Business Continuity, Disaster Recovery & Cybersecurity for Small Businesses

Empowering Your Business to Thrive Securely

ATIS-USA, Inc.

Who Am I?

Your Presenter

Atanas Vasilev, Founder & CEO of ATIS-USA, Inc.

- Working with small and medium businesses for 20+ years
- Expert in IT Management, Cybersecurity, and Backup & Disaster Recovery
- Experienced in both prepared and unprepared scenarios
- Certifications: Cisco CCNA, PMP, PMI-ACP, ITIL, Lean Six Sigma Black Belt, AWS Certified Cloud Practitioner, Fortinet Certified Associate Cybersecurity, Fortinet FortiGate 7.4 Operator, VMware vSphere: Install, Configure, Manage plus Optimize and Scale Fast Track [V6.5], Databricks Generative AI Fundamentals, PMI Generative AI Overview for Project Managers

What ATIS-USA Does

Managed IT Services

Keep your systems running smoothly so you can focus on your business

Cybersecurity

Protect you from growing threats that target businesses of all sizes

Business Continuity & Disaster Recovery

Ensure you can get back up and running quickly when things go wrong

Serving businesses with 1-200 employees

What You'll Learn Today

- Understand the real threats your business faces—including modern cyber threats
- Learn practical cybersecurity basics you can implement this week
- Discover how AI is changing both threats and defenses
- Walk away with a clear action plan for backing up data, recovering from disasters, and keeping your business running

"Practical information you can use starting today—no overly technical jargon."

Everyday IT Disasters

Common Disasters That Can Shut You Down

Hardware Failures

- Hard drives crash
- Servers overheat
- Power surges damage equipment

Human Error

- Accidental file deletion
- Coffee spills on laptops
- Sensitive data sent to wrong people

Natural Disasters

- Floods
- Fires
- Storms destroying physical equipment

"If your only backup is under your desk, that's not really a backup."

Cyber Incidents: The Modern Disaster

Ransomware

Criminals encrypt all your files and demand payment to unlock them

- Over 60% of small businesses hit by ransomware couldn't fully recover

Phishing Attacks

Sophisticated emails designed to trick employees into giving away passwords or clicking malicious links

- No longer obvious scams—they look like your bank, vendor, or CEO

Account Takeovers

Criminals get into your email, banking portal, or cloud systems

- Can steal data, send fraudulent invoices, or lock you out entirely

"Cyber threats aren't just IT problems—they're business continuity disasters."

You Are a Target

Why Small Businesses Are Prime Targets

"We're too small to be a target. Hackers go after big corporations, not us."

This is a dangerous myth. Here's why criminals love small businesses:

- You have money and valuable data
- You're connected to banks, customers, and vendors
- You often have weaker security than larger companies
- Attacks are largely automated—criminals scan thousands of businesses looking for vulnerabilities

"Accept that you are a target, and act accordingly."

5 Simple Protections That Work

Basic protections stop most attacks

Strong, Unique Passwords

Use a password manager—not "password123" or your business name

Multi-Factor Authentication (MFA)

Even if someone steals your password, they can't log in without the second factor

Keep Software Updated

Those update notifications? They're patching security vulnerabilities. Set to automatic.

Secure Your Wi-Fi

Use WPA3 encryption, change default router password, separate guest network

Train Your Staff

Your employees are both your greatest vulnerability and strongest defense

"Cybersecurity isn't a one-time project—it's an ongoing practice."

The Mindset Shift

- Cybersecurity isn't a one-time project—it's an ongoing practice
- Like maintaining your building or managing your finances, security requires regular attention
- Perfect security doesn't exist, but good-enough security stops the vast majority of attacks
- Criminals are opportunistic—if you're harder to break into than the business next door, they'll move on

"Good-enough security stops most attacks."

What This Means for Small Businesses

AI Changes the Game—For Both Sides

AI-powered security tools are becoming more accessible and affordable for small businesses

You can now get enterprise-grade protection without enterprise budgets

The fundamentals still matter—AI doesn't replace good security hygiene

Strong passwords, MFA, backups, and staff training are more important than ever

AI is an accelerator: good fundamentals get better, weak fundamentals face worse threats

"The choice is yours: use AI to strengthen your defenses or become more vulnerable to AI-powered attacks."

How AI Helps Attackers

The Threat Landscape Is Evolving

AI-Generated Phishing

Emails written by AI are nearly perfect—no typos, no broken English, completely legitimate-looking

Deepfake Attacks

AI-generated voice and video calls that mimic executives requesting wire transfers

Automated Vulnerability Scanning

AI helps criminals find weaknesses faster and launch attacks at massive scale

"AI has made attacks more convincing than ever."

How AI Helps Defenders

AI-Powered Security Tools Are Getting Smarter

Faster Threat Detection

AI recognizes patterns humans would miss—like logins from two countries within minutes

Smarter Ransomware Detection

AI identifies abnormal file encryption and stops attacks before they spread

Intelligent Backups & Recovery

AI prioritizes critical data, optimizes storage, and predicts hardware failures

"The tools available to small businesses today are dramatically better—and many are affordable."

What This Means for You

The Bottom Line for Small Businesses

The Good News:

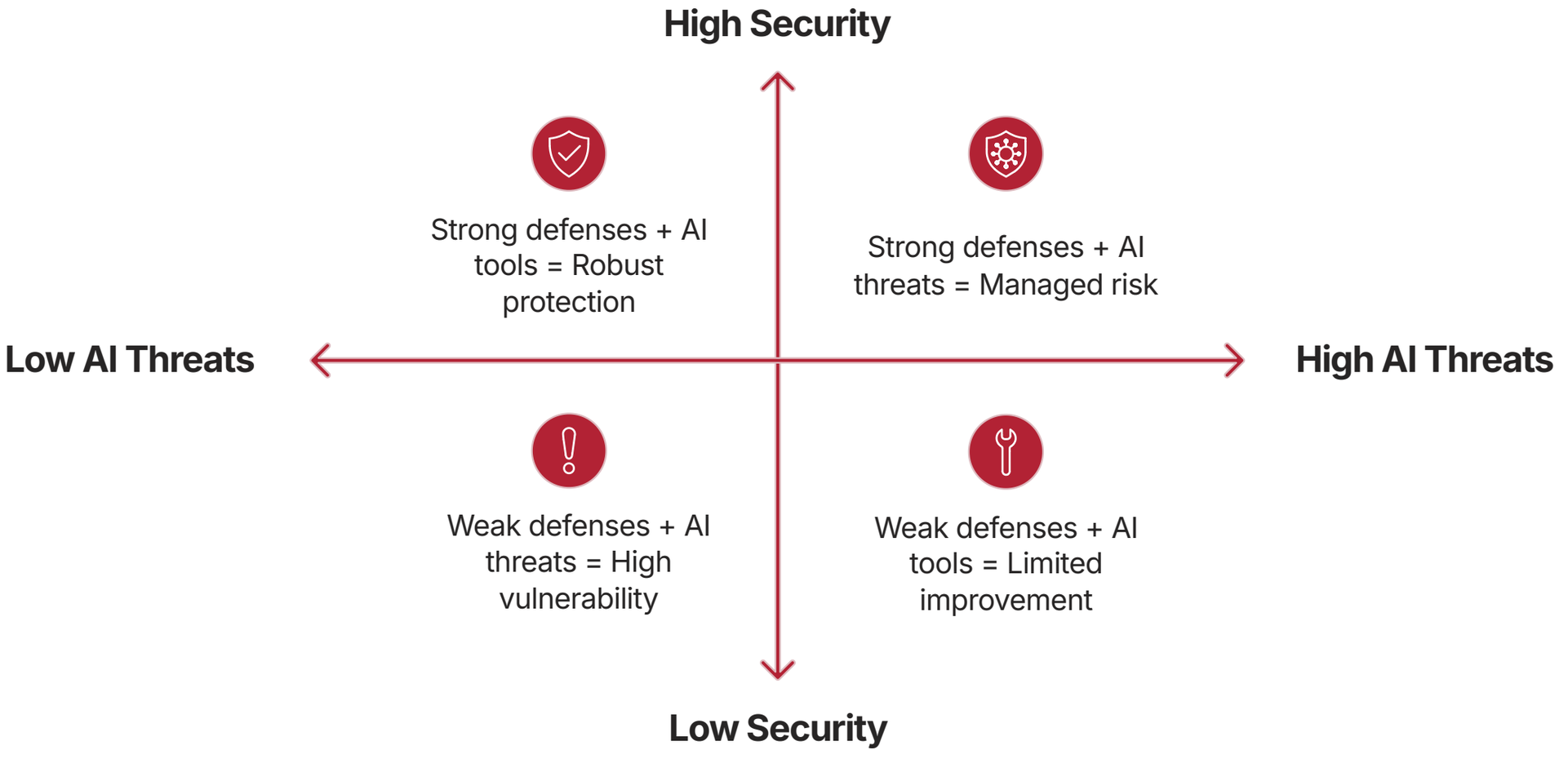
- AI-powered security tools are becoming more accessible and affordable
- You can now get enterprise-grade protection without enterprise budgets
- Modern tools are dramatically better than even three years ago

The Critical Point:

- Fundamentals still matter; AI doesn't replace good security hygiene
- You still need: strong passwords, MFA, backups, and staff training
- These basics are MORE important than ever as AI makes attacks more convincing

AI as an Accelerator

The Choice Is Yours



"If you have good fundamentals, AI tools make them better. If you have weak fundamentals, AI makes the threats against you worse. The choice is yours."

Plain-Language Definitions

Understanding the Basics

Backup

A copy of your data stored somewhere safe. Like photocopying important documents and storing copies off-site.

Disaster Recovery

The plan and process for getting your systems back online after something goes wrong.

Business Continuity

How your business keeps operating during and after a disaster. How do employees work? How do customers reach you?

"Backups are your safety net. Disaster recovery is your action plan. Business continuity is your survival strategy."

RTO and RPO Explained

Two Critical Concepts

RTO - Recovery Time Objective

The maximum acceptable downtime after a disruption. It dictates how quickly systems must be restored (e.g., minutes, hours, days).

RPO - Recovery Point Objective

The maximum acceptable data loss, measured in time. It determines how frequently data needs to be backed up (e.g., hourly, daily).

Example: Retail Store

RTO: 4 hours (point-of-sale system needed before afternoon rush)
RPO: 1 day (yesterday's sales can be manually recreated from receipts)

"Be realistic: Faster RTOs and tighter RPOs incur higher costs. Align these objectives with your actual business needs."

The 3-2-1 Backup Rule

Industry-Standard Best Practice

1

Three copies of your data

The original, plus two backups

2

Two different types of media

Combine media types (e.g., hard drive & cloud, or hard drive & tape)

3

One copy offsite

At least one backup stored physically offsite (e.g., cloud storage)

- **Copy 1:** Accounting data on your computer
- **Copy 2:** Nightly backup to local external hard drive
- **Copy 3:** Weekly sync to cloud storage (Dropbox, AWS) - this is offsite

Recovery scenarios:

- Computer dies → restore from external drive
- Office burns down → restore from cloud

Practical Backup Patterns

Solutions for Every Business Size

Micro Businesses (1-4 employees)

- External drives (affordable)
- Cloud services (e.g., Backblaze)
- Automated, monthly checks
- Simple, low-cost solution

Small Businesses (5-20 employees)

- Business-grade services
- Supports multiple devices & servers
- Includes versioning (ransomware protection)
- Robust protection

For Everyone

TEST YOUR BACKUPS

- Tested backups are essential
- Schedule recovery drills (bi-annually)
- Verify restore functionality
- Don't wait for disaster to test

"The best backup system is the one you'll actually use and maintain."

Written Disaster Recovery Plan

Your Emergency Playbook

This doesn't have to be a 50-page document. But it should answer these questions:

- Who is responsible for what?
- How do you access your backups?
- Step-by-step recovery procedures for each critical system.
- Vendor contacts, hosting provider's emergency number, and account details for all critical services.
- Communication templates for employees and customers during downtime.

Storage:

- Keep a printed copy off-site
- Keep a digital copy in the cloud
- Don't store your recovery plan only on the server that might die

"When disaster strikes at 2 AM on a Sunday, you'll want your hosting provider's emergency number handy, along with your account details."

Ransomware Attack: A Complete Example

How Everything Works Together

The Scenario - Monday Morning: Employee clicks a link in a phishing email, and ransomware starts encrypting files.

01

AI Detection (Minutes 0-2)

AI detects and isolates infection immediately.

02

MFA Protection

MFA prevents attackers from accessing cloud accounts.

03

Clean Backups Available

Clean local and cloud backups enable quick recovery.

04

Disaster Recovery Plan Executes

Documented plan guides immediate recovery actions.

05

Back in Business

Business restored within 4-hour RTO.

Without Preparation

- No AI detection → widespread network infection
- No MFA → compromised cloud accounts
- No recent backups → significant data loss
- No written plan → chaotic, slow recovery
- Result: Extended downtime, potential business failure

"Preparation is the difference between a minor incident and a business-ending disaster."

First-Hour Incident Response

Your Emergency Game Plan

When disaster strikes, follow these steps:

See It, Say It

Train everyone to report problems immediately. Early detection is everything.

Stop the Bleeding

Disconnect affected computers or move critical hardware to contain damage. The goal is to limit the spread of the incident.

Call Your Helpers

Utilize your written contact list to call IT providers, cybersecurity vendors, or your insurance company. Get experts involved promptly.

Switch to Plan B

Implement documented alternatives for critical operations. Ensure employees can access necessary files and work if primary systems are down.

Learn and Adjust

Conduct a post-mortem after the crisis to evaluate what worked and what didn't. Update your plan based on these valuable lessons.

"Train your team on this game plan. When stress hits, people fall back on training."

How Everything Connects

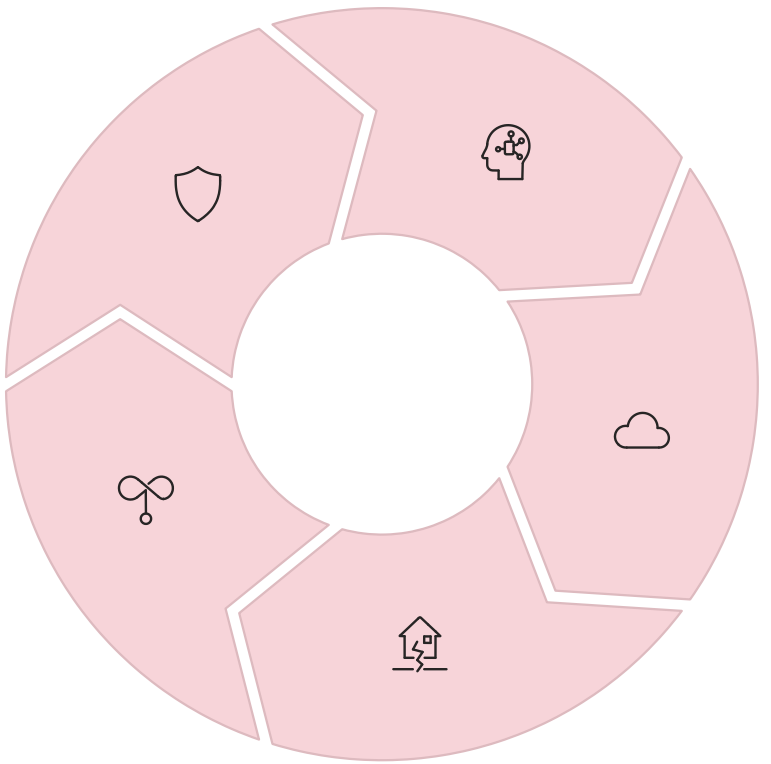
Your Integrated Defense System

Cybersecurity Basics

- Your first line of defense
- Reduce the chance of incidents

Business Continuity Planning

- Keep the lights on
- Serve customers and pay employees during recovery



AI-Powered Tools

- Faster detection and response
- Spot threats early, automate containment

Backups (3-2-1 Rule)

- Your insurance policy
- Recover when damage is done

Disaster Recovery Plan

- Your playbook
- Reduces panic, saves time, ensures nothing is forgotten

"None of these work in isolation. They're all part of one integrated system for resilience."

Real-World Success Story

Construction Company Ransomware Attack

The Client: Construction company (12 employees)

The Attack: Employee clicked link in fake invoice email. Ransomware attempted to encrypt files.

What Happened (Because They Were Prepared):

01

AI detected & quarantined ransomware.

02

Disaster Recovery (DR) plan activated.

03

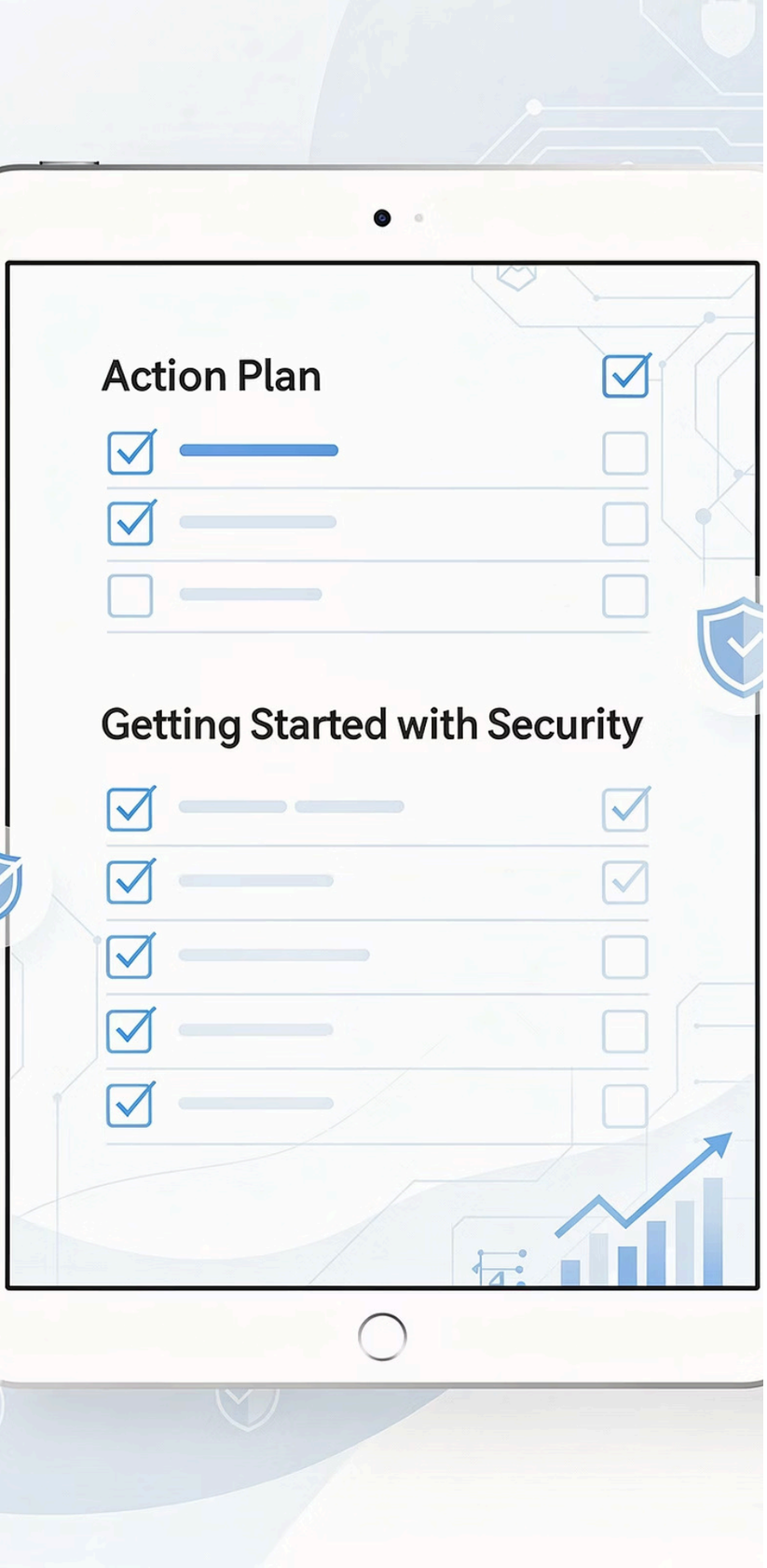
Files restored from clean morning backup.

The Results:

- Total downtime: 3 hours
- Total data lost: Zero
- Total ransom paid: Zero

> "We used to think backups and security were just expenses. Now we see them as the cheapest insurance we've ever bought."
>
> H.L. — Owner, Mid-sized Construction Firm

"That's the mindset I want you to walk away with today."



Your Next Steps Checklist

Action Items for This Week

Enable MFA on All Critical Accounts

Start with email and banking to block the majority of account takeover attacks.

Review Your Backup Situation

Ensure you know when your last backup was and if you can restore a file right now.

Test One Backup

Pick a random file and restore it to verify your backup process actually works.

Schedule a Team Conversation

Discuss phishing emails and suspicious activities with your team in your next staff meeting.

Write Down Emergency Contacts

Compile an accessible list of emergency contacts for IT, internet, cloud storage, and insurance.

Research IT Partners

Begin researching professional IT or cybersecurity partners if you don't already have one.

"Start small. Pick one thing and do it this week. Progress beats perfection."

ATIS-USA Can Help

Free Resilience Review

Free 30-Minute Resilience Review includes:

- Honest, no-obligation assessment of your backup & security.
- Identification of gaps and vulnerabilities.
- A prioritized action plan to gain clarity on next steps.

Resources Available:

- Downloadable worksheet & complete checklist
- 3-2-1 backup rule template
- Incident response steps & detailed guides
- Free risk assessment tools & case studies

Contact Information:

avasilev@atis-usa.com

202-621-4393

https://atis-usa.com/

"You don't need to do everything at once. Start small. Pick one thing from today's checklist and do it this week. Then pick another one next week."

Questions & Thank You

Time for your questions

- Technical questions
- Specific scenarios or challenges
- General inquiries

Key Takeaway:

The businesses that prepare are the ones that survive when things go wrong. And things will go wrong—it's not a question of if, but when.

Action Items:

- Take the checklist
- Schedule that resilience review
- Start this week

Your future self will thank you.

Contact Information:

Atanas Vasilev

avasilev@atis-usa.com

202-621-4393

ATIS-USA, Inc.

Thank you for your time today. Feel free to grab me afterward if you have individual questions.

Appendix: Handling Common Questions

Q: "How much should we budget for backups and cybersecurity?"

A: A good rule of thumb for small businesses is 3-5% of your total revenue for IT, with about a third of that going to security and backups. But it really depends on your industry and risk profile. In the resilience review, we can give you a more specific number.

Q: "Should we pay the ransom if we get hit?"

A: The FBI recommends not paying, and I agree. Paying doesn't guarantee you'll get your data back, it funds criminal operations, and it marks you as a business that pays—so you'll get targeted again. That said, if you have good backups, paying shouldn't even be on the table because you can just restore.

Q: "Is cloud storage safe for sensitive data?"

A: Yes, if you choose reputable providers and encrypt data before uploading. Major cloud providers like AWS, Microsoft Azure, and Google Cloud have security that far exceeds what most small businesses can implement on their own. The weak link is usually user credentials—which is why MFA is so important.

Q: "How often should we update our disaster recovery plan?"

A: Review it every six months and update it whenever something major changes—new software, new employees, new vendors, new office location. Also update it after any incident, even a minor one, to incorporate lessons learned.

Q: "What if we can't afford enterprise-grade security tools?"

A: Start with the free and low-cost basics: strong passwords, MFA, Windows Defender or built-in Mac security, automatic updates, and staff training. Those cost almost nothing and stop most attacks. As you grow, invest in better tools. But don't let perfect be the enemy of good.