A practical guide to cybersecurity

Ryan Peasley, MCSE
Senior Manager

Cybersecurity landscape

Increased cybersecurity threats since COVID and creating a remote workforce

- **Rapid Technology Adoption** – Microsoft reports 70% growth in Microsoft 365 usage since onset of COVID-19. Now 75 million daily active users, up from 44 million in March.
- **Opportunistic Cyber Criminals** - Email Phishing attacks increased 667% since the start of COVID-19.
- **Credential Stealing** – Attackers impersonate employees to steal passwords and data.
- **Password Spraying Attacks –** DHS and CISA issues May 5 alert warning of attacks on healthcare and other essential services.

Why are cyber attacks so successful?

Microsoft. (2019). Protect your organization aga
and information loss

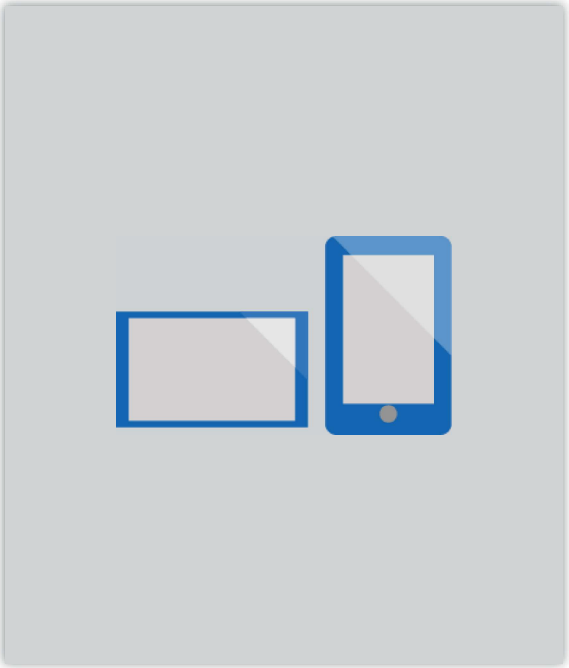
Where are the biggest security pains for organizations?

Email

Subpar antivirus antispam doesn't catch attacks

Users click on ransomware and phishing links

Accidentally send confidential data



Mobility

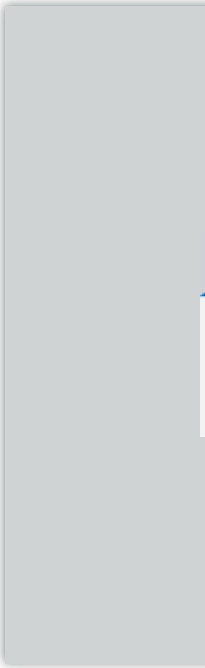
One extreme: Prohibit use because of security concerns

Or the other: Don't provide any protection for data on devices

User credentials

Users have same passwords across all accounts, increasing risk if compromised

Attackers have sophisticated methods to easily steal credentials



Compliance

Performance and specifically referer lot of gray area


Cybersecurity playbook

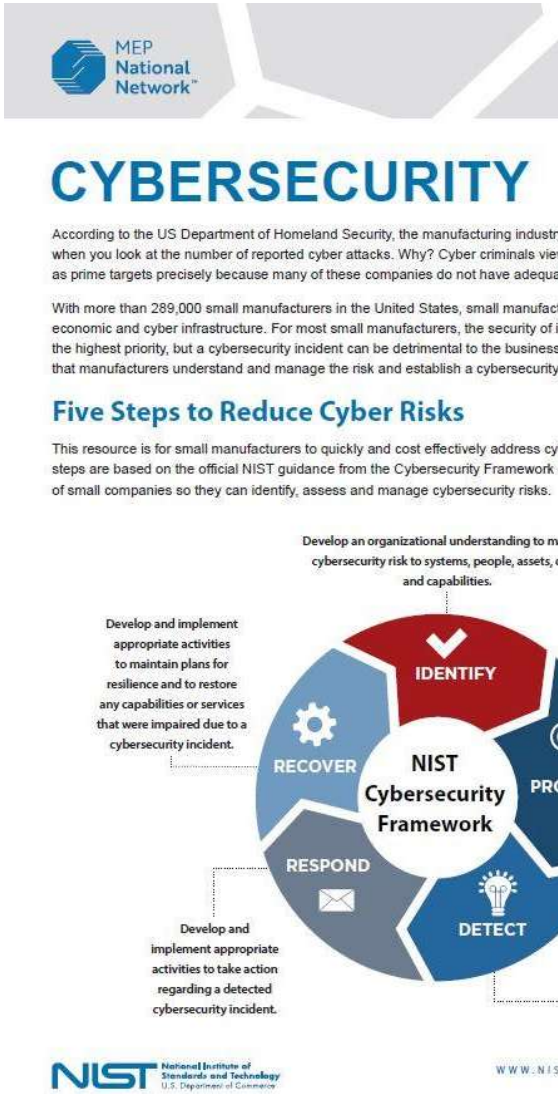
Make cybersecurity a priority

- Entire organization needs to make cybersecurity a focus
  - Board of Trustees
  - President and Vice Presidents
  - Administrative and Academic staff
  - Students
  - Everyone!

Perform a cyber risk assessment (self guided)

- Do it yourself
  - MEP National Network self guided assessment
  - 43 questions about your organization's security practices
  - Provides score in percentage. Aiming for 80% or higher
  - Highlights basic recommendations for your organization
  - Takes 15 minutes

https://www.surveymonkey.com/r/Z7RVFWV



Perform a cyber risk assessment (external vendor)

❑ Request these activities/scope in your RFP process

- Assessment of IT environment and cybersecurity controls
- Conduct interviews with key technology and security stakeholders
- Review organization's technology and cybersecurity culture
- Perform network and vulnerability scan of technology infrastructure
- Assessment of cybersecurity program and risk management practices including backup and disaster recovery
- Review IT and cybersecurity policies and procedures
- Send survey to the organization's staff to provide feedback on technology and security needs
- Provide a list of prioritized technology recommendations, roadmap and budget to achieve organization's goals

Common findings after your assessment

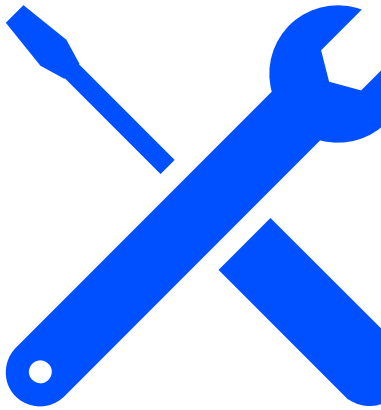
- Update/create security policies
- Reinforce proper cybersecurity behaviors with staff
- Enhance network security
- Migrate to cloud-based solutions with built-in security
- Business-class malware and anti-virus protection
- Routine maintenance of hardware and software systems
- User access management and passwords
- Improved disaster recovery plan and systems
- Monitor and respond to suspicious activity and breaches

Employee cybersecurity training

- ❑ Continuous training, not just a single event
- ❑ On-demand web-based training supplemented with live training works best
- ❑ Test employee habits with internal phishing emails to measure effectiveness
- ❑ Reinforce correct security behaviors to those who click on phishing emails
- ❑ Solutions for your consideration
  - KnowBe4
  - PhishLabs
  - HoxHunt

Maintenance of hardware and software systems

- Create monthly process to review, install and report on updates for:
  - Computers/server hardware
  - Microsoft Windows and Office
  - Antivirus
  - Software (Adobe, Firefox, Chrome, etc.)
  - Automate if possible
- Solutions for your consideration
  - Outsource to technology partner
  - Microsoft Intune
  - ManageEngine DesktopCentral

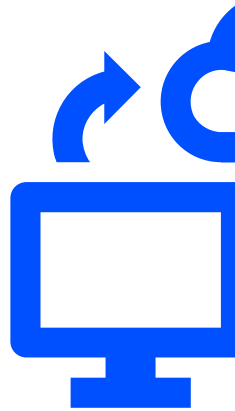


Manage accounts and passwords

- ❑ Implement stronger password standards
- ❑ Update default passwords
- ❑ Enable multi-factor authentication for:
  - VPN
  - Remote Desktop
  - Office 365
  - Google Workspace
  - Other remotely accessible systems
- ❑ Disable and remove old user accounts
- ❑ Disable users from installing software on work computers

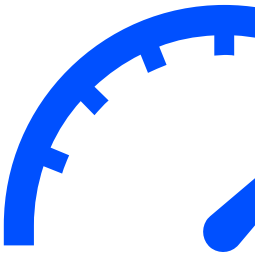
Improve disaster recovery plan and systems

- ❑ Update/create disaster recovery plan to include cyber incident
- ❑ Test your disaster recovery plan
- ❑ Implement backup and recovery solutions that are isolated from your network
- ❑ Solutions for your consideration
  - Veeam
  - Microsoft Azure Backup and Site Recovery
  - CrashPlan



Monitor and respond to suspicious activity

- ❑ Logins from outside your normal geography
- ❑ Login times outside of normal business hours
- ❑ Creation of email forwarding rules
- ❑ Changes to access levels and permissions
- ❑ Solutions for your consideration
  - ▶ Manually perform activities during routine maintenance activities
  - ▶ Endpoint Detection and Response
  - ▶ Add-on subscription to your anti-virus solution
  - ▶ Outsource to technology partner



Summary and tips to get started

Top tips for organizations getting started

1. Make it a priority now
   - Start small and grow into it
2. Seek help
   - You don't want to do this alone
   - Build your internal team
   - Consider outside experts
3. This is not a single event
   - Continuous process that needs to be incorporated into your organization's strategic plan
   - Make it a part of your organization's culture

Critical cybersecurity safeguards to protect your organization

1. Cybersecurity awareness training for all staff and families
   - Perform regularly and as part of employee onboarding
2. Multi-factor authentication
   - If not everywhere, at least on remote access methods (Office 365, Gmail, Remote Desktop, VPN, etc.)
3. Real time detection and response capabilities
   - Automatic scanning and alerting of vulnerabilities and cyber incidents
   - Antivirus is not enough
4. Store backups in multiple locations
   - Isolate from network and replicate to the cloud
5. Reduce and manage vulnerabilities
   - Harden systems / apply security patches / keep software and systems current / prioritize cloud solutions

Need additional help?

Reach out to

Ryan Peasley
Senior Manager

rpeasley@wipfli.com