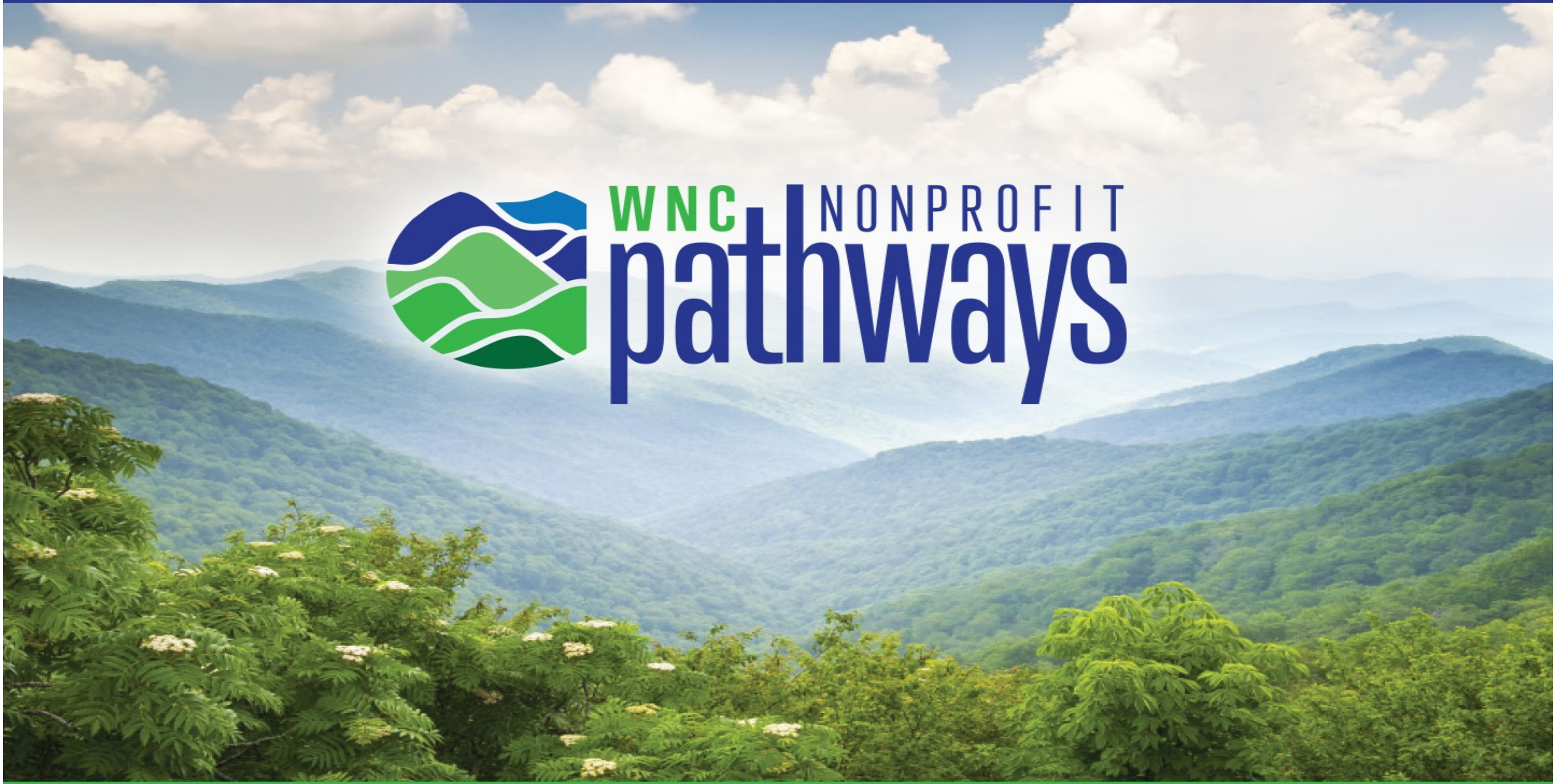

WNC NONPROFIT pathways

strengthening the organizations that help our communities succeed

Cybersecurity Training for Nonprofit Organizations

Today’s threat environment

Gordon Walton, President
Matthew Horton, Director of Technology
Alan Schwartz, Senior Systems Engineer

OneWhoServes, Inc.
Business Technology Services

OneWhoServes Inc.
business technology services

Who are we?

- OneWhoServes, Inc. was founded in April 2000
- All Systems Engineers are highly experienced (min 16 years), and HIPAA certified
- OWS team provides

  - Outsourced IT services to hundreds of SMBs

  - Comprehensive service, or support your IT staff

  - Server and cloud-based services and consulting

  - Data protection, business continuity, cybersecurity

  - Technology tuned to your needs in your language
- We support dozens of local nonprofits
- Presenters: Gordon Walton, President; Matthew Horton, Director of Technology; Alan Schwartz, Senior Systems Engineer

OneWhoServes Inc.
business technology services

The risk: high threat environment

- Cyber crime is growing at a tremendous rate: 31% of organizations report attacks
- 43% of cyber attacks target small business
- 95% of cybersecurity breaches are due to human error or action
- Most companies take nearly 6 months to detect a data breach
- FBI: 10-12% of cyber crimes are reported
- We deal regularly with client questions, adjustments, and remediation

OneWhoServes Inc.
business technology services

Why my organization?

- Tendency to think we are small, unimportant, under the radar…
- “Our info doesn’t have a lot of value”
- We don’t have a lot of money
- Target focus has shifted to small business & elderly – less knowledge, resources
- Perhaps not after your data, but your contacts and connections
- Your infrastructure may be the access point to another infrastructure

OneWhoServes Inc.
business technology services

The consequences

- Unauthorized access to business & confidential data
- Exposure of private data: clients, donors, patients
- Loss of business and revenue
- Loss of access to business files and data
- Theft of passwords and credentials
- Monetary losses by theft from accounts or by following fraudulent instructions
- Identity theft
- Damage to reputation

Cybersecurity threats 1

- Malware – malicious software on computers, most commonly delivered by email
  - persistent threat for many years, many forms
  - some with immediate impact, others lay low
  - viruses, worms, trojans with many functions
  - adware pushes unwanted, malicious advertising
  - spyware reports activity, keystrokes, passwords
- Ransomware – must pay to get access to files
  - encrypts all user files to make them inaccessible
  - can act on all mapped drives & attached storage
  - requires payment in Bitcoin to get encryption key

OneWhoServes Inc.
business technology services

Cybersecurity threats 2

- Phishing – attempts to get users to click malware
  - generally delivered by mass email
  - entices user to click, unleashes malicious payload
  - once activated, computer/network is compromised
- Spear Phishing – personally targeted phishing
  - perpetrator collects personal/relationship info
  - uses info to target user with crafted message
  - higher probability of success, appears legitimate
  - requests for money, data, personal info
- Whale phishing – targets principals and upper management
- Social engineering / phone calls – to get info
  - convinces target that request is legitimate

OneWhoServes Inc.
business technology services

Cybersecurity threats 3

- Advanced Persistent Threats (APT) – monitoring for an extended period

  - spyware or account/email access to harvest info
- Brute force password attacks – to gain access to organizational resources

  - password cracking is highly sophisticated

  - entire system entered by weakest link (password)
- Cryptojacking – your resources are used to mine for cryptocurrency, impacts performance and electricity
- Distributed Denial of Service (DDoS) – overwhelms network resources to make them unavailable for legitimate use (e.g. online ordering, access to Internet)
- Internet of Things (IoT) – provides points of malicious entry

OneWhoServes Inc.
business technology services

Technical safeguards and training combined

- Cybersecurity is not fundamentally a technical problem, it is a people problem
- Technical safeguards are important as 1st defense, but not flawless, and easily defeated by user action
- #1 source of breaches is people: biggest challenge is making sure an employee doesn't click wrong button
- User training is critical to cybersecurity protection
- Must recognize risks and respond appropriately
- Some threats are internal – errors, grudges, theft
- Create a culture of cybersecurity – it is a practice, not a set-and-forget project

OneWhoServes Inc.
business technology services

Cybersecurity Training

Technical safeguards – functions and limitations

Matthew Horton, Director of Technology

OneWhoServes, Inc.
Business Technology Services

OneWhoServes Inc.
business technology services

What are technical safeguards?

- Hardware, software, or services designed to defend against, or mitigate the damage from cyber threats
- Examples:

  - antivirus software
  - firewalls
  - spam and web filters
  - backup and recovery systems
  - monitoring and management systems

Home vs. business class safeguards

- Businesses have a different, unique set of challenges and needs than home networks
- Hardware / software vendors have distinct product lines for each market with important differences
- "Off the shelf" home products from local retailers, even ones marketed as premium products, are not suitable for business use
- You get what you pay for, you don't get what you don't pay for

Endpoint security

- Includes antivirus and antimalware software
- Two major types: definition-based, cloud-based
- Wide variation between product costs, capabilities, and required resources
- Product effectiveness changes over time – long term vendor contracts are not recommended

Gateway security

- Includes firewalls, gateway antivirus, spam filters, web filters, and DNS filtering
- A good firewall is essential – blocks unauthorized access from outside
- Gateway antivirus, web filtering, and spam filters stop threats before they reach the user
- Web filters are a good idea in general
- Effective spam filtering is required in today’s threat environment

Internal access controls

- Determine "Who gets access to what?"
- Implement group / file permissions on shared data
- Network segmentation – internal firewalls

  - isolate guest networks from business network

  - isolate systems such as smart TVs, cameras, and other IoT devices from sensitive data
- Perform audits of access to resources to find unused accounts or odd access patterns
- Defends against both internal and external malicious actors

OneWhoServes Inc.
business technology services

Wireless security

- Wireless networks extend your network beyond the four walls of your building
- Guest / visitor wireless networks should always be separated
- Internal network controls: RADIUS or certificate-based authentication is preferable to passwords
- Protect wireless networks with the strongest encryption standard available

Mobile devices – tablets and smartphones

- Consider carefully whether use of personal devices is allowed on organizational network (BYOD)
- Have a BYOD policy in place – defines device requirements, security, data management, exit plan
- Consider Mobile Device Management (MDM) software
- Mobile devices get viruses too!
- Must have remote wipe capability for sensitive data
- Personal devices should ONLY join isolated guest wireless networks

OneWhoServes Inc.
business technology services

Remote access and VPNs

- Remote access must be carefully considered
- Protect access using Multifactor Authentication
- Geo-blocking limits connections from world regions
- Connection auditing monitors unauthorized access
- Terminal servers should never be directly exposed to the Internet – use a Remote Desktop gateway
- Always use the strongest encryption standard for VPNs

OneWhoServes Inc.
business technology services

Patching

- Installing Operating System and software updates is critical – hackers utilize discovered vulnerabilities to gain unauthorized access
- Operating Systems – servers and workstations
- Update firmware for network devices – switches, routers, firewalls, access points
- IoT devices are typically NOT patched and are prime targets to gain access to networks
- A Remote Monitoring and Management (RMM) solution can help with patch management

Backups

- Key consideration when choosing backup method: “How long can we afford to be down?”
- Good backups store multiple file versions and use a media rotation schedule
- Backups must be offline and offsite to protect against natural disasters and ransomware
- Report monitoring and periodic testing of backup integrity are essential

Backups of cloud data (Office 365, G Suite, etc.)

- Check your contracts: cloud providers often shift backup responsibilities to the client
- Cloud provider backup policies protect their interests, not yours
- Ransomware can extend to cloud connections, so backups of that data are essential
- User error and accidental deletions are far more common than you think

OneWhoServes Inc.
business technology services

Limitations of technical safeguards

- Technical safeguards are NOT 100% effective!

  - hardware and software are made by people

  - encryption protocols are broken over time, exploits are discovered and used

  - some threats aim to bypass technical safeguards by focusing on the human element

- Implementation is often limited by budget, safety vs. convenience, and technical resources available

Cybersecurity Training

Cybersecurity as a practice

Alan Schwartz, Senior Systems Engineer

OneWhoServes, Inc.
Business Technology Services

OneWhoServes Inc.
business technology services

Cybersecurity as a practice

- Password practices and password management
- Email and data encryption
- Multifactor Authentication (MFA, 2FA)
- Network and Active Directory management (staff access)
- Remote Monitoring and Management for servers and workstations (RMM)
- Cybersecurity training and testing
- Network penetration testing
- Business Continuity and Disaster Recovery planning
- HIPAA and other regulatory compliance

OneWhoServes Inc.
business technology services

Password policies and password management

- Research shows that longer passwords are more secure than complex passwords
- Consider using a passphrase
- Use a pin or password on your phone and tablet
- Password management tools help keep passwords in a secure, centralized location
  - these tools can allow you to securely share accounts and passwords with others
  - software can create unique, long, random passwords for each site
  - add-ins will allow Web browsers to autofill passwords so sites will automatically login
  - works across multiple devices
- https://haveibeenpwned.com/ - check to see if your email address has been included in a breach

OneWhoServes Inc.
business technology services

Email and data encryption

- Most email systems have the ability to send encrypted email
- Passwords, financial information, PHI/PII and other confidential/proprietary business information sent outside your organization must use encrypted email
- Consider disk drive encryption if storing any of this information on a computer to protect your data if the computer is lost or stolen
- Encrypt your phone or tablet if it stores protected information

Multifactor Authentication/2 Factor Authentication (MFA/2FA)

- MFA uses two different credentials to log into accounts
- Usually combination of something you know (password) and something you have (code/app on your phone)
- Weak or stolen passwords are used in 95% of all attacks
- Gives an additional layer of security - if your password is supplied, no one can get in without your action
- Easy to use but you must have your phone/tablet
- Use for remote access, password management tools, banking sites, email, social media, and anything else that should be secure

OneWhoServes Inc.
business technology services

Network and Active Directory management (staff access)

- Users should be given the least privileged access required to perform their duties
- User accounts for former employees should be disabled in a timely manner
- Usernames and passwords should never be shared
- Each employee should have a named account (not use a generic account) so that actions are auditable
- Occasional user and file / folder access audits are recommended

Cybersecurity training and testing

- A security breach is often expensive and detrimental for business
- Users are the largest risk to your systems
- Threats include: spam, phishing, spear phishing, malware, ransomware, and social engineering
- An organization can have the best hardware, software, and IT team and still be vulnerable to a breach
- Quarterly training and testing are strongly recommended
- Targeted training for Executives, HR, Finance, IT, and healthcare are recommended
- Companies without security awareness training for employees suffered 300% higher financial losses due to cyber crime

OneWhoServes Inc.
business technology services

Network penetration testing

- Pentest is simulated cyber attacks against your technology system to discover exploitable vulnerabilities
- External penetration tests target the assets of an organization that are visible on the Internet
- Internal penetration tests are done within local network to simulate an attack by a malicious insider

  - can determine vulnerability due to compromised employee credentials resulting from phishing attack

  - does not necessarily simulate a rogue employee

OneWhoServes Inc.
business technology services

Business Continuity and Disaster Recovery planning

- Business continuity plan (BCP) defines procedures and processes in the event that the organization experiences a disruption

  - specifies all necessary steps and timeframes to get resources, processes, and functions up and running again

  - defines plan for interim operation during full recovery process

- Disaster recovery plan (DRP) defines process to recover organizational IT infrastructure in case of a disaster

  - disaster could be due to natural or man-made causes

  - IT environment often suffers severe disruptions, which can result in data loss or loss of ability to perform mission

- BCP and DRP are important to meet regulatory requirements

HIPAA, PCI, and SOX compliance

- Regulatory requirements drive IT security standards & configurations
- Most have common themes but there are notable differences
- Specific IT planning and infrastructure are important for compliance
- Physical, network, & process security measures required to safeguard protected health information (PHI) and ensure HIPAA compliance
- Covered Entities (providing healthcare treatment, payment, and operations) and Business Associates (anyone who has access to patient information and provides support in treatment, payment, or operations) must meet HIPAA compliance requirements
- Other entities such as subcontractors and any other related business associates must also be in compliance

Conclusion

- Threat environment is severe and getting worse
- Breaches are occurring frequently at large and small organizations
- IT technical safeguards must be kept up to date
- Staff training will significantly reduce risk
- Automated RMM software agents proactively manage network with 24/7 monitoring
- Don’t take your IT for granted, don’t set-and-forget – it must be actively managed!

Questions?

OneWhoServes, Inc.
Business Technology Services
828-251-1111
info@onewhoserves.com
www.OneWhoServes.com

(We will be happy to answer questions for attendees at any time – just call or email.)

OneWhoServes Inc.
business technology services

Other tools you may find helpful

- TechSoup – Provides special pricing on hardware & software to nonprofits
- Microsoft – Office 365 Nonprofit Business Essentials free to nonprofits
- Google – G Suite for Nonprofits provides free G Suite Basic using your domain
- Canva – Create high quality visual content for Print or social media
- Google AdWords - Ad Grants provides access to $10,000 USD of in-kind advertising every month for text ads
- Dreamhost - Free shared web hosting for all US-based registered nonprofits
- MailChimp – Email marketing free for less than 2000 email subscribers
- Asana – Task management tool free for up to 15 users
- Amazon Smile – Nonprofits can register for donations based on sales
- Capterra.com – Excellent resource for helping with software selection
- https://haveibeenpwned.com/ - check to see if your email address has been included in a breach

OneWhoServes Inc.
business technology services

The presenters

Gordon Walton, President

Gordon founded OneWhoServes, Inc. in April 2000. He earned his bachelor's degree and master's degree in electrical engineering and has worked in the computer industry since 1978. He has designed computers, written software, designed and built special purpose systems for unique applications, and served as the one-man Information Technology department at a large nonprofit. He has held positions in design engineering, customer service, sales, and management in hardware and software companies in corporate, nonprofit, and government environments. Gordon has given presentations on technology topics at the local Association of Fundraising Professionals Summer Philanthropy Institute and has presented full-day technology training sessions for the Duke University Nonprofit Management Program. He has served for 6 years on the Homeward Bound board and 6 years on the Helpmate board.

Matthew Horton, Director of Technology

Matthew provides server- and cloud-based IT services and consulting to clients. He is an expert in system architecture, technologies suitable for SMBs, data backup and business continuity, HIPAA compliance, and cybersecurity. Matthew has been working with computer hardware and software since he was twelve and has been studying computer networking since he was fourteen. He enjoys problem solving and the creative process that's involved with building solutions and resolving complex issues. He joined OWS in 2007 and holds MCSE, CCNA, A+, CAN, and Cisco certifications.

Alan Schwartz, Senior Systems Engineer

Alan joined OneWhoServes in July of 2019 after managing the IT Department for a local healthcare software vendor. He is a well-rounded IT professional with 20 years of experience from server to tablet, network to cloud, and every environment in between. Alan is highly skilled in infrastructure planning and implementation, project management, bringing technical understanding to non-technical users, and mentoring of IT support teams, with specializations in healthcare and HIPAA regulations and compliance, legal practices, and cybersecurity. He enjoys resolving client issues and working with clients of all sizes to enhance their IT systems so they work better for their businesses.

OneWhoServes Inc.
business technology services