$100,000**

Typical Restoration fees **\$100,000**

Cost of Cybersecurity **PRICELESS!**
(fraction of the expense)

**Does not include downtime or damage to reputation*

RESPONSE PLAN

```
graph TD; A[RESPONSE PLAN] --- B[DETECTION AND INITIAL RESPONSE]; A --- C[ANALYSIS]; A --- D[RECOVERY]; A --- E[CONTAINMENT]; A --- F[ERADICATION];
```

**DETECTION AND
INITIAL RESPONSE**

ANALYSIS

RECOVERY

CONTAINMENT

ERADICATION

POST MORTEM AND PREVENTION

```
graph TD; A[POST MORTEM AND PREVENTION] -.- B[POST-INCIDENT ACTIVITIES]; A -.- C[CONTINUOUS MONITORING AND IMPROVEMENT]; A -.- D[LEGAL AND COMMUNICATION ACTIONS];
```

**POST-INCIDENT
ACTIVITIES**

**CONTINUOUS
MONITORING AND
IMPROVEMENT**

**LEGAL AND
COMMUNICATION
ACTIONS**

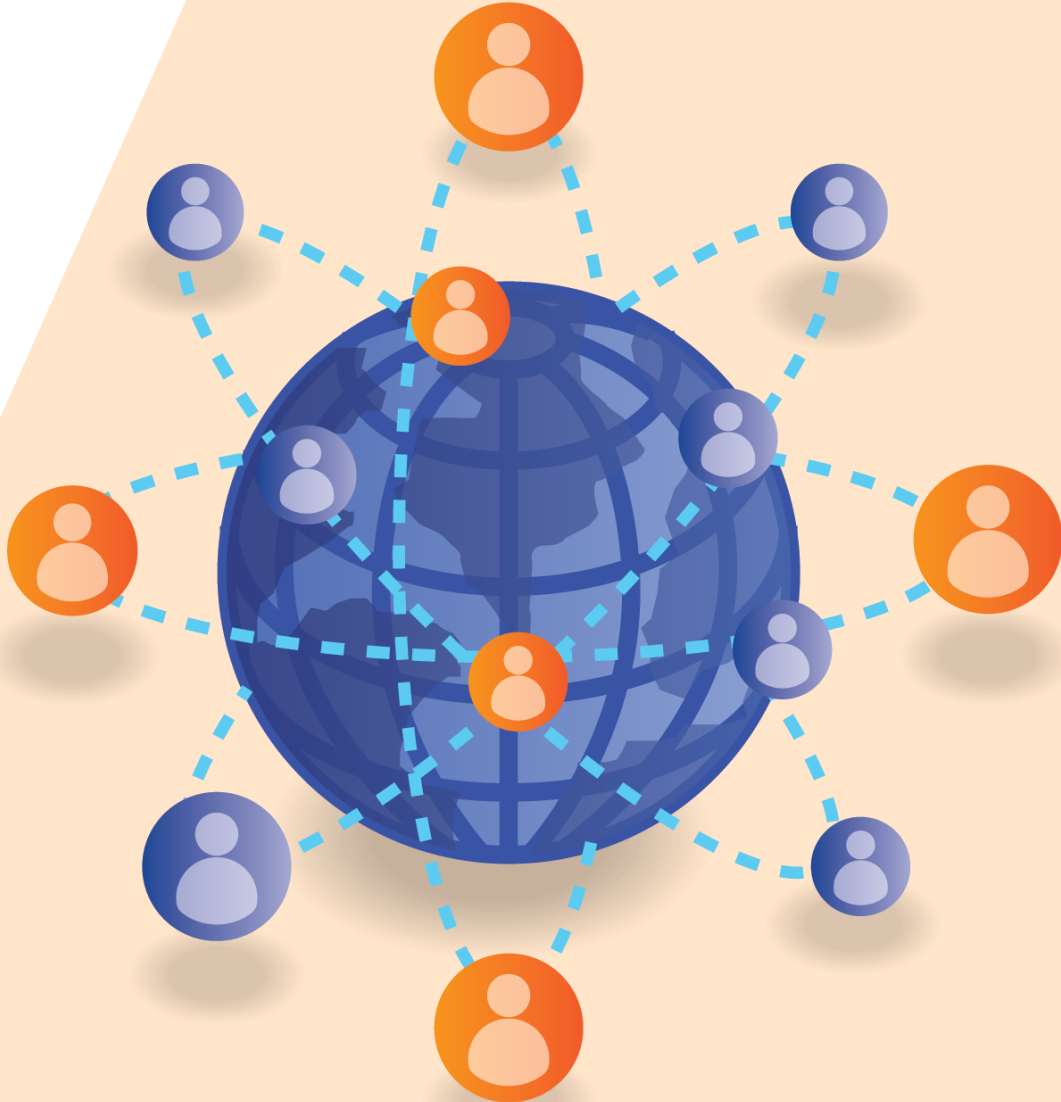


Quick Poll

Enter into the chat...

**If you lost access to
all company data for
48 hours, could you
still operate?**

BACKUP & RECOVERY: Your Safety Net



- Regular Backups
- Secure Storage
- Fast Restoration
- Business Continuity
- Tested & Verified

IDEAL BEST COMPANY PRACTICES

- 1 Regularly update or enable auto updates on both the operating system and applications that are installed on your computers and other devices to protect them from attack.
- 2 Know and understand all devices connected to your networks. This includes your Wi-Fi networks, cloud-based storage such as Dropbox or Google Drive, and local networks.
- 3 **Ensure all accounts are configured with multifactor authentication, where possible, including social media accounts.**
- 4 Deploy a border firewall* and endpoint firewalls* to protect your internal network from the internet and your endpoints from each other.
- 5 **Regularly back up critical systems and data, following the 3-2-1 rule. 3 versions of your data, 2 different media and 1 offsite**
- 6 Document information flows. It's important to not only understand what type of information your enterprise collects and uses but also to understand where the data is located and how it is used.
- 7 Deploy malicious code detection and prevention solutions such as antivirus or anti-malware software.
- 8 Develop an incident response and business continuity plan.
- 9 Use strong, unique passwords for every account. Don't share passwords. Require individual accounts for employees using computers and business applications.
For administrative functions, require a separate account that is not the person's everyday user account.
- 10 **Conduct cybersecurity awareness training for employees.**
- 11 Limit access to sensitive systems and data to only those personnel who absolutely need that access.
- 12 Use caution with email attachments and untrusted links and watch for suspicious activity on your accounts.

RESOURCES

■ **Center for Internet Security (CIS)**
CISecurity.org

■ **Federal Bureau of Investigation (FBI)**
FBI.gov/Investigate/Cyber

■ **Federal Trade Commission - Data Security**
FTC.gov/DataSecurity

■ **Homeland Security - Cybersecurity & Infrastructure Security Agency (CISA)**
CISA.gov

■ **Homeland Security - Stop. Think. Connect.**
DHS.gov/StopThinkConnect

■ **National Cybersecurity Alliance**
StaySafeOnline.org

■ **National Institute of Standards and Technology (NIST)**
NIST.gov

■ **Ohio Secretary of State Office of Public Integrity**
Ohio.Sos.gov/PublicIntegrity

■ **Small Business Administration (SBA)**
SBA.gov/ (search "Cybersecurity")

■ **Integrated Network Concepts (INC)**
Integrated.net

CLOSING THOUGHTS

Hope and Denial are not a strategy

Follow the 3-2-1 rule

3 versions of your data, 2 different media and 1 offsite

Put your instant response plan on paper!

QUESTIONS

Schedule a free consultation!

Scan the QR code
to schedule your **FREE** 1 hour
Cybersecurity Risk Assessment.
A \$500 value!

Each entry is also entered to win
\$100 Visa gift card!

