Cybersecurity Preparedness: Disaster Recovery Best Practices

Scott Cave, CBCP
Atlantic Business Continuity Services
Myths:

- Size
- Industry
- Duration
Cybersecurity Issues

• Phishing Attacks
• Spearphishing Attacks
• Ransomware
• Internal Sabotage
• External Hacking
• Trade Secrets
• Personally Identifiable Information
• Financial Data
5 Planning Tips for Businesses

• Strong Password Management
• Proactive User Training
• Cloud Diligence
• Tactical Planning
• Response and Recovery Plan
#1 Passwords: 1st Line of Defense

- Policy – in writing and automated
  - Length: at least 12 characters
  - Strength: UPPER, lower, numbers, special
  - Expiration: no more than 90 days
  - Factors: TWO (for all systems, especially cloud)
  - Sharing: NONE (unique password per user per acct)
  - Management Tool: YES (secure storage and access)
  - Lock-outs for consecutive unsuccessful attempts
Users: the Weakest Link

• Everyone has a responsibility for Cybersecurity
• They need continual training to learn, understand, and practice these responsibilities:
  – Policies, then training
  – Phishing
  – Ransomware
  – Data Security
  – Email safe usage
  – Social media usage
  – Passwords
  – Devices
Cloud: Tread Carefully

- Due Diligence before signing up
  - SLA
  - Data, Data, Data
  - Who owns it, who retains it, for how long, and where?
- Watch out for free services – no critical or sensitive data
- Pay for higher tier with additional features:
  - User roles
  - Encryption
  - Backup
- Look for optional add-ons for extra security:
  - e.g. Office 365 with Advanced Threat Protection
  - Two-factor authentication
#4 Tactics: Planning your Defense

• Proactive mindset that requires continual effort
  – Outsource if necessary

• Develop layered security approach:
  – All devices (Bring Your Own Device)
  – Privileges (Least Privileged Access, remove local administrative rights)
  – Servers (on-premises, hosted/cloud)
  – Applications (patches, updates)
  – Network (firewall, content filter, DNS watch list, etc)
  – Storage (encryption)
  – Website (encrypted and protected)
  – Back-ups vs. sync (multiple copies, multiple locations, and testing)

• Monitor:
  – Identify logs and review them regularly
  – Automate

• Adjust as you read, learn, and experience issues
#5  Response Plan: If all else Fails

- Disaster Recovery Plan for IT Systems
- Data Breach Response Plan:
  - Detection
  - Notification
  - Remedy
  - Documentation
  - Crisis Management
  - Root Cause Analysis
  - Adjustments to prevent future recurrences
Business Continuity Elements

Crisis Mgmt
- Emergency Action Plan (OSHA)
- Communications

Technology
- IT Systems, Data, Phones
- Utilities (power, internet, voice)

Continuity
- Operational Continuity, Customers, Vendors
- Facilities, Financial, Assets, Vital Records
Recent Lessons Learned

- Integrating plans with County OPCONs
- Re-entry procedures
- Proactive communications
- Advance team for evacuation – early reservations
- Flexibility in plans and schedules
- Well-trained and redundant staff
Procrastination is a problem when it comes to doing my disaster plan. As a business owner I have a lot to do. It’s not like a disaster is going to happen tomorrow. Besides, we have that new business pitch. I’ve been waiting for this to happen for a while now. I’ll get the disaster plan finished eventually. Nothing to worry about, it’ll happen.

Whether natural or man-made, at least one in four businesses affected by a disaster never reopen. Though emergencies are unpredictable, when you have a plan in place you can adapt, recover and stay in control.

*It’s never too late to protect your business until it is.*

Make a plan.

READY.GOV
Questions?

Scott Cave, CBCP
Atlantic Business Continuity Services
(843) 879-5025
scave@atlanticprep.com
www.AtlanticPrep.com