Wine Resources on a Beer Budget:

Free and Discounted Cybersecurity Resources to Make Your Government Budget Stretch Further

Stacey A. Wright
Stacey.Wright@cisecurity.org
Director of Strategic Partnerships
Center for Internet Security, Inc.® (CIS®)
Multi-State Information Sharing & Analysis Center® (MS-ISAC®)
Elections Infrastructure ISAC® (EI-ISAC)

Standards, Frameworks, & Regulations
CIS Controls – 20 Critical Controls that if followed secure organizations against the top cyber threats. • https://www.cisecurity.org/controls/ • **CIS RAM** is an information security risk assessment method that helps organizations implement and assess their security posture against the CIS Controls: https://learn.cisecurity.org/cis-ram
ISO 27001 Information Security Standard - An information security standard, that specifies a management system that is intended to bring information security under management control and gives specific requirements. • https://www.iso.org/isoiec-27001-information-security.html
ISACA's Control Objectives for Information and Related Technologies (COBIT) - An international good-practice framework for IT management and governance. COBIT provides an implementable "set of controls over IT and organizes them around a logical framework of IT-related processes and enablers." • http://www.isaca.org/COBIT/Pages/default.aspx
NIST Cybersecurity Framework (CSF) - A voluntary framework- based on existing standards, guidelines, and practices – for reducing cyber risks to U.S. critical infrastructure. • https://www.nist.gov/cyberframework
CIS Benchmarks – 140+ configuration guidelines for various technology groups to safeguard systems against today's evolving cyber threats. • https://www.cisecurity.org/cis-benchmarks/
Payment Card Industry Data Security Standard (PCI DSS) - An information security standard for organizations that handle branded credit cards from the major card schemes. The PCI Standard is mandated by the card brands and administered by the Payment Card Industry Security Standards Council. • https://www.pcisecuritystandards.org/pci_security/
Health Insurance Portability and Accountability Act (HIPAA) - U.S. law to modernize the flow of healthcare information, stipulate how Personally Identifiable Information maintained by the healthcare and healthcare insurance industries should be protected from fraud and theft, and address limitations on healthcare insurance coverage. • https://www.hhs.gov/hipaa/index.html
E.U. General Data Protection Regulation (GDPR) - EU law on data protection and privacy for all individual citizens of the European Union (EU) and the European Economic Area (EEA). It also addresses the transfer of personal data outside the EU and EEA areas. • https://eugdpr.org/

CISA Cyber Essentials - a guide for leaders of small businesses and small local governments to develop an actionable understanding of where to start implementing organizational cybersecurity practices

- https://www.cisa.gov/cyber-essentials

Federal Trade Commission (FTC) Tips and Advice for Small Businesses -

- https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity

Global Cyber Alliance (GCA) Cybersecurity Toolkit for Small Businesses –

- https://gcatoolkit.org

National and International Resources

Cybersecurity and Infrastructure Security Agency (CISA) - responsible for protecting America's critical infrastructure from physical and cyber threats. This mission requires effective coordination and collaboration among a broad spectrum of government and private sector organizations.

- https://www.dhs.gov/CISA
- **National Risk Management Center**: http://cisa.gov/national-risk-management
- **DHS Services Catalog for SLTT Governments**: https://www.us-cert.gov/sites/default/files/c3vp/sltt/SLTT_Hands_On_Support.pdf
- **DHS Election Security Library**: https://www.dhs.gov/publication/election-security-resource-library
- **Homeland Security Information Network (HSIN):** https://hsin.dhs.gov

Information Sharing and Analysis Centers (ISACs) - ISACs are organizations that were created to facilitate better information sharing among public and private sector. There are currently 24 ISACs. ISACs are primarily created to protect a particular industry or group. ISACs provide key threat intelligence, indicator sharing, and industry specific trends.

- https://www.nationalisacs.org/

Multi-State Information Sharing and Analysis Center (MS-ISAC) - The MS-ISAC provides a free and voluntary membership with no mandated information sharing requirement.
Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) - was established by the EIS-GCC to support the cybersecurity needs of the elections subsector.

Membership benefits include access to intelligence products and insider federal resources, as well as CIS Security Benchmark discounts, HSIN Portal access, and Malicious Code Access Program (MCAP) admittance. Services include:

- Malicious Domain Blocking and Reporting (MDBR)
- Computer Emergency Response Team (CERT) assistance
- Cybersecurity Advisories providing patch notifications
- Monthly Cyber Tips Newsletter in template form so you can add your own logo
- https://www.cisecurity.org/isac/

Emergence Management and Response Information Sharing and Analysis Center (EMR-ISAC) - collects and shares critical infrastructure protection (CIP) and emerging threat information to the Emergency Services Sector (ESS). The EMR-ISAC maintains a community of interest on the Homeland Security Information Network and routinely publishes an "Infogram" and CIP bulletins with information relevant to the sector.

- https://www.usfa.fema.gov/operations/ops_cip_emr-isac.html

Electricity Information Sharing and Analysis Center (E-ISAC) - Available to all electricity asset owners and operators, and select government and cross-sector partners in North America. Includes access to a secure portal, the GridEx exercise, customized situational awareness of security threats, physical and cybersecurity bulletins, task force reviews, and monthly con calls.

- https://www.eisac.com/

Federal Bureau of Investigation (FBI) – cyber intrusion and ransomware intelligence, travel security, and

insider threat information.

- https://www.fbi.gov

National Security Agency (NSA) / **Central Security Service** (CSS) – includes cybersecurity advisories, technical guidance, threat intelligence and assessments, cybersecurity education, and cybersecurity products and services.

- https://www.nsa.gov/what-we-do/cybersecurity/

DHS Office of Academic Engagement –
Lots of education specific resources including: Campus Resilience (CR) program; monthly newsletter; guides; roundtables; national and local exercises; exercise starter kits

- https://www.dhs.gov/topic/academic-engagement

Critical Infrastructure Cyber Community (C^3) Voluntary Program - pointers to resources aligned to the NIST Cybersecurity Framework, including geographically specific resources, hands-on support for critical infrastructure, Cybersecurity Advisors (CSAs), Protective Security Advisors (PSAs), and the Critical Infrastructure Partnership Advisory Council (CIPAC) Framework.

- https://www.dhs.gov/ccubedvp

Fusion Centers - are state-owned and operated centers that serve as focal points in states and major urban areas for the receipt, analysis, gathering and sharing of threat-related information between SLTT, federal and private sector partners.

- https://www.dhs.gov/fusion-centers

CIS SecureSuite - provides organizations access to multiple cybersecurity resources including our CIS-CAT Pro configuration assessment tool, build content, full-format CIS Benchmarks™, and more. Start secure and stay secure with integrated cybersecurity tools and best practice guidance for over 150 technologies.

- https://www.cisecurity.org/cis-securesuite/

Hiring

National Initiative for Cyber Security Education (NICE) and the **NICE Cybersecurity Workforce Framework** (800-181) – is a partnership between government, academia and the private sector focused on cybersecurity education, training and workforce development. 800-181 defines cybersecurity roles and responsibilities based 7 Categories and includes more than 130 job descriptions with detailed roles, responsibilities, skills, abilities, and recommended career paths.

- https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework

CyberSeek – provides detailed, actionable data about supply and demand in the cybersecurity job market

- https://www.cyberseek.org

Scholarship for Service - Scholarships to fund the typical student costs including tuition and education and related fees, plus stipends. In return, the students must work for the U.S. government (including SLTTs) for an equivalent amount of time upon graduating.

- https://www.sfs.opm.gov/

Training and Continued Learning

Federal Virtual Training Environment (FedVTE) - Free, online, on-demand and live cybersecurity training that is available to U.S. government employees and veterans. FedVTE includes over 60 courses including preparations for certification exams like Network+, Security+, CEH, and CISSP.

- https://fedvte.usalearning.gov

National Initiative for Cybersecurity Careers and Studies (NICCS) – one-stop shop for Cybersecurity Careers and Studies that offers over 2000 courses mapped to the National Cybersecurity Workforce Framework, as well as 40+ courses available to SLTT government employees and U.S. Veterans. It also

provides tools for managers, monthly events and customized job searches.
- https://niccs.us-cert.gov/

SANS Internet Storm Center - all-volunteer effort to provide early warning, threat detection and analysis, technical and procedural information, intrusion detection log entries, community Slack channel, and a daily podcast.
- https://isc.sans.edu/

Texas Engineering Extension Service (TEEX) – supported by FEMA, this site includes in-person course availability (U.S. only) and 10 free courses in three cyber discipline-specific tracks, including: non-technical for end-users; technical for IT professionals; and for business managers and professionals.
- http://www.teex.org

Industrial Control System Computer Emergency Response Team - Classroom and online training in industrial control systems security fundamentals is available for a range of learners. Regional courses and workshops are offered, including a five-day, hands-on training event in Idaho Falls, Idaho.
- https://ics-cert.us-cert.gov/Training-Available-Through-ICS-CERT

Industrial Control System (ICS) / SCADA Cybersecurity Resources – large compendium of ICS and SCADA resources.
- http://www.robertmlee.org/a-collection-of-resources-for-getting-started-in-icsscada-cybersecurity/

U.S. Department of Justice (DoJ) **Computer Crime and Intellectual Property Section** (CCIPS) - Provides speakers for training and outreach to state and local law enforcement, prosecutors, and government officials. In addition CCIPS attorneys are available to speak to prosecutors, law enforcement and others regarding a range of IT, cybersecurity and privacy topics.
- https://www.justice.gov/criminal-ccips/arranging-speakers

Cybrary - provides everyone who seeks to learn about cybersecurity with quality, up-to-date training and resources completely free of cost. There may be participation requirements.
- https://www.cybrary.it/

SEI Digital Library - Digital Library provides access to more than 3,500 documents from three decades of research into best practices in software engineering.
- https://www.sei.cmu.edu/

SANS Reading Room - Over 2,630 original computer security white papers in 101 different categories, with 2-4 webinars per week.
- https://www.sans.org/reading-room

RSA conferences – including recorded presentations and keynotes from U.S. and international conferences since 2013.
- https://www.rsaconference.com

AWS Machine Learning (ML) Curriculum – Amazon released the same ML curriculum used to train its developers and data scientists, including 65+ ML training courses totaling 50+ hours, plus hands-on labs and documentation. Developers, data scientists, data platform engineers, and business decision makers can use this training to learn how to apply ML, artificial intelligence (AI), and deep learning (DL).
- **https://aws.amazon.com/training/learning-paths/machine-learning/**

Coding Resources – online resources that provide a small number of programming courses for free.
- **Code.org:** https://code.org
- **Codecademy:** https://www.codecademy.com/
- **W3 Schools:** https://www.w3schools.com/

- **Learn Python the Hard Way:** https://learnpythonthehardway.org

Colleges Courses Online – Taking these courses is free but they will not provide credits toward a degree. These sites include courses from: MIT, Harvard, UC Berkeley, UT, BU, Brown, Georgia Tech, Arizona State, Cornell, University of Maryland, Australian National University, TUDelft, University of Adelaide, University of British Columbia, Sorbonne Universities, Rwthaachen University, and University of Queensland.

- **edX**: https://www.edx.org
- **Coursera**: https://www.coursera.org

More universities offer courses directly through their websites:

- **Harvard online learning:** http://online-learning.harvard.edu/ (sort by "free")
- **MIT:** https://ocw.mit.edu

Lynda.com – Lynda provides courses on a variety of subjects including: Cybersecurity, programming, and web design for a monthly fee. Lynda is partnered with public library systems, as such it's possible to get a free account with some library memberships.

- https://www.lynda.com/

Webcasts and Podcasts

- MS-ISAC National Webcasts: https://www.cisecurity.org/ms-isac/services/ms-isac-national-webinar/
- SEI CERT podcasts: https://www.sei.cmu.edu/publications/podcasts/index.cfm
- SANS vLive! webcasts: https://www.sans.org/webcasts/
- RSA Conferences: https://www.rsaconference.com
- Recorded Future: https://www.recordedfuture.com/resources/webinars/
- FireEye: https://www.fireeye.com/company/webinars.html
- Search.org: https://www.search.org/resources/podcasts/
- Justice Clearinghouse: https://justiceclearinghouse.com/
- ISACA: http://www.isaca.org/Education/Online-Learning/Pages/webinars.aspx
- BrightTalk: https://www.brighttalk.com/community/it-security
- Information Security magazine: https://www.infosecurity-magazine.com/webinars/
- NW3C: https://www.nw3c.org/online-training
- SANS ISC Storm Center: https://isc.sans.edu

Cyber Challenges and Experimental Spaces

U.S. Cyber Challenge – consists of Cyber Quests, free, online, spring competitions, and USCC Cyber Camps where the top performers from Cyber Quest are invited to participate in intensive one-week camps, in partnership with universities and colleges throughout the country.

- https://www.uscyberchallenge.org/

Vulnerable Test Sites –

- Hackazon: http://cybersecology.com/hackazon-review/
- Google Firing Range: https://github.com/google/firing-range
- OWASP Juice Shop Project: http://www.owasp.org/index.php/OWASP_Juice_Shop_Project

SANS Cyber Aces Online – Cyber Aces is an online course that teaches the core concepts needed to assess, and protect information security systems. The course is self-paced combination of tutorial and videos, available as open courseware so you can take it anytime.

- https://www.cyberaces.org/

CyberPatriot and CyberPatriot Elementary School Cyber Education Initiative (ESCEI) **–** CyberPatriot is the National Youth Cyber Education Program created by the Air Force Association (AFA) to inspire K-12 students toward careers in cybersecurity or other science, technology, engineering, and mathematics (STEM) disciplines critical to our nation's future. ESCEI is a set of three fun, interactive learning modules aimed at increasing grade K-6 students' awareness of online safety and cybersecurity principles. Supplemental activities

are also available to get students collaborating with each other about their newly learned cyber skills.

- https://www.uscyberpatriot.org/

SANS CyberStart and **Cyber Fast Track** – SANS sponsored challenges, tools, and games for students; introducing the topics of Linux, programming, web attacks, binary attacks, cryptography, and forensics.

- https://www.sans.org/CyberStartUS/
- https://cyber-fasttrack.org/

Mitre Cyber Academy – Making security resources available to the people who need them with a training portal, hands-on exercises, and competitions.

- https://mitrecyberacademy.org/

Network and IT Support

MS-ISAC Cybersecurity Advisories – Emailed notifications regarding high profile vulnerabilities and patch notifications for common software. These notifications aid in running a patch management program. Notifications are sent for most remote code execution (RCE), hardcoded password, and remote privilege escalation vulnerabilities. This does not include things that are less critical such as requiring authentication or local access required vulnerabilities.

- https://www.cisecurity.org/resources/advisory/

Computer Emergency Response Team (CERT) and **Hunt and Incident Response Team** (HIRT) - Typically available at the national or state level and within some universities or non-profits. These teams will provide: incident response, malware analysis, computer and network forensics, assessments, and/or log analysis.

- U.S. SLTTs can report an incident or request assistance from MS-ISAC:
  Phone: 1-866-787-4722 - Email: soc@msisac.org
- U.S. critical infrastructure can report an incident or request assistance from CISA:
  Phone: (888) 282-0870
- Canadian CERT: https://cyber.gc.ca/en/
- List of European CERTs: https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map

CIS CyberMarket – a collaborative purchasing program that serves U.S. SLTT government organizations, nonprofit entities, and public health and education institutions to improve cybersecurity through cost-effective group procurement. By leveraging the collective purchasing power of our participating public and nonprofit organizations, CIS CyberMarket works with industry-leading cybersecurity providers to secure significant group purchasing opportunities to meet the ever-evolving cybersecurity needs of our members. CIS may derive some revenue from the promotion of these opportunities.

- https://www.cisecurity.org/services/cis-cybermarket/

Domain-based Message Authentication, Reporting & Conformance (DMARC)

- **DMARC Setup Guide** – guides organizations through creating a DMARC policy, as well as policies for Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM)
- **DMARC Risk Scanner** - helps organizations to assess the DMARC implementation of their domains, and those of subcontractors and other partners
- https://www.globalcyberalliance.org/use-a-solution/

Quad9 - free security solution that uses the DNS to protect your system against the most common cyber threats. It improves your system's performance, plus, it preserves and protects your privacy

- **https://quad9.net/**

Shodan – a search engine for Internet-connected devices. Use it to find vulnerable devices on your network or where particular types of devices are located in a geographic region.

- https://www.shodan.io/

Censys – a search engine for Internet-connected servers and devices. Use it to find vulnerable devices on your network.

- https://censys.io/

No More Ransom - An initiative by the National High Tech Crime Unit of the Netherlands' police, Europol's European Cybercrime Centre and two cyber security companies, Kaspersky Lab and Intel Security, with the goal to help victims of ransomware retrieve their encrypted data without having to pay the criminals. Known decryptors are posted here and you can upload an encrypted file to determine what variant of ransomware is on a network.

- https://www.nomoreransom.org

New Jersey Cybersecurity and Communications Integration Cell (NJCCIC) **–** helpful and detailed website with a weekly bulletin, news and alerts, and cyber threat profiles for most botnets, mobile malware, ransomware, and trojans commonly encountered.

- https://www.cyber.nj.gov/

KnowBe4's free tools: is a list of free network security tools and assessments to help identify vulnerabilities and secure networks.

- https://www.knowbe4.com/free-it-security-tools **(check out the Ransomware Simulator Tool)**

GHIDRA – software reverse engineering (SRE) suite of tools developed by NSA's Research Directorate in support of the cybersecurity mission.

- https://ghidra-sre.org

Investigatory Tools for criminal investigations, forensics, and network security

VirusTotal - A publicly accessible platform used to analyze suspicious files and URLs to detect malware such as viruses, worms, and trojans.

- https://www.virustotal.com/

Malicious Code Analysis Platform (MCAP) - a web-based service that enables members to submit and analyze suspicious files in a controlled and non-public fashion.

- Available to MS-ISAC and EI-ISAC members

Malware Investigator - a tool that provides users the ability to submit suspected malware files and within as little as an hour, receive detailed technical information about what the malware does and what it may be targeting.

- Available to InfraGard members

Regional Computer Forensics Lab (RCFL) - A U.S. based, one-stop, full service forensics laboratory and training center devoted entirely to the examination of digital evidence in support of criminal investigations. Training is available in the nationwide training centers. Investigative areas include terrorism, child pornography, Crimes of Violence, Trade secret theft, internet crimes, financial fraud, and crimes against intellectual property. There may be costs associated with some services.

- https://www.rcfl.gov/

Anomali – a platform that provides machine-to-machine indicator transfer using the STIX/TAXII format. Receiving indicators may be free. U.S. SLTTs can join MS-ISAC and receive free research accounts to their intelligence platform, ThreatStream.

- https://www.anomali.com/

Search.Org ISP List - all known law enforcement contacts for companies.

- http://www.search.org/resources/isp-list/

TALOS IP Address Reputation Center

- https://www.talosintelligence.com/reputation_center

OSint Framework – an online search guide that provides links to various search engines for usernames, email addresses, domain names, IP addresses, images/videos/docs, social networks, instant messaging, people search engines, dating, telephone numbers, public records, business records, transportation, geolocation tools/maps, search engines, forums/blogs/IRC, archives, language translation, metadata, mobile emulation, terrorism, dark web, digital currency, classifieds, encoding/decoding, tools, malicious file analysis, exploits & advisories, threat intelligence, OpSec, documentation, and training.

- https://osintframework.com/

MalwareAnalysis.Tools – an online search guide that provides links to various search engines

- http://malwareanalysis.tools

National Software Resource Library - Supported by the U.S. DHS, federal, state, and local law enforcement, and NIST, the NSRL is a collection of digital signatures of known, traceable software applications to promote efficient and effective use of computer technology in the investigation of crimes involving computers. This site also contains a curated Kaspersky Labs software hash set.

- https://www.nist.gov/software-quality-group/national-software-reference-library-nsrl

Department of Justice Considerations for Darkweb Activities- legal considerations when gathering online cyber threat intelligence and purchasing data from illicit sources

- https://www.justice.gov/criminal-ccips/page/file/1252341/download

IOCs

DHS **Automated Indicator Sharing** (AIS) **–** free capability that enables the exchange of cyber threat indicators between the Federal government and the private sector at machine speed

- https://www.dhs.gov/ais

Domain IP Abuse Websites – these websites track malware families and provide lists of known Command and Control (C2s) IP addresses and other potential indicators.

- Abuse.ch: https://ransomwaretracker.abuse.ch
- Malware Domain List: http://www.malwaredomainlist.com
- CryptoWall Tracker: https://www.cryptowalltracker.org/
- Black Hole DNS Sinkhole: http://mirror1.malwaredomains.com/

Spamhaus - free access is restricted to low-volume non-commercial users (non-commercial, less than 100,000 SMTP connections and query volume is less than 300,000 queries)

- https://www.spamhaus.org

COVID-19 Cyber Threat Intelligence

- https://www.anomali.com/learn/covid19
- https://www.domaintools.com/resources/blog/free-covid-19-threat-list-domain-risk-assessments-for-coronavirus-threats
- https://bazaar.abuse.ch/browse/tag/COVID-19/

COOP Planning

FEMA COOP Division - Directives, templates and guidance for federal organizations, state, territory, tribal and local entities, for the purpose of continuity planning and emergency preparedness. Includes: Training Guide – Gaining Leadership Buy-In; COOP Planning & Devolution Planning Template; Continuity Exercise Design Course; Telework Exercise; COOP for First Responders; Continuity Guidance Circular; Continuity Resource Toolkit; and a Continuity Assessment Tool.

- https://www.fema.gov/media-library/resources-documents/collections/343

Assessments and Exercises

Nationwide Cyber Security Review (NCSR) - a voluntary self-assessment survey designed to evaluate cybersecurity management within SLTT governments, including all states (and agencies within), local government jurisdictions (and departments within), tribal and territorial governments can participate.

- https://www.cisecurity.org/ms-isac/services/ncsr/

CISA Assessment Services	CyHygiene	Phish Campaign	Remote PenTest	VADR	RVA	Red Team	Common Plat Enum
Duration	Ongoing	6 weeks	6 weeks	1-2 week(s)	2 weeks	90 days	6 weeks
Perspective	Untrusted; External	Untrusted; External	Cooperative; External	Cooperative; Internal and External	Cooperative; Internal and External	Adversarial; External	Academic; Laboratory
Objective	Assess and Monitor Exposure	Measure an organization's propensity to click on email phishing lures	Identify Exploitable Attack Vectors	Assess Technical Design and Program Maturity	Identify System Vulnerabilities	Assess Detection and Response Capability	Harden Products
Value to Customer	Greater insight into exposure; assists with risk management			Improved Processes, Policies, and Design	Decreased Risk	Benchmark and Train Staff	Products are more secure and resilient out of the box
Value to DHS (ROI)	Greater insight into exposure; assists with triage and urgency			Practical understanding of operational maturity and vulnerability		Attack Chain, Measurable Events Response	See Above
Wait Time Capacity	No wait time No limit	~ 3 months 32	~ 3 months 64	~ 3 months 50	~ 9 months 60	~ 6 months 4	

FEMA Homeland Security Exercise and Evaluation Program (HSEEP) - provides a set of guiding principles for exercise programs, as well as a common approach to exercise program management, design and development, conduct, evaluation, and improvement planning. Exercises are a key component of national preparedness - they provide elected and appointed officials and stakeholders from across the whole community with the opportunity to shape planning, assess and validate capabilities, and address areas for improvement.

- https://www.fema.gov/hseep

European Union Agency for Cybersecurity (ENISA) Cyber Exercises - includes links to the Cyber Europe programme, Cyber Exercise Platform, trainings and studies, and cyber exercises supported by ENISA. https://www.enisa.europa.eu/topics/cyber-exercises

Mitre's Cyber Exercise Playbook - provides an overview of the cyber exercise process from inception to reporting. It introduces the terminology and life cycle of a cyber exercise and then focuses on the planning and execution aspects of such exercises, to include objectives, scenarios, reporting and assessment procedures, network architecture, tools, and lessons learned from utilizing the scenarios outlined during an exercise with Partner Nations. Reading this document and reviewing the reference materials should enable exercise planners to understand the purpose, objectives, planning, and execution processes for conducting cyber

exercises.

- https://www.mitre.org/sites/default/files/publications/pr_14-3929-cyber-exercise-playbook.pdf

CIS' 6 Tabletop Exercises to Help Prepare your Cybersecurity Team - Tabletop exercises are meant to help organizations consider different risk scenarios and prepare for potential cyber threats. All the exercises featured in this white paper can be completed in as little as 15 minutes, making them a convenient tool for putting your team in the cybersecurity mindset. In addition, each scenario will list the processes that are tested, threat actors that are identified, and the assets that are impacted.

- https://www.cisecurity.org/white-papers/six-tabletop-exercises-prepare-cybersecurity-team/

Working Groups

InfraGard - A partnership between the FBI and the private sector that grants a free, vetted membership providing access to TLP: AMBER, GREEN, WHITE and U//FOUO information along with briefings and meetings on cyber security related topics. To join you must be a U.S. citizen and pass a criminal history background check. There is an annual meeting, and local chapters host meetings and webinars.

- https://www.infragard.org/

FBI Cyber Task Force - The FBI CTF operates in support of the national effort to counter threats posed by terrorist, nation-state, and criminal cyber actors, each CTF synchronizes domestic cyber threat investigations in the local community through information sharing, incident response, and joint enforcement and intelligence actions.

- In the U.S. contact your local FBI Field Office to determine their needs and requirements.

USSS Electronic Crimes Task Force (ECTF) **-** is meant to bring together federal, state, and local law enforcement, prosecutors, private industry and academia for the prevention, detection, mitigations, and aggressive investigation of attacks on the nation's financial and critical infrastructures.

- In the U.S. contact your local USSS Field Office to determine their needs and requirements.

National Fusion Center Association's Cyber Intelligence Network/Threat – mailing list for cyber focused members of the fusion centers and other agencies that work with them. Vetted access includes access to a 24x7 situational awareness room.

- cinregistration@nfcausa.org

ISACA - an international professional association focused on IT governance.

- http://www.ISACA.org

Information Systems Security Association (ISSA) **-** Professionals who have as their primary responsibility information systems security in the private or public sector, or professionals who supply information systems security consulting services to the private or public

- http://www.ISSA.org

ISC2 - an international, nonprofit membership association for information security leaders like you. We're committed to helping our members learn, grow and thrive. More than 150,000 certified members strong, we empower professionals who touch every aspect of information security

- https://www.isc2.org/

International Association of Computer Investigative Specialists (IACIS) **-** is dedicated to the training and certification of the digital forensics community in support of its membership. Our vision is to be the premier organization of choice for the digital forensics community by providing law enforcement focused membership services, training and certification

- **http://www.IACIS.com**

High Technology Crime Investigation Association (HTCIA) - is a non-profit organization committed to high technology training, education, networking through local chapters & international events

- http://www.HTCIA.org

Industrial Controls Systems Joint Working Group (ICSJWG) **-** supports information sharing and reduced risk to the nation's industrial control systems through enhanced collaboration between:
Federal Government
Private owners of industrial control systems across all critical infrastructure sectors
Operators of industrial control systems across all critical infrastructure sectors.

- **https://ics-cert.us-cert.gov/Industrial-Control-Systems-Joint-Working-Group-ICSJWG**

Scientific Working Group on Digital Evidence (SWGDE) – website brings together organizations actively engaged in the field of digital and multimedia evidence to foster communication, cooperation, quality and consistency within the forensic community. The website has a good resources page. Membership requires an annual fee.

- https://www.swgde.org/

Information Sharing & Analysis Organizations (ISAO) – a non-governmental organization established October 1, 2015, and led by the University of Texas at San Antonio (UTSA) with support from LMI. Our mission is to improve the Nation's cybersecurity posture by identifying standards and guidelines for robust and effective information sharing and analysis related to cybersecurity risks, incidents, and best practices.

- https://www.isao.org/
- Faith Based ISAO - https://faithbased-isao.org/about/

HackerSpaces - a community-operated physical place, where people can meet and work on their projects. This website is for anyone and everyone who wants to share their hackerspace stories and questions with the global hackerspaces community. These spaces may have a membership/participation fee.

- https://wiki.hackerspaces.org/

Meetup - a social networking platform that allows users to schedule, share, and search for events related to a particular topic. Meetup is a useful tool for identifying cybersecurity events, discussion groups, and exchanges in your area. These spaces may have a membership/participation fee.

- https://www.meetup.com/

Insider Threat Resources

National Insider Threat Task Force and Maturity Framework
Insider threat information for senior officials and leadership, program personnel, and employees, including: training and awareness materials.

- https://www.dni.gov/files/NCSC/documents/nittf/20181024_NITTF_MaturityFramework_web.pdf

Spreading the Word

MS-ISAC Monthly Newsletter – a two-page cybersecurity newsletter for end-users distributed in template form to allow for rebranding and redistribution by your agency.

- https://www.cisecurity.org/resources/advisory/

OUCH! Newsletter – OUCH! is the world's leading, free security awareness newsletter designed for everyone. Published every month in multiple languages, each edition is carefully researched and developed by the SANS Security Awareness team, instructors and community members. Provided in multiple languages.

- https://www.sans.org/security-awareness-training/ouch-newsletter

National Cyber Security Awareness Month - effort between government & industry to ensure every American has the resources to stay safer online

- https://www.cisa.gov/national-cyber-security-awareness-month

Stop.Think.Connect™ - a public awareness campaign aimed at increasing the understanding of cyber threats

and empowering the American public to be safer and more secure online. Resources include tips, advice, videos, posters, and educational campaigns.

- https://staysafeonline.org/

National Counterintelligence and Security Center (NCSC) Raise Your Shield – U.S. Office of the Director of National Intelligence supported website dedicated to raising awareness among government employees and private industry about foreign intelligence threats, the risks they pose, and the defensive measures necessary for individuals and organizations to safeguard that which has been entrusted to their protection.

- https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-know-the-risk-raise-your-shield

Citizen Support

FraudSupport.org – a website powered by the Cybercrime Support Network (CSN) to aid victims of cybercrime and online fraud. Designed to be user friendly it supports citizens and small businesses.

- https://fraudsupport.org

IdentityTheft.gov – a U.S. government website to support victims of identity theft. By answering a few simple questions, victims are able to report and receive tailored advice on the steps they need to take to recover from identity theft.

- https://identitytheft.gov/

Resources for Children

K-12 Computer Science Framework - a collaboration between the Association for Computing Machinery, Code.org, Computer Science Teachers Association, Cyber Innovation Center, and National Math and Science Initiative, the K-12 computer science framework helps inform the development of standards and curriculum to build a capacity for teaching computer science.

- https://k12cs.org/

StopBullying.gov – U.S. government website to provide training, state laws and policies, school resources, and resources for children focused around an anti-bullying campaign.

- https://www.stopbullying.gov/

NetSmartzKids – a program from the National Center for Missing and Exploited Children to promote online safety

- https://www.missingkids.org/netsmartz/home

Be Internet Awesome with Google – online resources to help kids be safe, confident explorers of the online world

- https://beinternetawesome.withgoogle.com/en_us

Public Broadcasting Service – quizzes, games, and library of resources to educate children, parents, and teachers about cybersecurity.

- https://www.pbs.org/wgbh/nova/labs/lab/cyber/
- **PBS CyberChase**: https://pbskids.org/cyberchase/

FBI's Safe Online Surfing – a website with games and teacher resources to keep children safe online.

- https://sos.fbi.gov/

Australian Government Electronic Safety website for children– a website with games and teacher resources to keep children safe online.

- https://www.esafety.gov.au/kids-quiz/

K-12 Cybersecurity Resource Center – compendium of resources and news about the K-12 cybersecurity sector.

- https://k12cybersecure.com/

Resources for Elections

Cloudflare Athenian Project –
- **Qualifications:**
  - Administration of elections; Contain voter data; Reporting of election results
- **Services:**
  - DDoS Attack Mitigation
  - Data Protection: HTTPS encryption, Rate Limiting, and Web Application Firewall (WAF)
  - Website Integrity: Protect from common vulnerabilities
  - Website Availability: Cloudflare's CDN
  - Support & Services: Included 24/7/365 phone, chat, and email support for critical issues
- https://www.cloudflare.com/athenian/

Google Protect Your Election Initiative –
- **Qualifications:**
  - Website containing election information
- **Services:**
  - Project Shield – protects news and election sites from DDoS attacks
  - Password Alert – free Chrome extension that makes sure Google's password is only entered into a Google site
  - Two-Step Verification – 2FA
  - Advanced Protection Program - safeguards Google Accounts by leveraging physical security keys, limiting access to your emails and files from third - party services, and adding extra step s to verify your identity.
- https://protectyourelection.withgoogle.com/intl/en/

Protected Voices – FBI initiative to mitigate the risk of cyber influence operations targeting U.S. elections
- https://www.fbi.gov/investigate/counterintelligence/foreign-influence/protected-voices

Resources for Law Enforcement

FBI Cyber Shield Alliance – Virtual Academy - provides extensive resources for state, local, tribal, and territorial (SLTT) law enforcement partners via the Law Enforcement Enterprise Portal to access eGuardian as a way to report cyber incidents, to share intelligence, and to access federally sponsored training. Courses include malware investigator, Cyber Investigation Certification Program (CICP) and the Cyber Shield Alliance (CSA).
- https://www.cjis.gov/CJISEAI/EAIController

IACP Cyber Center – online resource designed to assist law enforcement personnel who are investigating and preventing crimes that involve technology.
- http://www.iacpcybercenter.org/

National White Collar Crime Center (NW3C) – U.S. support for law enforcement and regulatory agencies involved in the prevention, investigation and prosecution of economic and high-tech crime. Some international availability. Training options include instruction in all areas of economic and cyber crime investigation and prosecution.
- https://www.nw3c.org

National Sheriff's Association (NSA) **– Institute for Cybersecurity –** multiple online and in person training opportunities for NSA members
- https://www.sheriffs.org/gcps/cybersecurity

Internet Crime Complaint Center (IC3) - place to file a complaint regarding an online crime (e.g. auction fraud, phishing emails, malware, etc.). Law enforcement can get an account and query the reports. IC3

publishes alerts, advisories, and reports.

- https://www.ic3.gov/default.aspx

Search.org Training - self-paced and instructor led courses at varying levels of difficulty. Course examples include Network Investigations & Digital Triage, Social Networking Sites, and Crime involving Handheld Computing Devices.

- https://www.search.org/get-help/training/high-tech-crime-investigations/self-paced-training/

U.S. DoJ, Bureau of Justice Administration (BJA) **National Training and Technical Assistance Center** (NTTAC) - connects state, local, and tribal justice agencies in need with specialized national experts to help address those needs. BJA NTTAC provides no-cost webinars, training, and technical assistance to the justice community based on their needs. Their website includes a searchable catalogue of services, events and training available to justice agencies.

- https://bjatta.bja.ojp.gov/tools

National Computer Forensics Institute (NCFI) - Free forensics training for state and local law enforcement, prosecutors and judges through funding from the federal government. Includes travel, lodging, equipment (in some classes), and course fees

- https://www.ncfi.usss.gov/ncfi/

Police Executive Research Forum (PERF) – Police research and policy organization and a provider of management services, technical assistance, and executive-level education to support law enforcement agencies.

- http://www.policeforum.org/

National Criminal Justice Training Center (NCJTC) – NCJTC offers a wide range of training and technical assistance programs that can be adapted and tailored to meet specific needs. Training is available online, in-house at your facility, or in one of NCJTC's many training facilities.

- https://ncjtc.fvtc.edu/training/

Criminal Intelligence Coordinating Council's (CICC) **Five in 5** - a weekly newsletter that highlights law enforcement and criminal-intelligence related articles, resources, and research that is relevant to CICC members and partners. The weekly focuses on promising practices, case studies, and success stories while also identifying products, reports, training and toolkits to enhance criminal intelligence capabilities.

- https://it.ojp.gov/global/working-groups/cicc