Cybersecurity From Home

Presenter

Dustin S. Mooney

Principal Consultant | Rigid Bits, LLC

RIGIDBITS

Objectives

1. Understand a risk-based approach to cybersecurity
2. Consider attack surface and new threats
3. Utilize a Plan of Action and Milestones
4. Implement cybersecurity WFH best practices

Agenda

1. Cybersecurity 101
2. WFH Cybersecurity
3. Action Items
4. Key Takeaways

Cybersecurity 101

“There is no secure. There is only more or less risk.”

Cybersecurity 101

- Risk = Likelihood x Impact
- Vulnerability
- C.I.A. = Confidentiality, Integrity, Availability
- Identify, Mitigate and Reduce Risk Exposure

Cybersecurity 101

- Risk = **Likelihood** x Impact
- **Vulnerability** 
- C.I.A. = Confidentiality, Integrity, Availability
- Identify, Mitigate and Reduce Risk Exposure

Ease of discovery
How easy is it for this group of threat agents to discover this vulnerability?

Ease of exploit
How easy is it for this group of threat agents to exploit this vulnerability?

Awareness
How well known is this vulnerability to this group of threat agents?

Intrusion detection
How likely is an exploit to be detected?

Cybersecurity 101

- Risk = Likelihood x **Impact**
- Vulnerability
- **C.I.A. = Confidentiality, Integrity, Availability**
- Identify, Mitigate and Reduce Risk Exposure

C.I.A.

Specific cybersecurity impacts to your **systems** and **data**

Additional Impacts

Loss of customer trust

Regulatory fines/penalties

Financial impact

Cybersecurity 101

- Risk = Likelihood x Impact
- Vulnerability
- C.I.A. = Confidentiality, Integrity, Availability
- **Identify, Mitigate and Reduce Risk Exposure**

Utilizing technology to operate a business efficiently comes with the cost of associated technological risks.

Cybersecurity decisions making based on fear reflects an attempt to eliminate risk which is not inherently feasible.

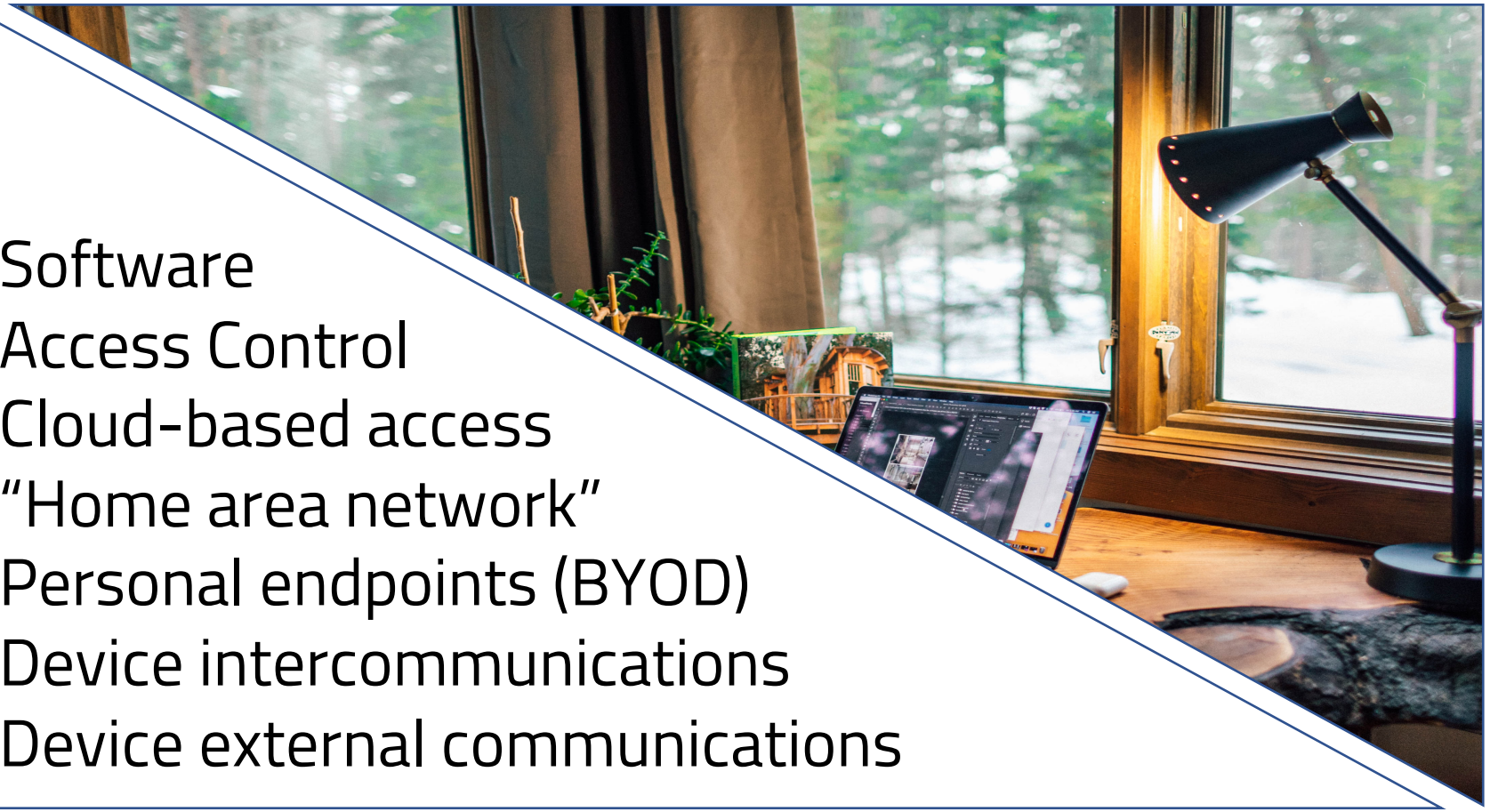
W.F.H. Cybersecurity

Attack Surface Shift

Attack Surface Shift: Office

Device external communications
Device intercommunications
Company issued endpoints
Print and file sharing
Cloud Systems
Extranet

Attack Surface Shift: Home



Software
Access Control
Cloud-based access
“Home area network”
Personal endpoints (BYOD)
Device intercommunications
Device external communications

Cybersecurity WFH Challenges

Insight

Employee actions: Clicking malicious emails, downloading sensitive data locally, visiting malicious website.

Visibility

New risks and vulnerability: Compromised endpoints, email compromise, communications, configurations.

Understanding

Policy adherence: Adherence to cybersecurity policy, knowledge how to respond, roles and responsibilities.

Cybersecurity WFH Solutions

Techniques

Protection Techniques: WFH cybersecurity policy, defense in depth, vulnerability identification, human element

Communication

Increased Communications: Report phishing hotline/email, weekly check-in emails, incident reporting

Testing and Training

Staying sharp: Weekly/Monthly test phishing emails, training campaigns

Action Items

POA&M – Plan of Action & Milestones

POAM ID	Controls	Weakness Name	Weakness Description	Weakness Detector Source	Weakness Source Identifier	Asset Identifier	Point of Contact
Unique identifier for each POAM Item	Applicable 800-53 Control(s)	Name of the weakness as provided by the scanner or otherwise summarizing the weakness	Description of the weakness and other information	The scanner name or other source that detected the vulnerability	Vulnerability identifier (Plugin ID) as provided by scanner (plugin ID/None)	Identifier Specified in the Inventory This is a unique string associated with the asset, it could just be IP, or any arbitrary naming scheme This Field should include the complete identifier (no short hand), along with the port and protocol when provided by the scanner. Each Asset should be separated by a new line (Alt+Enter)	Person Responsible for implementing this task
Unique Identifier	Control Number	Text	Text	[Nessus, Qualys, Webinspect, Security Assessment Report, etc]	Identifier	Identifier (port/protocol)	Text
V-1Example	AC-1	Open port on Example Firewall	Unprovisioned port left open on example firewall	Nessus	12345	172.246.15.3 (80/TCP) http://vuln.gov/queries 172.246.16.17 (80/tcp)	John Doe - Example CSP

Cybersecurity WFH Action Items: 1

Topic	Tasks	Purpose
Obtain a POA&M	• Acquire POA&M Template • Add tasks related to securing WFH risks and vulnerabilities	A POA&M will help your organization stay focused and organized. As well as show progress over time.
Home LAN/WiFi	• Acquire security intelligence enabled router • Change default passwords • Create separate networks for work and home use • Turn on security related features and monitoring	Reduce attack surface by restricting LAN/WiFi access. Protect against attacks by active monitoring and blocking of malicious content using security intelligence enabled routers.
Protect Endpoints	• Acquire and/or Extend Endpoint Detection and Response (EDR) licensing software for home and BYOD style endpoints	Next generation endpoint protection will better protect workstations and must have monitoring/console capabilities to keep track of identified threats.
Remote Access – VPN, RDP	• Require multifactor authentication for all remote access capabilities • Harden VPN+RDP configurations. Limit Access. • Turn on advanced authentication logging	Remote access solutions need to be protected and monitored due to their sensitive nature. Use MFA in all possible configurations.

Cybersecurity WFH Action Items: 2

	Tasks	Purpose
Remote Access - Cloud	• Create an inventory of all cloud-based applications and systems in use. Use this list to determine gaps • Require multifactor authentication for all remote access capabilities • Turn on authentication and user action logging • Review user accounts. Limit use of Administrative accounts	Cloud applications and systems come with unique risks. Reduce risks by protection authentication and increase monitoring where possible.
Email	• Harden outlook configurations and turn on advanced audit logging. Configure alerts for specific actions • Turn on and require MFA • Test users through simulated Phishing Exercises. Track progress and communicate with frequent abusers • Configure SPF, DKIM, DMARC	Business Email Compromise is a large problem with many simple fixes. Utilizing MFA will drastically reduce your risk and will likely halt authentication compromise attacks.
Password Management	• Acquire password management software • Monitor the Dark Web for compromised passwords • Review password policy	Password reuse can increase risk and use of compromised passwords may lead to system compromise.

Cybersecurity WFH Action Items: 3

	Tasks	Purpose
Process Considerations	• Create a policy and require dual approval of financial and sensitive transactions • Review policies for adding user accounts to remote access and cloud-based access	Using dual approval can defeat fraud attempts from business email compromise (defense in depth).
Incident Planning	• Create or review your IR Plan • Disseminate to individuals with roles and responsibilities • Determine how the company will respond to a security incident like BEC, malware infection, or data leaks • Update call logs with accurate team members and phone numbers • Review state, federal, and regulatory breach notification requirements	Incidents can still happen on BYOD devices or WFH situations. Prepare adequately and understand reporting requirements in accordance with applicable laws and regulations.
Cyber Liability	• Review coverages. Determine if policies apply to employees working from home • Ensure coverage amounts are sufficient	Understanding cyber liability coverages and protection amounts is key for preparing to respond to an incident.

WFH Employee Responsibilities

- Be an asset, not an addition to the problem
- Be vigilant about phishing emails in general and ones specific to world events
- Create your own “WFH” network
- Use a unique device for work or limit access
- Reporting phishing emails and malware infections
- Be cautious with web browsing, saving data, and the transfer of sensitive information

Takeaways

Key Points

1. Make cybersecurity business decisions based on risk
2. Consider C.I.A. impacts on your business
3. Reduce risk exposure
4. Understand your unique attack surface shift
5. Utilize a Plan of Action and Milestones
6. Add action items to your POA&M and implement

Closing Thoughts

"If you do not change direction, you may end up where you are heading."

End.

info@rigidbits.com
https://rigidbits.com