American Bus Association

Strengthening Cyber Resilience in a Post COVID-19 World

January 2021

Benjamin Gilbert
Cybersecurity Advisor, Region III
(*Virginia, West Virginia, District of Columbia*)
Cybersecurity Advisor Program
Cybersecurity and Infrastructure Security Agency

CISA
CYBER+INFRASTRUCTURE

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

Defend Today,
Secure Tomorrow

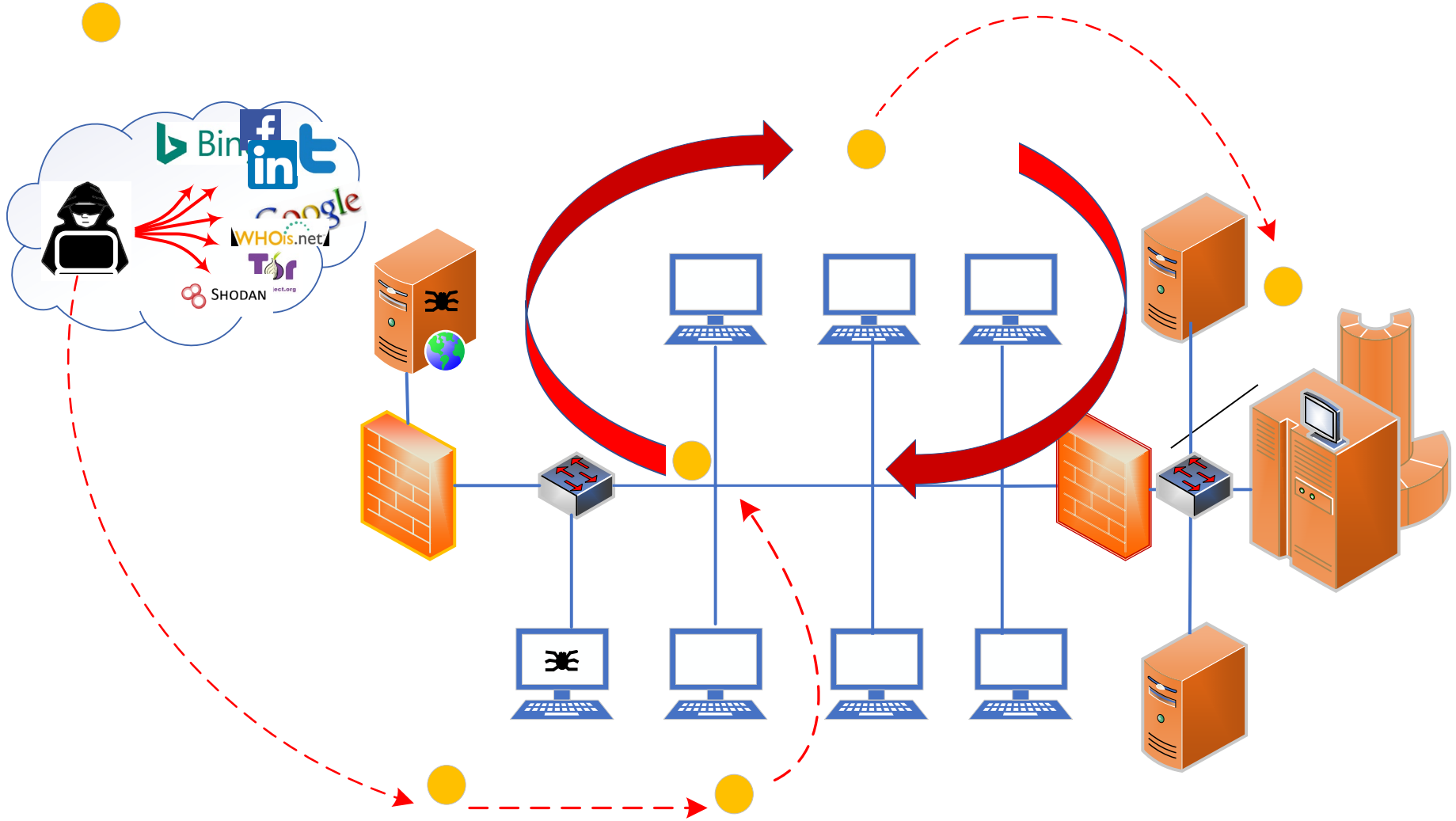
Today's Risk Landscape

America remains at risk from a variety of threats:

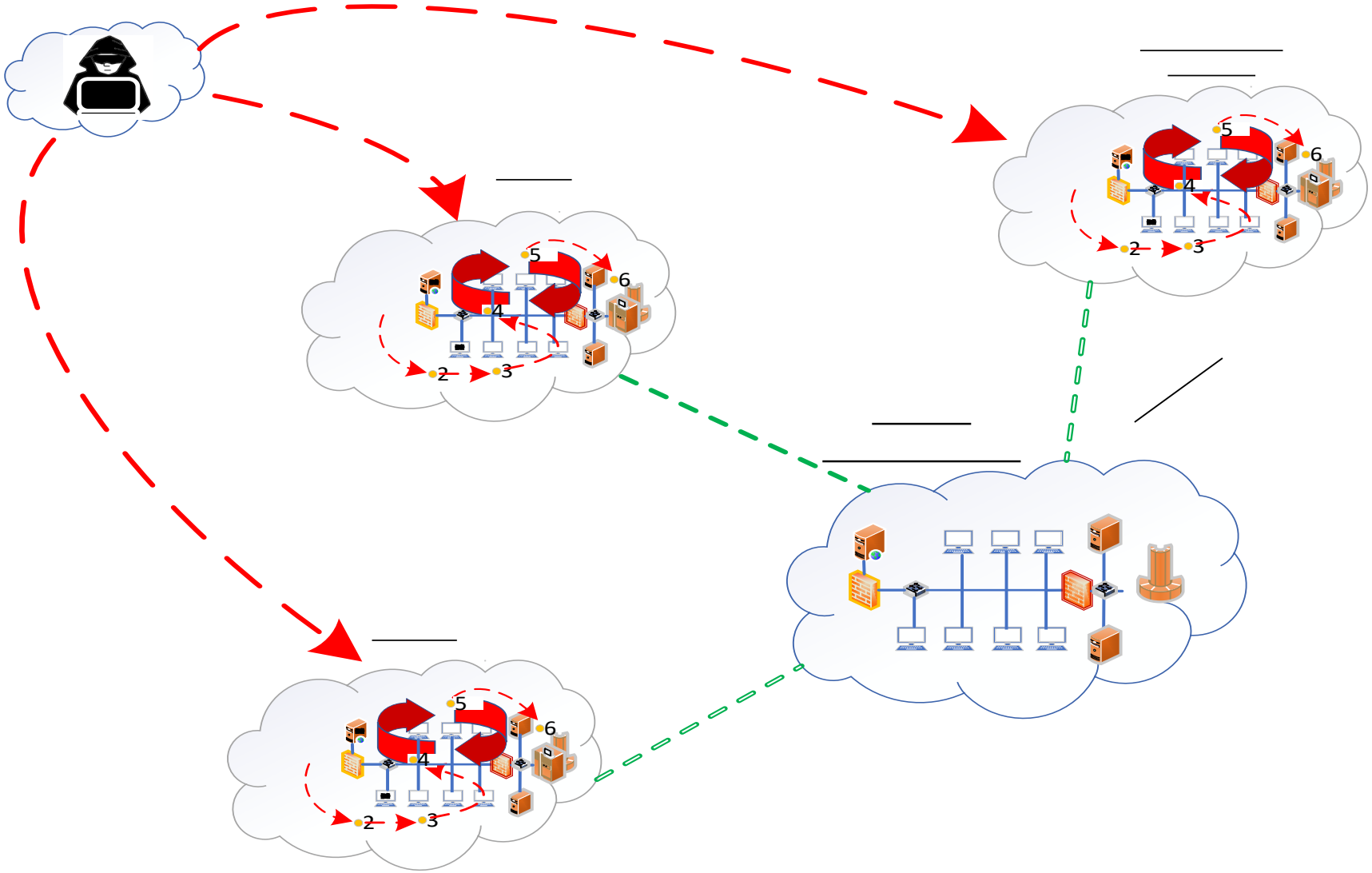
Cyber Threats Can Cause Operational Impacts

- **Ransomware**
  - WannaCry
  - REvil/ Sodinokibi (targeting MSPs)
  - Ryuk (targeting medical, education, SLTT)
  - Robinhood, Maze, Fobos, CovidLock, CryptoLocker, ,Pysa, VoidCrypt…
- **Advanced Persistent Threats**
  - APT29, APT41, APT39, APT38
- **malware**
  - Trickbot, Emotet, LokiBot
  - [wiperware] NotPetya
  - [ICS/OT specific] Triton/hatman malware targets Safety Instrumented Systems (SIS)
- **Threats to Supplychain and External Dependencies**
  - Supplychain attack (*e.g. SolarWinds compromise*)

Methodology of a Cyber Attack



Even More Complex Methodology of a Cyber Attack



Protective Measures - 1

IT Security Professionals and Leadership - The Essentials (short term)

- **Inventory all technology and information assets**. Identify high-value assets, **prioritize**, and deploy controls according to criticality to the organization's operations.
- **Deploy antivirus on servers and workstations** and ensure all are up-to-date
- **Turn on logging for all network appliances, servers and services** and implement a plan for managing logs
- **Backup data regularly** using secure, well-tested and accessible solutions. Know the limitations, where data resides, and how to access when primary means start to fail
- **Implement patch management practices** that can allow for patching vulnerabilities in a timely manner, (e.g., <30 days for critical vulnerabilities, <60 days for less severe vulnerabilities, etc.)
- **Implement strong user management practices**. This includes using strong password policies, least privilege practices, and using multi-factor authentication on high-value assets.

CISA
CYBER+INFRASTRUCTURE

Protective Measures - 2

IT Security Professionals and Leadership - The Essentials (longer term)

- **Have a plan for responding to cyber incidents** and **respond** to cyber incidents that are reported. Periodically review and update incident response plan accordingly.
- **Develop and strengthen situational awareness** - Sign up for membership with industry ISACs and leading cybersecurity centers and monitor for notifications and alerts.
- **Implement innovative security awareness training** as part of an incident management strategy
- **Implement a secure network architecture**. This includes ensuring properly configured network and security devices, network segmentation (or network isolation if systems are unpatchable), application and device whitelisting/blacklisting, hw/sw hardening, adoption of zero-trust models, etc.
- **Utilize cyber attack frameworks** during response and recovery of cyber attacks
- **Conduct internal audits and periodic cyber assessments** (risk-based, practice-based, and technical vulnerability assessments) in order to understand current security posture, gaps, capabilities, and operational capacities. Develop and implement mitigation plans.

CISA
CYBER+INFRASTRUCTURE

Protective Measures - 3

Organizational Leaders

- Know business risks and treat cyber as a business risk, to operations and to supply chains
- Foster a culture of operational resilience and cyber readiness
- Incorporate cybersecurity as a part of business strategy, including all external relationships
- Build a network of trusted relationships with sector partners and government agencies for access to timely cyber threat information, incident reporting, and response coordination

Everyone

- Participate in security awareness training and know
- Be aware of your digital footprint and know the end-user security features available to you
- Know the data backup options available and ensure locally stored data is backed up
- Be vigilant, accountable, and report incidents and suspicious activity immediately

CISA
CYBER+INFRASTRUCTURE

Post COVID Reopening Strategies

- CISA published V3.1 Guidance on Essential Critical Infrastructure Workforce
- CDC published guidance for Workplaces During COVID-19
  - Should you consider reopening?
    - Are you ready to protect employees at higher risk?
    - Are recommended health/safety actions in place?
    - Is ongoing monitoring in-place?
- Teleworking guidance published on CISA website

For more information, visit https://www.cisa.gov/telework

Tips for video conferencing:

1. **Use only approved video conferencing tools**
   - Don’t install unapproved clients – join browser-based sessions instead
   - Ensure links are correct
2. **Secure your meeting**
   - Consider attendees
   - Have a plan to terminate the meeting
   - Secure private meetings by password protecting and/or having a waiting room
   - Control attendees
3. **Secure your information**
   - Manage screensharing, recording, and file sharing options
   - Protect sensitive information
4. **Secure yourself**
   - Don’t reveal information unintentionally
   - Consider your surroundings (e.g. practice good OPSEC)
   - Check and update home networks

CISA Telework Essentials Toolkit

https://www.cisa.gov/publication/telework-essentials-toolkit

Executive Leaders

- Review and update organizational policies and procedures
- Implement cybersecurity training requirements
- Determine cyber risks with moving organizational assets outside of the perimeter
- Foster cyber secure culture

IT Professionals

- Patching and vulnerability management with hardware and software
- Implement enterprise cybersecurity controls
- Enforce multi-factor authentication for remote employees
- Maintain and enforce a list of organizationally approved software
- Perform frequent backups
- Address risk of phishing emails by Implement Domain-Based Message Authentication Reporting and Conformance (DMARC)

Teleworkers

- Ensure home network is properly configured and hardened
- Follow secure practices and procedures for handling PII, and other sensitive information
- Use caution when opening email attachments or clicking on links
- Report suspicious activities to your organization's IT security team

https://www.cisa.gov

Including:

- CISA Insights
- Cyber Essentials
- Cybersecurity Assessments

https://www.cisa.gov

Including:

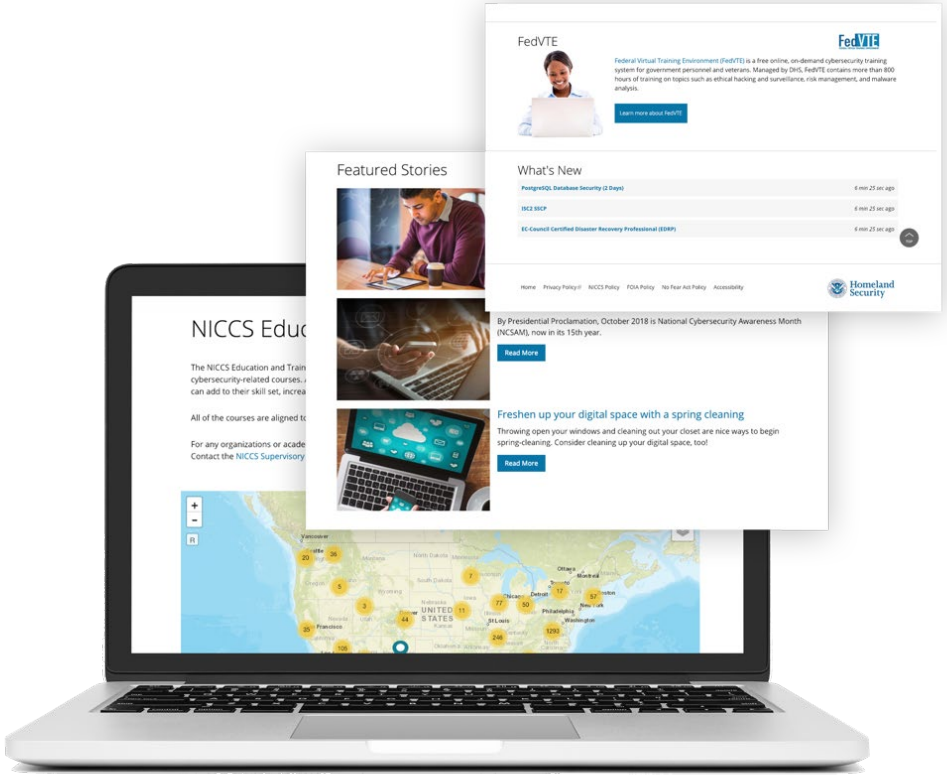
- Coronavirus Teleworking Guidance
- #Protect2020
- ITC Supply Chain Risk Management
- 5G

Cybersecurity Training Resources

CISA offers easily accessible education and awareness resources through the National Initiative for Cybersecurity Careers and Studies (NICCS) website.

The NICCS website includes:

- Searchable Training Catalog with 4,400 plus cyber-related courses offered by nationwide cybersecurity educators
- Interactive National Cybersecurity Workforce Framework
- Cybersecurity Program information: **FedVTE**, Scholarships for Service, Centers for Academic Excellence, and Cyber Competitions
- Tools and resources for cyber managers
- Upcoming cybersecurity events list



CISA CYBER+INFRASTRUCTURE

For more information, visit NICCS.US-CERT.gov

No-Cost CISA Cybersecurity Services

- **Preparedness Activities**
  - Cybersecurity Assessments
  - Cybersecurity Training and Awareness
  - Cyber Exercises and "Playbooks"
  - Information / Threat Indicator Sharing
  - National Cyber Awareness System
  - Vulnerability Notes Database
  - Information Products and Recommended Practices

- **Response Assistance**
  - 24/7 Response assistance and malware analysis
  - Incident Coordination
  - Threat intelligence and information sharing

- **Cybersecurity Advisors –** Regionally deployed advisors
  - Incident response coordination
  - Public Private Partnership Development
  - Advisory assistance and cybersecurity assessments

CISA Contact Information

Benjamin Gilbert, CISSP, CRISC, CEH **Cybersecurity Advisor, CISA Region III**	Benjamin.gilbert@hq.dhs.gov cyberadvisor@hq.dhs.gov
CISA URL	https://www.cisa.gov
To Report a Cyber Incident to CISA	***Call 1-888-282-0870*** ***email*** *CISAservicedesk@cisa.dhs.gov* ***visit*** *https://www.cisa.gov*