



CyberSecurity Webcademy:
Being Prepared for an Incident

Presenters



Justin Krentz – Account
Executive in Pennsylvania



Tyler Lewan – Account
Executive in Colorado

Agenda



Summary of previous sessions



Being Prepared for an Incident



What's next?

Summary of Session #1: The Basics

- Security Assessment**
- Staff**
- Spam Email**
- Passwords**



Summary of Session #2: Securing Your Environment

- ✓ **Computer Updates**
- ✓ **Log Management**
- ✓ **Firewalls**
- ✓ **Encryption**



Summary of Session #3: Make it Hard for Cyber Criminals to Get In

- Advanced Endpoint Detection**
- Multi-Factor Authentication**
- Web Gateway Security**
- Dark Web Research**

Risk #1: Whoa, Back Up

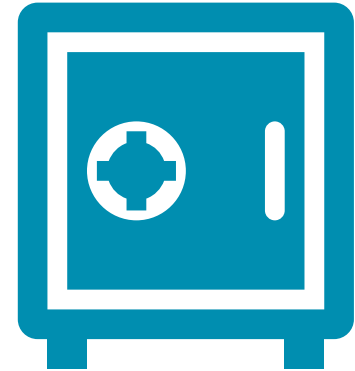


Back Up/Disaster Recovery Procedures

- Most processes are executed inconsistently
- No policies or plans in place for a restore or disaster scenario
- You can't predict when data loss will happen

Prevention #1: Comprehensive Backup plan

- Backup local and to the cloud
- Have an offline backup for each month of the year
- Disaster Recovery testing, planning and updates
- Test your backups often!



Advantages #1: Back Up

- Without backups, natural disasters could put you out of business
- Your business has the right solutions to recover its critical data
- Recovery Time expectations
- Lost data hurts your brand's reputation



Risk #2: Going Down, Down, Down



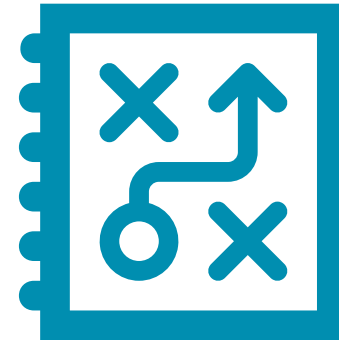
Source: Cisco 2020 Benchmark Report

- Data breach can happen when you least expect it
- Wasting time and energy deciding what to do
- Only as good as your processes and practices
- Can't maintain continuity in an emergency

Prevention #2: Response Plan

A detailed set of instructions to follow in the event of a security breach

- Enable your team to analyze the breach
- Determine what went wrong
- Limit the damage
- Make whatever improvements to prevent similar events from occurring



Advantages #2 - Response Plan

- Can limit downtime
- Team members have steps to follow
- Secure the situation and get the company back on track



Risk #3: Your Biggest Risk



- Combat cybercriminals by investing on technology, not the human side
- Employees are first line of defense
- Thinking cybersecurity is IT's responsibility
- Pushing policies without proper explanation

Prevention #3: CyberSecurity Culture (CSC)

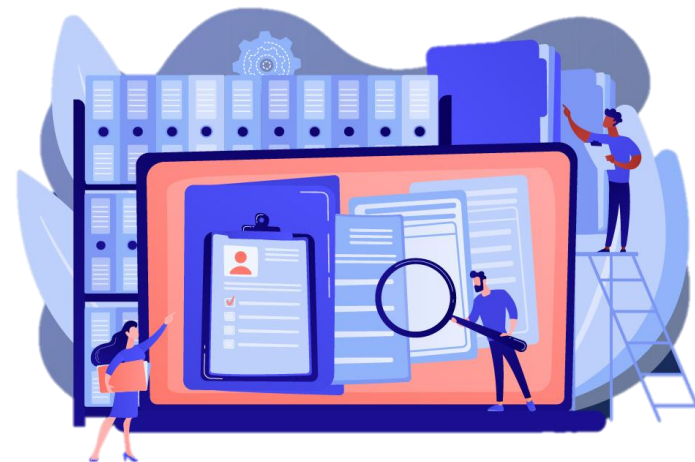
- Explaining and raising awareness about cyber risks and implications
- Enforcing procedures that will assimilate easily with daily work routines and practices
- Showing how behavior can help or hinder the entire organization's structure



Advantages #3: Promoting CSC

Transition from a fragmented approach to a
Cybersecurity Culture

- Don't skip the basics
- Continually educate and inform
- Measure the effectiveness of your CSC and adjust accordingly
- Reward/ recognize/ celebrate successes



Prevention #4: Cyber Insurance

Hard Costs

1. Liability – 1st, 3rd, Multimedia

2. Fines and Penalties

3. Crisis Management Services

4. Data Replacement and Recovery

Soft Costs

5. Business/Dependent Interruption

6. Reputational Damage

7. Crime Coverages

8. Newer Coverages

Your Graduation Gift!



16 Ways to Protect Your Business From a Cyber Attack!

 Security Assessment It's important to establish a baseline and close existing vulnerabilities. When was your last assessment?	 Security Awareness Train your users- often! Teach them about data security, email attacks, and your policies and procedures.	 Spam Email Secure your email. Most attacks originate in your email. We'll help you choose a service designed to reduce spam and your exposure to attacks.
 Passwords Apply security policies on your network. Examples: Deny or limit USB file storage access, enable enhanced password policies, or set user screen timeouts.	 Computer Updates Keep Microsoft products updated for better security. Look for a "critical update" service via automation to protect from attacks.	 Log Management SEIM, Security Incident & Event Management uses big data engines to review all event and security logs from all covered devices.
 Firewall Turn on intrusion detection and intrusion prevention features. Send the log files to a managed SIEM.	 Encryption Whenever possible, the goal is to encrypt files at rest, in motion, and especially on laptops.	 Advanced Endpoint Detection Protects your computers data from malware, viruses, and cyber attacks through file-less and script-based threats.
 Multi-Factor Authentication Adds an additional layer of protection to ensure that even if your password does get stolen, your data stays protected.	 Web Gateway Security Internet security is a race against time. Cloud based security detects web and email threats as they emerge and blocks them on your network within seconds.	 Dark Web Research Knowing in real-time what passwords and accounts have been posted on the Dark Web will allow you to be proactive in preventing a data breach.
 Security Expertise Work with IT professionals who understand the framework for managing today's security requirements.	 Backup Backup local and to the cloud. Have an offline backup for each month of the year. Test your backups often.	 Response Plan Having a well-prepared incident response plan to follow ensures that can limit downtime.
 Cyber Insurance if all else fails protect your practice with cyber damage and recovery policies.		

National Cybersecurity Awareness Month

Observed every October

- Week 1: If You Connect It, Protect It
- Week 2: Securing Devices at Home and Work
- Week 3: Securing Internet-Connected Devices in Healthcare
- Week 4: The Future of Connected Devices

staysafeonline.org

Thank you!

Justin Krentz:

Jkrentz@verticalsol.com

724-493-0933

Tyler Lewan:

tlewan@verticalsol.com

847-987-9606



Vertical  **Solutions**
an R.L. Nelson & Associates Company