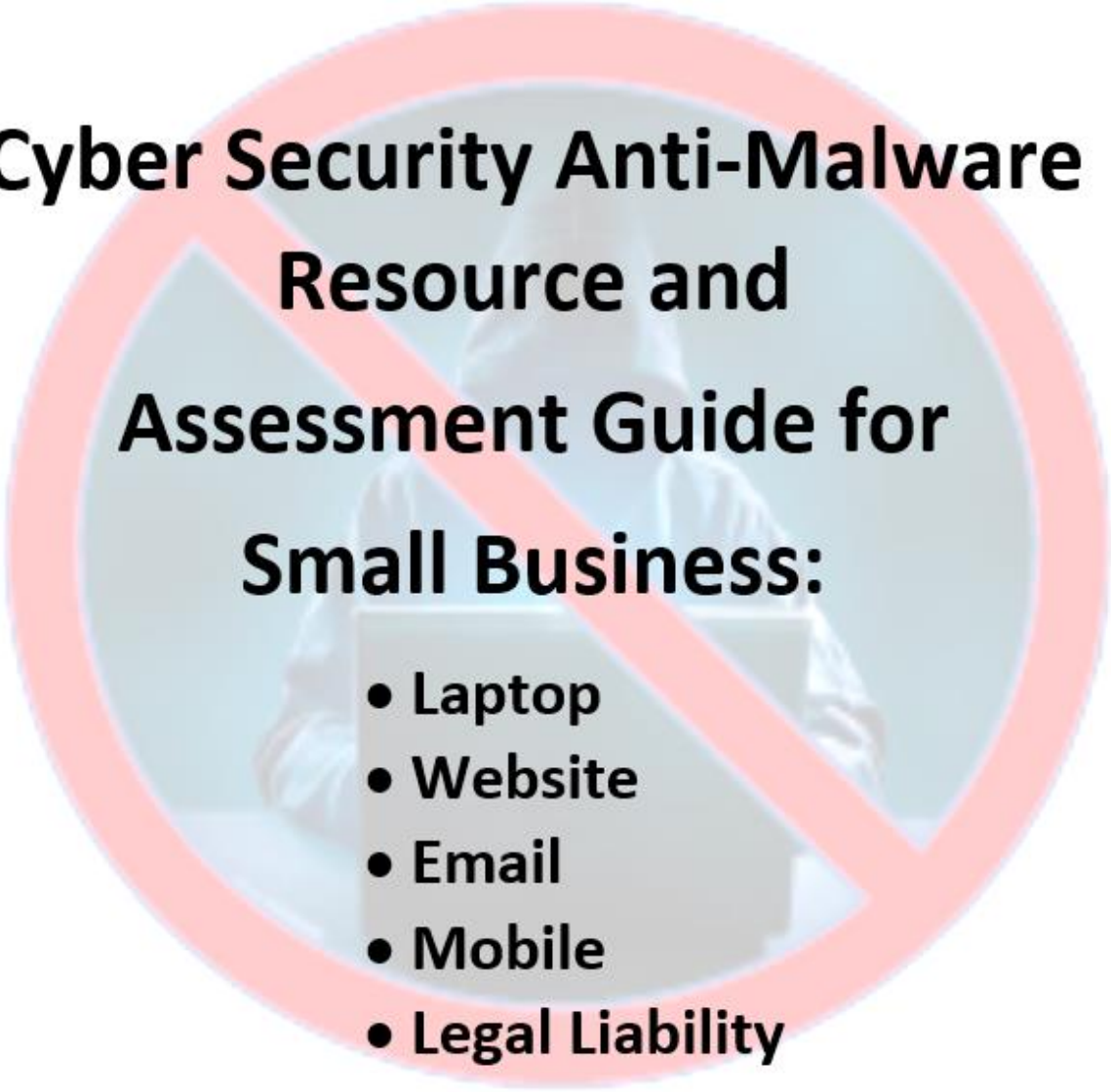
Ohio | Small Business Development Centers

Cyber Security Anti-Malware Resource and Assessment Guide for Small Business:



- Laptop
- Website
- Email
- Mobile
- Legal Liability

June 2018

ACKNOWLEDGMENTS

Special thanks to our presenters:

LAPTOP
Shawn Waldman
Chief Executive Officer
Secure Cyber Defense
937-353-7503
swaldman@secdef.com
www.secdef.com

WEBSITE
Israel Arroyo Jr. M.S, CISSP, GPEN, GWAPT, C|EH (GySgt USMC Res.)
Founder and CEO
Stealth Entry LLC
Cyber Security Solutions
614-423-9334
iarroyo@stealthentry.com
www.stealthentry.com

eMAIL
Bill Wagg
Client Care Specialist
thinkCSC
614-786-7100 ex. 126
bwagg@thinkcsc.com
www.thinkcsc.com

MOBILE
Spence Witten
Vice President, Global Sales
Lunarline, Inc.
440-876-7785
spence.witten@lunarline.com
www.lunarline.com

LEGAL
John Landolfi
Partner
Vorys, Sater, Seymour and Pease LLP
Columbus Office
614-464-8390
jllandolfi@vorys.com
www.vorys.com

Also, a special thank you to **Scott Taber**, Cyber Security Awareness Program Specialist, Michigan Small Business Development Center, Grand Valley State University, for reviewing the schematics before distribution.

ANTI-MALWARE SOFTWARE

Software to help protect against viruses, Trojan horses, worms, spyware and keylogger programs, ransomware, rootkits, bootkits and even adware.

EMAIL

eMail Filtering (recommended):

- Office 365
- Gmail

If Office 365 and Google not used, then for spam filtering use:

- Sonicwall – www.sonicwall.com

Anti-Virus Software:

- TrendMicro – www.trendmicro.com
- AV Defender— www.avdefender.com

End-User Training (constant end-user training; internal spam testing):

- KnowBe4— www.KnowBe4.com

Backup & Disaster Recover (MOST IMPORTANT for EMAIL SECURITY):

Look for 3 things:

- ***Time*** to recover
- ***Cost*** to recover
- How much ***downtime*** can business afford:
  - If **not** time sensitive (e.g., can wait 3 weeks): * Barracuda— www.barracuda.com
  - If time sensitive (e.g., need same day): * ShadowProtect (StorageCraft) www.storagecraft.com
    * VEEAM— www.veeam.com

ANTI-MALWARE SOFTWARE

Software to help protect against viruses, Trojan horses, worms, spyware and keylogger programs, ransomware, rootkits, bootkits and even adware.

LAPTOP

www.lookout.com -- recovers physically lost mobile device -- FREE

Find My iPhone app--FREE

https://eraser.heidi.ie/download/--"Eraser" freeware tool

WPA2 Personal-- strongest encryption available

Avast Anti-Virus -- FREE

AVG Anti-Virus -- FREE

Trend Micro – Home - Paid

Trend House Call for Home Networks – FREE Scan

Trend Worry Free Business – Paid – Small Business Pack

Nessus Home – Free Vulnerability Scanner

TunnelBear Secure VPN (or **Nord**)

Crash Plan – Backup

Carbonite -- Backup

ANTI-MALWARE SOFTWARE

Software to help protect against viruses, Trojan horses, worms, spyware and keylogger programs, ransomware, rootkits, bootkits and even adware.

MOBILE

The Bare Minimum

- **Basics of mobile data securit**

– Maintain physical control over phone
– Keep phone and apps updated
– Erase apps you don't need
– Enable password protection
– Use long passwords and PINS
– Enable remote wipe if available
– Turn off Bluetooth/Discoverability
– Encrypt data when possible at rest and in motion
– Install anti-virus, or even better, a comprehensive endpoint protection system
– Do not use wall USB receptacles found at public locations (i.e., airports)
– Do not use public wi-fi
– Consider a VPN

Stay Malware Free

- **Mitigation techniques**

– Keep phone and app software updated
– Only download apps from an official repository
– Vet apps before installing
– Android apps detail required permissions during installation; be aware of apps asking for unnecessary permissions.
– Watch out for social engineering attacks:
  - Don't click on links from emails or SMS messages
  - Don't open untrusted applications
  - Don't scan random QR codes

Mobile Devices – Bluetooth

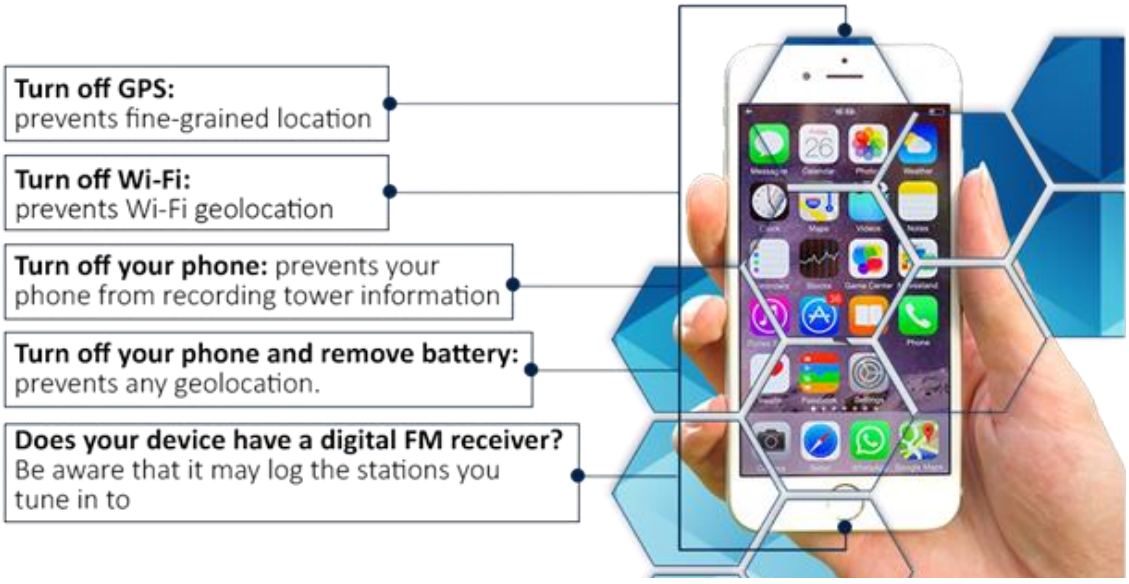
- **Keeping safe on Bluetooth**
  - Keep firmware and OS up to date
  - Remember that older devices may be especially vulnerable
  - Disable Bluetooth when not needed
  - Make devices discoverable and connectable only when necessary
  - User strong password for pairing
  - Pair devices in a secure area
  - Use only when absolutely necessary

Mobile Devices – Public

- **Connecting to a public Wi-Fi network?**
  - Do not have your computer set to auto-connect to networks
  - Forget networks
  - Use the HTTPS protocol
  - Monitor SSL security status
  - Utilize a VPN
  - Avoid visiting sensitive websites or transmitting sensitive data
  - Be suspicious of updates pushed over an untrusted network
  - Disable Wi-Fi when not is use and Bluetooth is not needed

Advanced: Hide and Seek

- **Geolocation Vulnerability Mitigation**



Suggested Tools

The Basics

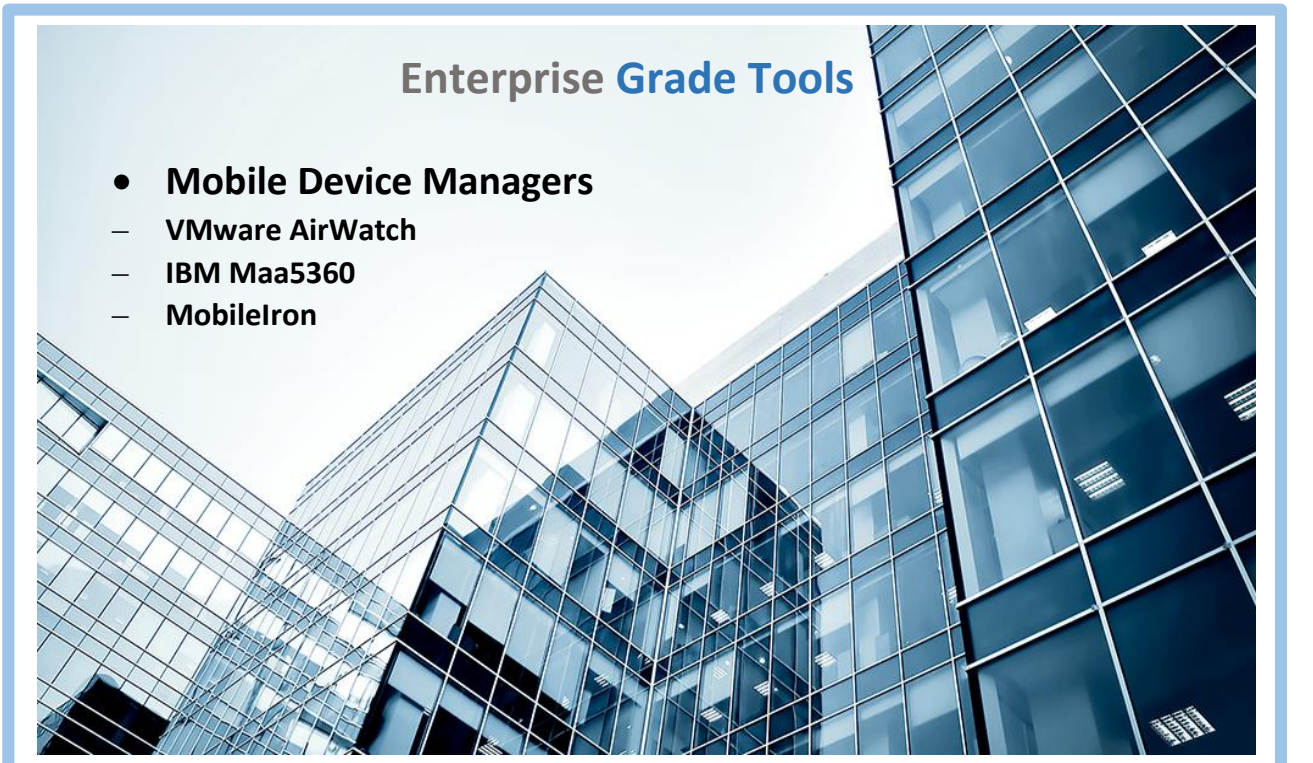
- **Anti-virus (most are free!)**
  - F-Secure
  - Avast
  - Avira
  - Bitdefender
  - Sophos
  - Norton
  - McAfee

Advanced / Enterprise Solutions

- **Comprehensive solutions that provide additional bells and whistles**
  - McAfee Mobile Security
  - Lookout
  - Trend Micro Mobile Security

Encrypted Communications

- **Virtual Private Networks**
  - F-Secure Freedome VPN
  - NordVPN
  - KeepSolid VPN Unlimited
  - Disconnect me
  - CyberGhost VPN
  - IPVanish VPN
  - Hide My Ass


Enterprise Grade Tools
Mobile Device Managers
VMware AirWatch
IBM Maa5360
MobileIron

ANTI-MALWARE SOFTWARE

Software to help protect against viruses, Trojan horses, worms, spyware and keylogger programs, ransomware, rootkits, bootkits and even adware.

WEBSITE

TOOLS AND TECHNIQUES FOR SAFE SURFING

- You can configure your browser of choice such as Internet Explorer, Microsoft Edge, Google Chrome, Mozilla Firefox and Apple's Safari Browser to detect website that may be infected with malware or steal your login credentials
- There are websites you can go to and input the URL of a website and it will tell you if the website is infected with malware or has vulnerabilities:

Web Browser Configuration tips

- https://support.microsoft.com/en-us/help/815141/internet-explorer-enhanced-security-configuration-changes-the-browsing
- https://transparencyreport.google.com/safe-browsing/search
- https://support.mozilla.org/en-US/kb/how-does-phishing-and-malware-protection-work

Free Resources and information

- https://www.dhs.gov/cyber-safety
- https://staysafeonline.org/
- https://www.getsafeonline.org/protecting-your-computer/safe-internet-use/

Online tools

- https://safeweb.norton.com/
- http://onlinelinkscan.com/

ANTI-MALWARE SOFTWARE

Software to help protect against viruses, Trojan horses, worms, spyware and keylogger programs, ransomware, rootkits, bootkits and even adware.

LEGAL

LIABILITIES and RAMIFICATIONS

See next two pages…

Ohio | Small Business Development Centers

CYBER RISK MANAGEMENT PROCESS

Part I -- Assessment

IMPACT SCREENING

Identify risk assessment to your people, process, data, and inventory.

- What are you trying to protect?
- Where does it live?
- What is worst-case scenario?
- What is impact on business?

IDENTIFY THREATS

COMMON TYPES OF ATTACKS

MALWARE	SPOOFING
PHISING	SPYWARE
BOTNETS	TROJAN HORSES
PHARMING	VIRUSES
RANSOMWARE	WORMS
SPAM	WI-FI EAVESDROPPING

IDENTIFY SOFTWARE VULNERABILITIES

Operating system without restrictions or limited access. For example:

- Missing data encryption
- OS command injection
- SQL injection
- Buffer overflow
- Missing authentication for critical function
- Missing authorization
- Unrestricted upload of dangerous file types
- Reliance on untrusted inputs
- Cross-site scripting and forgery
- Download of codes w/out integrity checks
- Use of broken algorithms
- URL redirection to untrusted sites
- Path traversal
- Bugs
- Weak passwords
- Virus-infected software

SELECT / IMPLEMENT / ASSESS / MONITOR SECURITY CONTROLS

Select baseline security controls; apply guidance and supplement controls as needed based on risk assessment.

Implement security controls within company architecture using sound systems engineering practices; apply security configuration settings.

Assess security control effectiveness (i.e., controls implemented correctly, operating as intended, meeting security requirements for information system).

Monitor and continuously track changes to the information system that may affect security controls

DETERMINE LEVEL OF RISK

Rudimentary Risk: Risk management is ad hoc, with limited awareness of risks; no collaboration with others.

Risk Awareness: Risk-management processes and program in place but are not integrated enterprise-wide; collaboration is understood, but organization lacks formal capabilities.

Risk Attentiveness: Formal policies for risk-management processes and programs are in place enterprise-wide, with partial external collaboration.

Risk Responsiveness: Risk-management processes and programs are based on lessons learned and embedded in culture, with proactive collaboration. Employee training.

ASSESS SECURITY OF YOUR VENDORS

You want to ensure the service providers and IT suppliers do not, themselves, create any business disruption or negative impact on your business' performance. Here are some things to look for:

- Check the software provider's credentials, certificates, references.
- Make sure that the vendor adheres to the same security standards that protect your company.
- Make sure the vendor is familiar with the most recent advancements in cyber protection, and if the vendor is marketing its own product, the vendor should be using its own product.
- Monitor performance/relationship. Key areas to monitor include the company's financial health, business continuity plans, and security controls which could affect your own company.
- Vendor offers frequent training for employees and new hires on physical security as well as cyber security to prevent a hacker from walking in and taking a PC.

Elements of an Incident Response Plan

Sources: *NIST Rick Management Framework*
NIST Framework Tiers of Maturity
Forrester Research, Inc.
securityscorecard.com
seasecurity.com

CYBER SECURITY MANAGEMENT PROCESS

Part II – 4 Steps in Developing Incident Response Plan

1 *Buy-in*

Ask basic questions:

- Do you have an Incident Response Plan in place today?
- When was the last time you tested the plan and simulated an exercise?

Get stakeholder buy-in:

- Top management: Provides funding and staffing for development and implementation.
- Project Team: At forefront of developing and implementing plan and communicating to end-users details and benefits to company and them.

2 *Draft*

Key Components:

- A single employee should be in charge of incident response.
- I.d. right people, roles, and responsibilities:
  - Legal
  - Internal communications (w/communications plan)
  - HR
- Assess current state and current visibility
- Look at Incident Response Flow
- Plan starts with alert response
- Be realistic about range of opportunistic attacks
- REAL INCIDENT: Do not wait to call, careful touching things, provide all details, follow IRP, follow chain of custody, set proper expectations.
- ***CONTACT LAWYER(S), especially to ensure state and federal laws are followed, including right to privacy, evidence collection, and possible prosecution or lawsuit.***

3 *Review*

1. Evaluate tech stack (combo software programs and languages) being monitored today:
   - Existing security
   - Networks events
   - Remote endpoints
   - Applications
2. Attack chain—look at internal network access across attack chain; explore network, see if lateral movement, mission target, where to detect, how to improve
3. 3 main ways attackers breach companies:
   - Vulnerabilities
   - Misconfigurations---too many privileges; "least" privilege should be enforced; when employees leave, deactivate

4 *Test Test Test*

Types of Testing:

- **Tabletop Exercises:** Realistic attack scenario—response who does what
- **Penetration Tests**: External, internal, mixed, neither, how did they get in and avoid detection?
- **Purple Team Exercises:**
  Closest to a real attack. Performs attack, defenders i.d. hackers and take action. Invoke communication channels, investigate.

Sources: Rapid 7
John Landolfi, Vorys, Sater, Seymour, Pease
Dashe & Thomson

Ohio | Small Business Development Centers

CYBER SECURITY ASSESSMENT

ASSETS EVALUATED			
Asset	**Check all that apply**	**Asset**	**Check all that apply**
Building(s)		Firewalls	
Employees		Mobile Devices	
Electronic Data		Data stored on local server	
Trade Secrets		Data stored in cloud	
Vehicles		VPN connection to partners	
Servers		Other:	
Desktop PCs			
Laptops			

NOTES

VALUE OF ASSETS (Quantitative)	If data lost tomorrow, how much time and money would it cost to re-create it?	How much would a competitor pay to obtain it?	What revenue would be lost from the data being compromised?	Would there be financial or legal penalties to pay?
Building(s)				
Employees				
Electronic Data				
Trade Secrets				
Vehicles				
Servers				
Desktop PCs				
Laptops				
Firewalls				
Mobile Devices				
Data stored on local server				
Data stored in cloud				
VPN connection to partners				
Other:				
VALUE OF ASSETS (Qualitative)	How would lost data impact your ay-to-day operations?	Could employees even work?	Would it affect your company's reputation?	How far would it set you back in productivity?
Building(s)				
Employees				
Electronic Data				
Trade Secrets				
Vehicles				
Servers				
Desktop PCs				
Laptops				
Firewalls				
Mobile Devices				
Data stored on local server				
Data stored in cloud				
VPN connection to partners				
Other:				

CALCULATE THE ANNUALIZED LOSS EXPECTANCY

Step 1:

- Identify situations (man-made or natural) where the asset could be adversely affected.
- How likely are these to happen and how often (per year).
- Calculate dollar loss of each situation.
- Determine cost on a per year basis by multiplying likelihood (how often) by the cost to get the ***Annualized Loss Expectancy*** (amount you can spend recovering from each situation).

Step 2:

Weigh cost of prevention against value of asset. If it costs more to protect the asset than it is worth, it does not make sense to use that control or prevention method.

Step 3:

Implement and Monitor Security Controls. Re-evaluate risk. Implement and monitor to ensure solution is performing according to your expectations. Also monitor vendor risk management.

Source: **securityscorecard.com/blog/risk-assessments-step-step-guide**