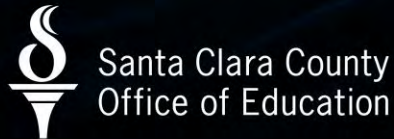


SECOND ANNUAL CYBERSECURITY SUMMIT 2024

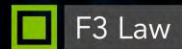
APRIL 25 • 9:00 A.M. - 3:30 P.M.



In Partnership with



Sponsored by



Emergency Evacuation Bowers Hall



Exit Doors (**Red Arrows**) are at:

- the back
- the side

of the Bowers Hall



Wi-Fi: The Tech Guest

(No password required)



**Restrooms are located to the right of
the Bowers Hall Main Entrance**

Leadership, Service, & Advocacy

County Superintendent of Schools



Dr. Mary Ann Dewan

County Board of Education



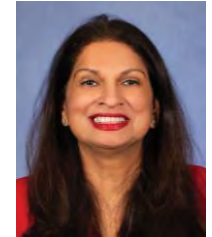
Maimona Afzal Berta
Area 6



Victoria Chon
Area 5



Joseph Di Salvo
Area 4



Raena Lari
Area 7



Grace Mah
Area 1



Don Rocha
Area 3



Tara Sreekrishnan
Area 2



Superintendent's Welcome

Mary Ann Dewan, Ph.D., County Superintendent of Schools



Introduction

David Wu, Head of Technology
Santa Clara County Office of Education



Why Me?

What Attackers Want & How They'll Get It

Keynote Speaker

Matt Linton, Chaos Specialist
Google

Why Me?

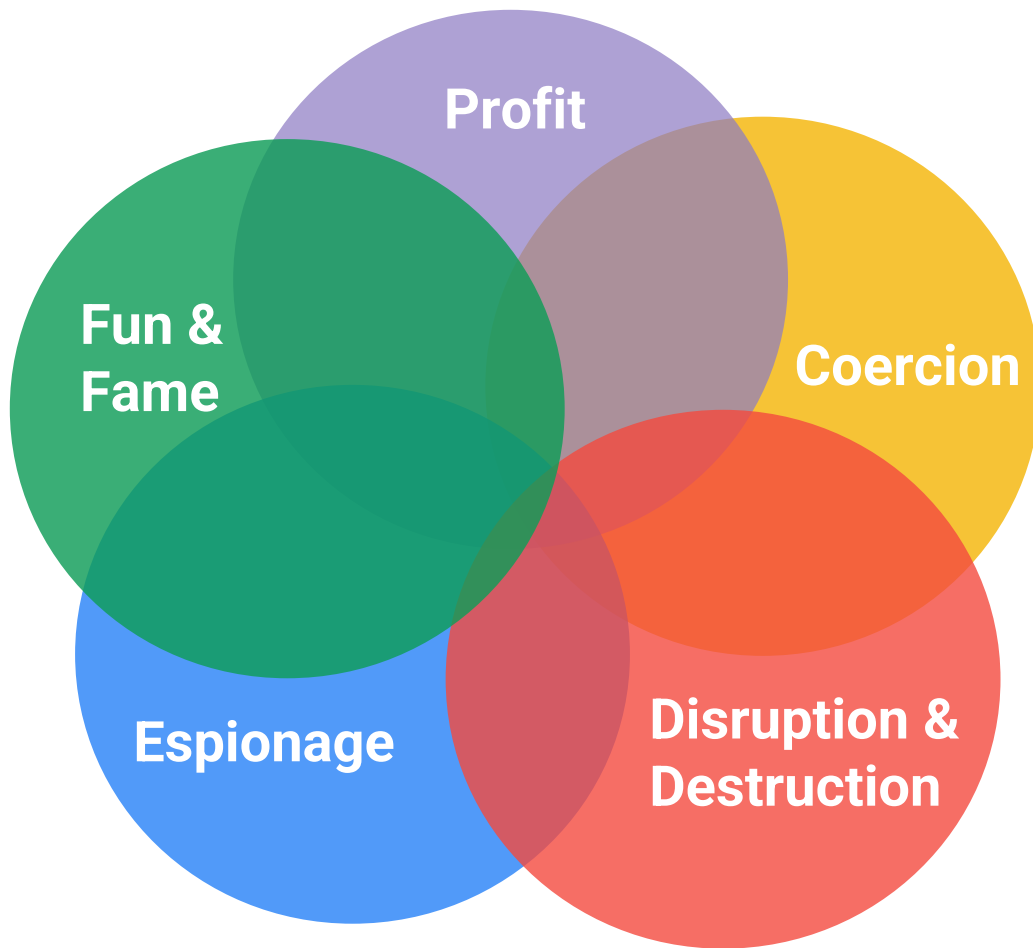
What attackers want
and how they'll get it

Matt Linton
Chaos Specialist

Google



Why They Hack



The attack lifecycle (very briefly)



The Attacker Ecosystem



Your Adversary



Access Brokers



Malware Vendors



Payment Intermediaries



Traffic Distribution Services



Data Abusers

Fun & Fame

For the lulz and the learning

Fun & Fame

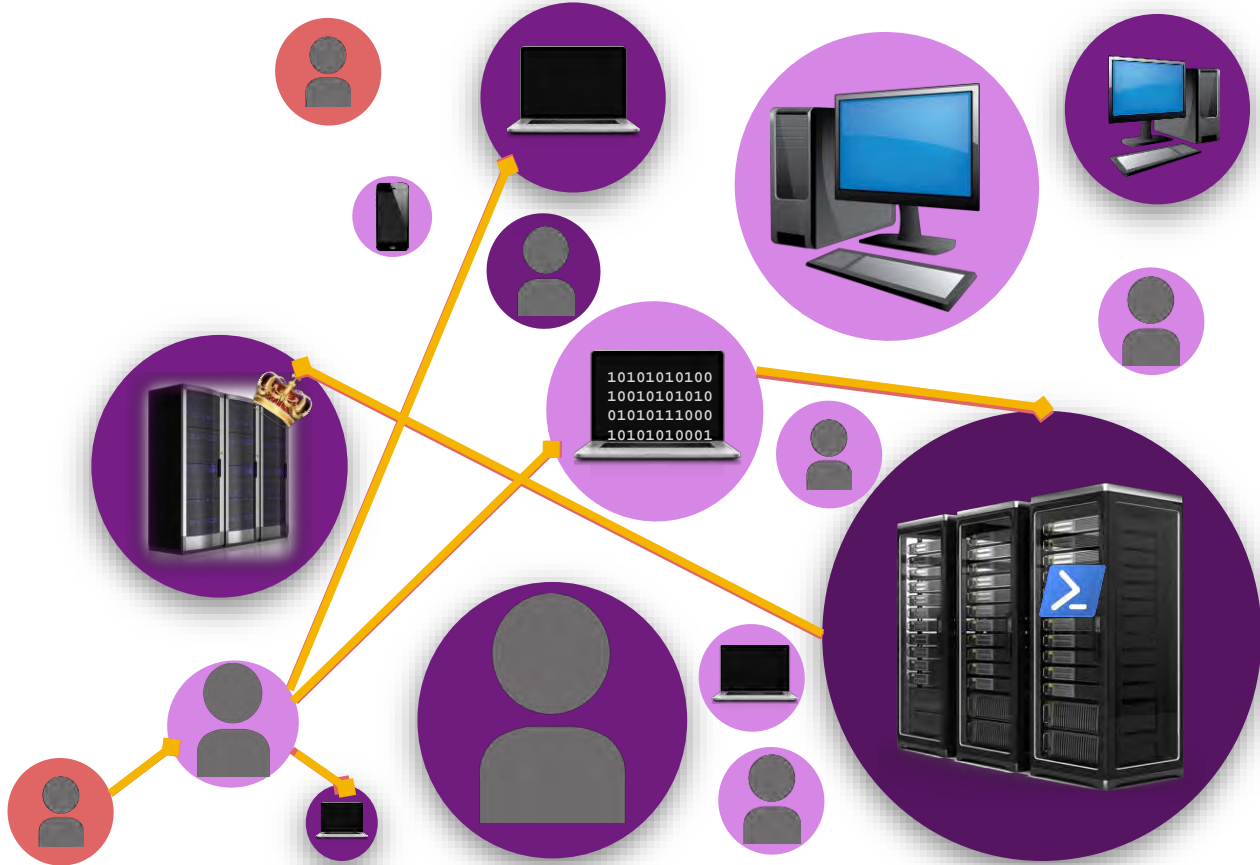
Loose collectives, typically including some performative or social reason for hacking.

In-group Cred; Notoriety; Fun



"Hackers" - United Pictures (1995)

Fun & Fame Case Study: Lapsus\$



Profit

– *exploitation or abuse to earn the attacker money*

Profit-motivated attackers

The New York Times

Cyberattack Forces a Shutdown of a Top U.S. Pipeline

The operator, Colonial Pipeline, said it had halted systems for its 5,500 miles of pipeline after being hit by a ransomware attack.

US Crime + Justice Energy + Environment More

Audio Live TV

Cybercriminals behind ransomware attack plan to release hacked data, Los Angeles Unified School District says

By Taylor Romine and Ray Sanchez, CNN

Published 11:29 AM EDT, Sat October 1, 2022

Thank you for your order, Here is your details

INVOICE NO.

INV13092022BBH

Product Details

NORTON 360

Order Summary

INVOICE NUMBER: INV13092022BBH
ISSUE DATE: 13 Sep 2022
Finish Date: 1 year from Start Date
Payment Mode: Auto debit from account
Status: Completed

PRODUCT NAME	Quantity	Grand Total
NORTON 360 (INV13092022BBH)	1	\$559.00 USD
	Sub-total	\$559.00 USD
	Discount	00.00
	Total	\$559.00 USD

If you wish to not to continue subscription and ask for a **Refund** then please feel free to call our **Refund & Settlement Dept.** as soon as possible!

You can Reach us on : **+1 - (650) - (265) - 7485**

Thank you!,

BILLING & SETTLEMENT DEPARTMENT

Coercion

*Get someone to do
something you
want them to do*

Coercion in action

The New York Times

China Appears to Warn India: Push Too Hard and the Lights Could Go Out

As border skirmishing increased last year, malware began to flow into the Indian electric grid, a new study shows, and a blackout hit Mumbai. It now looks like a warning.



@DFRLab

Apr 2, 2021 · 7 min read · Listen



Cyber-enabled information operation targets Poland with radiological leak hoax

Malicious actors carried out operation after U.S. company announced plans to invest in Poland's nuclear power program

Disruption / Destruction

*Incapacitate your
target or take
revenge*

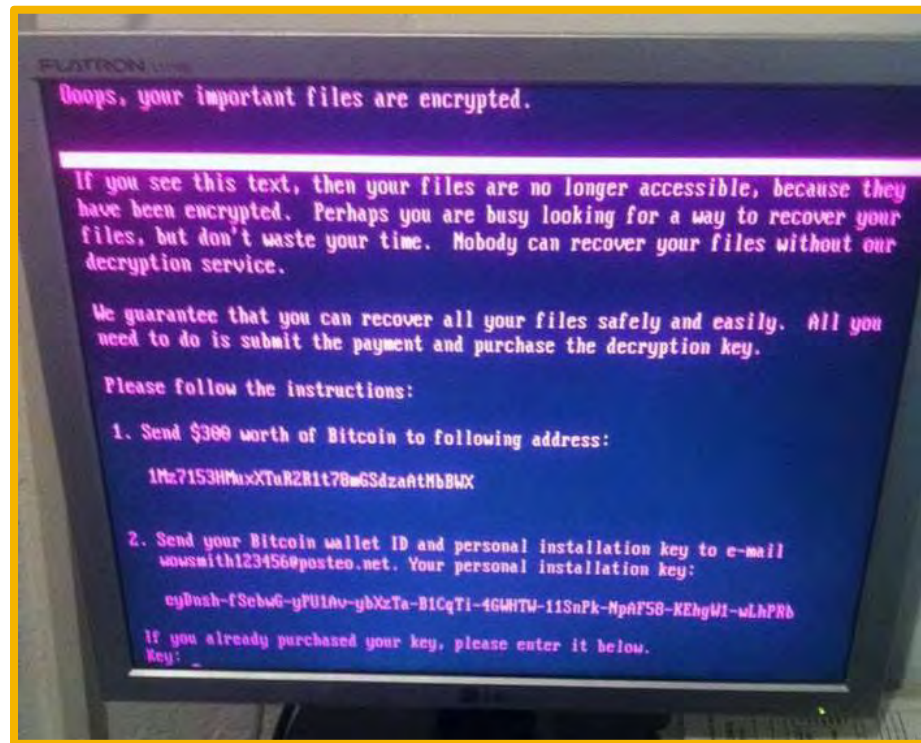
Disruption & Destruction

- Destroy, Sabotage, Destabilize
- Florida water treatment plant
- Spain's Radioactivity Alert Network



NotPetya

- When: 2017
- Who: Russia (Alleged)
- Why: Continue degrading Ukrainian capabilities
- Technique: Supply chain attack



Lessons from NotPetya

- Supply chain is increasingly critical part of conflict
- Geopolitical goals are common
- Collateral damage can be large
- Automation helps defend against malware, but also helps malware spread more quickly

New Weapon of War

Russian hackers allegedly target Ukraine's biggest private energy firm

By [Sean Lyngaas](#), CNN

Updated 10:32 AM EDT, Tue July 5, 2022

[HOME](#) > [MILITARY & DEFENSE](#)

Ukrainian hackers created fake profiles of attractive women to trick Russian soldiers into sharing their location, report says. Days later, the base was blown up.

Sophia Ankel Sep 5, 2022, 10:27 AM

PRO-RUSSIA hackers claim responsibility for intense, ongoing cyberattack against Lithuanian websites

By [Sean Lyngaas](#), CNN

Published 12:10 PM EDT, Mon June 27, 2022

Espionage

*Steal all the
secrets*

Espionage

- “Hacking Google” Episode 000
- “Hacking Google” Episode 002

Chinese hackers stole emails from US State Dept in Microsoft breach, Senate staffer says

By Raphael Satter and Zeba Siddiqui

September 27, 2023 7:41 PM PDT · Updated 2 months ago

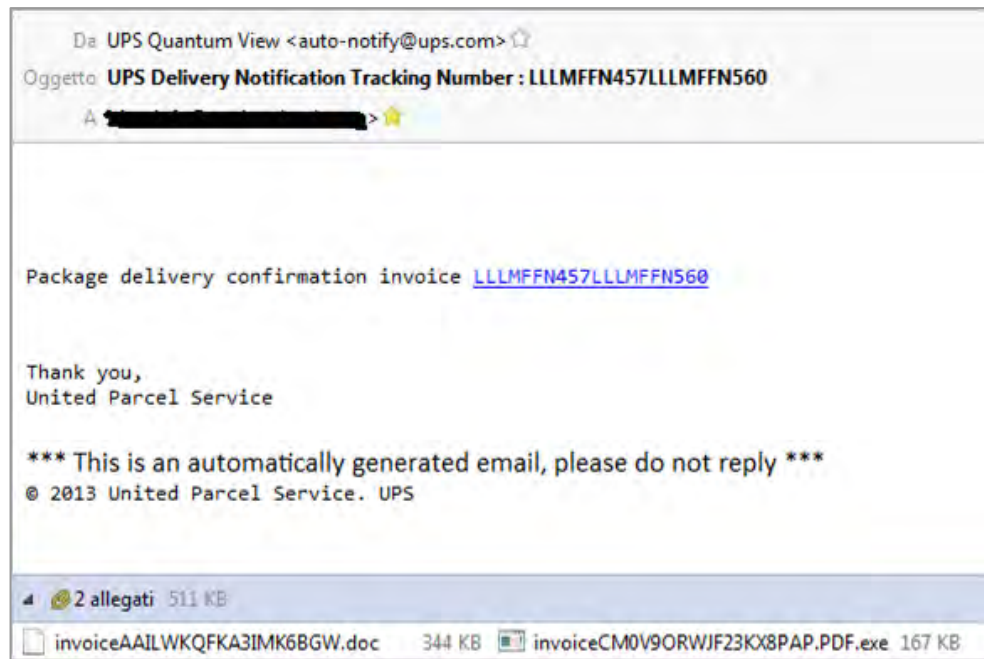


Have **you** ever experienced an attack or intrusion?

What do you have access to which someone might want?

Malicious Email, Chats, SMS, Calls....

- Your account & computer are valuable to an attacker!
- You're a link in that Lateral Movement chain



Phishing

Crafted emails, chats, SMS, etc that will try to get you to:

- Expose credentials (fake login page)
- Open attachments (malware)
- Run executables (ups_delivery.exe)
- Take actions (run Teamviewer, LogMeIn, Respond to IRS audit, send gift cards)

Social Engineering

- Attempts to get you to do things when attacker lacks access
- Fake tech support chats
- CEO impersonation
- Insistence that things happen right away or (\$consequence)
- ***Create a false sense of urgency or severity***

“Dad, I’m in jail! I need bail money immediately! Can you venmo it to the police?”

“Your tax payment will be considered criminally late in 24 hours! You can pay this tax bill with iTunes gift cards under a new apple partnership with the government...”

Software vulnerabilities

- Compromise publicly exposed things w/ known CVE's
 - Many have been known for months or years
- Find vulnerabilities in your custom code
- Follow vendor patch release cycles for “1-day bugs”

Supply-chain Attacks



(some) Supply Chain Attacks

- 2024: 'xz' backdoor Target: ???
- 2020: SolarWinds Target: .gov (esp)
- 2017: NotPetya Target: Ukraine (dst)
- 2017: CCleaner Target: .gov / Tech industry (?)
- 2013: Target Target: Target.(\$)

What can you do?

Advanced actor defenses

- Patch early & often; **Turn on auto-updates**
- Use your OS provider's defenses ahead of third-parties
 - E.g, Windows Defender, not third-party AV
- Collect & store logs for investigation if something happens
- **Detection & Response** are an equal partner in security!

Phishing Defenses

- Use a password manager!
 - Different passwords for every site (credential stuffing defense)
- Stop forcing “password rotation”; use strong unique passwords instead
- Encourage people to report phishing so D&R can check in
- Stop performing hostile “Phishing Exercises”
 - You cannot train employees to be immune to phishing
 - These trainings are counterproductive

Social Engineering Defenses

Organizational:

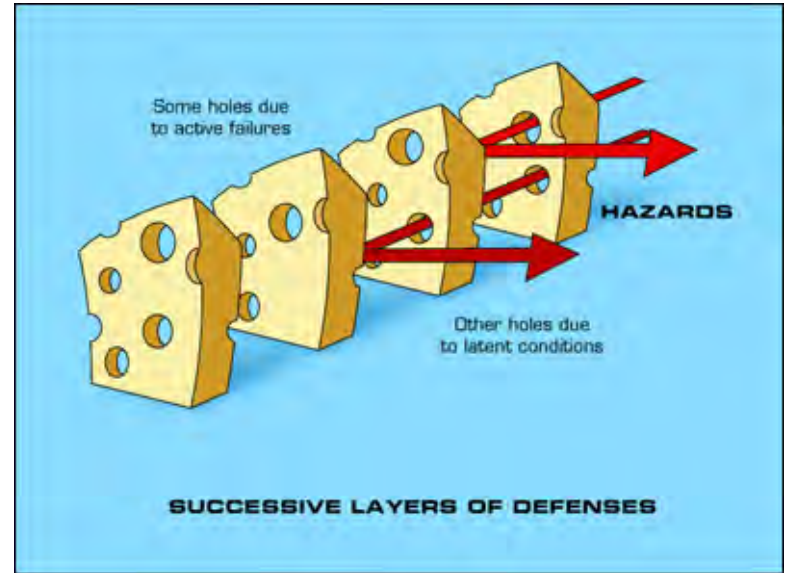
- Support staff by ensuring your own org's procedures are clear and understandable
- Document official channels for things (e.g, the tech support chat address)
- **Create a blameless security culture so people will report if they were fooled!**

Individual:

- Don't engage with false senses of urgency
- Validate through back-channels (e.g, call the CEO's office to verify)
- Skepticism is key
 - "Hey wait, when is the IRS ever this helpful?"

Failure is inevitable; Detection & Response are key

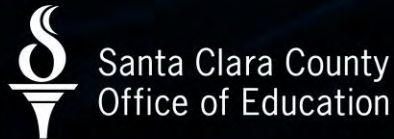
- Everyone will ultimately fail at some point
- You'll fail at different points than your co-workers
- Report things as soon as you realize they've happened
- Blameless culture is key



Q & A

SECOND ANNUAL
CYBERSECURITY
SUMMIT 2024

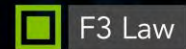
APRIL 25 • 9:00 A.M. - 3:30 P.M.



In Partnership with



Sponsored by





Cyber Insurance 101:

What is the Current Cyber Threat Landscape & how does Cyber Insurance Assist

Brandon Welch, Cyber Services Team Leader – West Cyber Risks
Beazley

beazley

Cyber Insurance 101

04/25/2024



Agenda



Cyber Insurance Coverages



Cyber Threat Landscapes



How to Prepare for a Data Security Incident?



Q+A

01

Cyber Insurance Coverages

Trends and Threat Intel

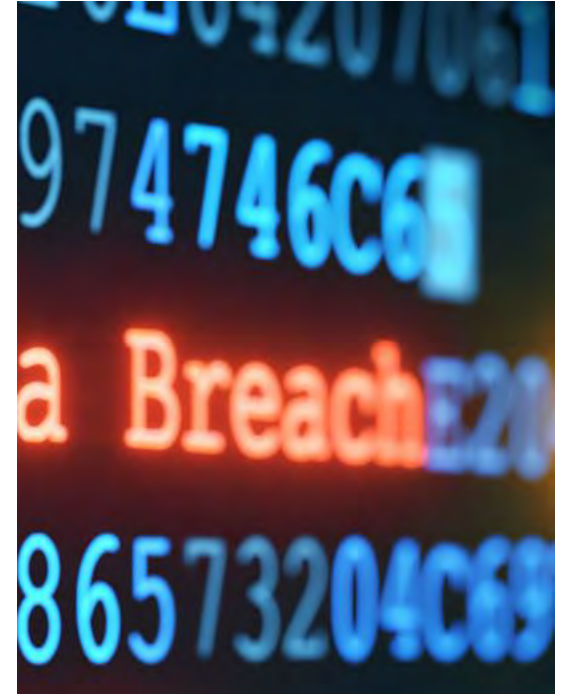
First Party – Breach Response Services

Purpose

- Respond and Contain
- Investigate
- Compliance

Specific services

- Privacy Counsel
- Digital Forensics/Incident Response
- Crisis Management
- Notification/Call Center/Credit Monitoring



First Party – Other types of Coverages

Data Recovery
Cyber Extortion
Business Interruption



Third Party – Defense Counsel



02

Cyber Threat Landscape

Cyber Threats – Explanations and Examples

Ransomware – Explanation

Group behind Oakland, Calif., ransomware posts second, bigger data dump

It's the second time hackers have leaked data stolen from the city, and now police officers are demanding compensation.

BY BENJAMIN FREED • APRIL 5, 2023



Oakland

- United States
 - www.oaklandca.gov
- views: 1036
- amount of data: ??? gb
- added: 2023-03-01
- publication date: 2023-03-04

information: Oakland is the largest city and the county seat of Alameda County, California, United States. A major West Coast port, Oakland is the largest city in the East Bay region of the San Francisco Bay Area, the third largest city overall in the Bay Area and the eighth most populated city in California.

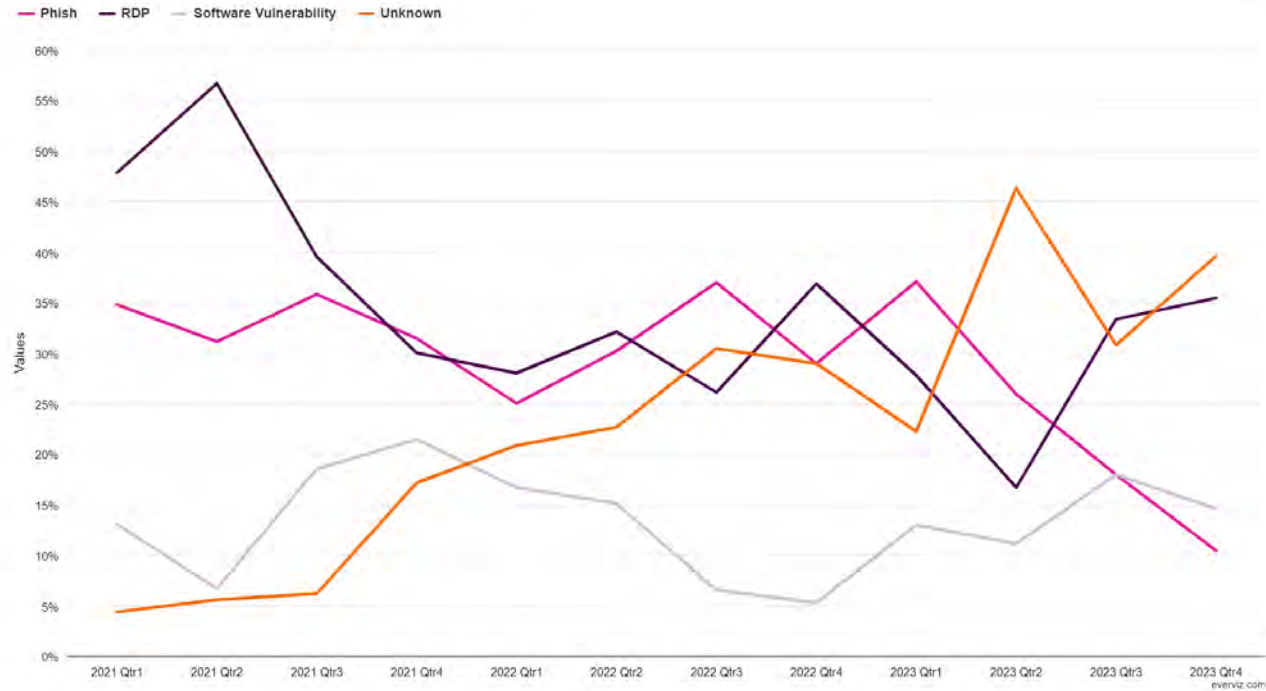
comment: Private and personal confidential data, financial information. IDs, passports, employee full info, human rights violation information. For now partially published compressed 10gb. If there no reaction full dump will be uploaded. Each of the archives can be used independently.

DOWNLOAD LINKS <https://134e4a2d-0j8t7evvzhfveqjdygF0ubdy60u23hce84f8d.onion/jk>
For password: 1x1R4*81PWE!P4Xg0T4s

PUBLISHED

Ransomware – Threat Vectors

Ransomware Vectors



Ransomware – Claims Example

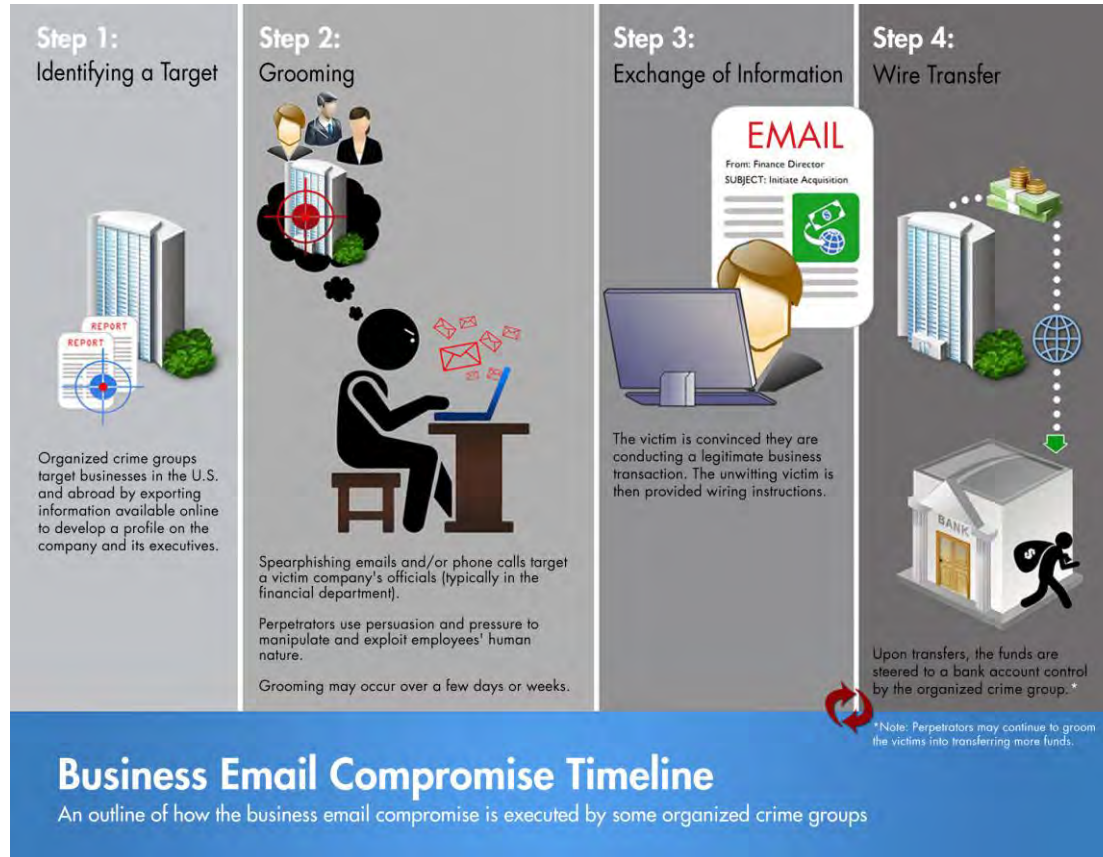


Incident: Ransomware Attack

Response: Privacy Counsel, Digital Forensics/Incident Response, PR/Crisis Management, and Ransomware Negotiation

Costs: Breach Response Services, Ransom, Downtime, Third Party Investigations

Business Email Compromise – Example and Explanation



Business Email Compromise – Example

An employee of a large school district who regularly handles the personal information of other school district employees had his email compromised. The Email inbox had several years of data. The insured engaged breach response Services to respond to the incident, investigate, and ensure that any obligations were handled. Due to the high amount of data in the email inbox, data mining was required to understand whose information was exposed. The district had to notify 3500 individuals.



Third Party Data Security Incident – Explanation



Third Party Data Security Incident - Examples



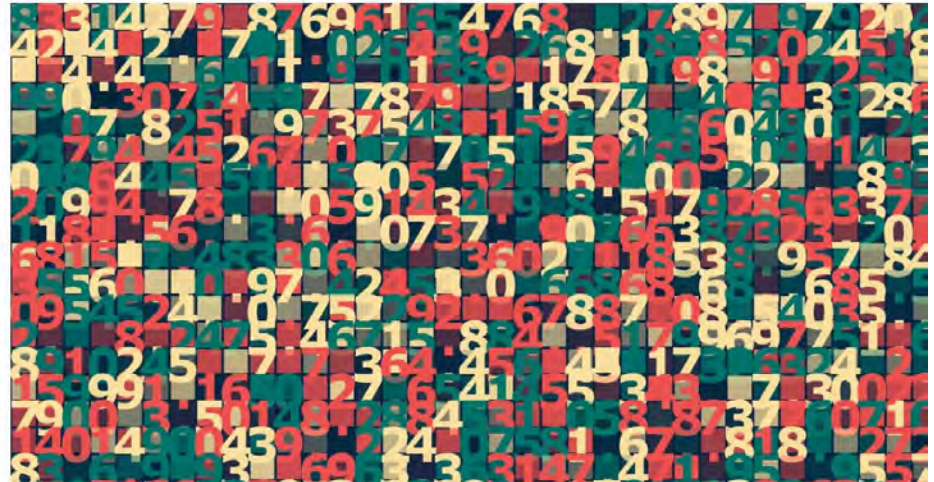
Featured Article

MOVEit, the biggest hack of the year, by the numbers

At least 60 million individuals affected, though the true number is far higher

Carly Page @carlypage_ / 8:45 AM PDT • August 25, 2023

 Comment



04

How to Prepare for a Data Security Incident?

Next Action Steps

Incident Response Plan

Plan for a Data Security Incident – It's not a matter of if, but when.

An Incident Response Plan (IRP) should provide for the following:

Scope – What does your Incident Response Plan response to?

Escalation Path – Who to notify and when?

Internal Individuals/Roles – Who owns what workstreams/processes?

External Individuals/Roles – Who can assist us/bolster our response?

Chain of Custody Issues – Documentation

Consult with legal professionals over this plan as there may be legal requirements.



Closing Comments

1. Free Resources – CISA, CAL OES, the Insurance Carrier!
2. If a member of your team thinks there's a problem, there may be!
3. Use your Incident Response Plan! It is an emergency plan, so it should be reviewed and updated like other disaster planning

05

Q+A

Thank you!



Marcelo Quiñones
Lead Deputy



AI and Cybersecurity, a Legal Perspective and Guide for Education Leaders

Marcelo Quiñones, Lead Deputy County Counsel
Tara Fonseca, Deputy County
Office of the County Counsel, County of Santa Clara



AI AND CYBERSECURITY: A LEGAL PERSPECTIVE AND GUIDE FOR EDUCATION LEADERS

MARCELO QUIÑONES, LEAD DEPUTY COUNTY COUNSEL
TARA FONSECA, DEPUTY COUNTY COUNSEL



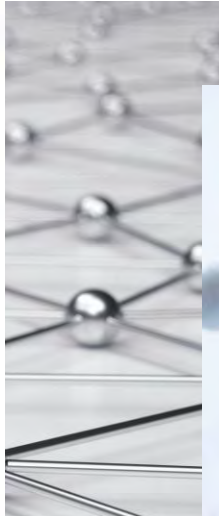
WHAT IS GENERATIVE AI?

- A form of artificial intelligence in which algorithms produce new content in the form of text, images, audio, and video in response to a prompt submitted by a user
- Leverages large language models (LLM) that have been trained on vast amounts of data (usually scraped from the internet)
- Predicts next word or pixel based on the probability of it occurring in the training data
- Examples: ChatGPT, Dall-E, Bard, Midjourney, Jasper

PRIVACY AND DATA SECURITY

Why is privacy and data security important in the context of AI?

Given the large amount of data needed to train AI systems, the automating nature of algorithms and the scalability in its applications, the use of AI raises important questions in relation to personal data, data protection and privacy.



PRIVACY AND DATA SECURITY: EXISTING LEGAL LANDSCAPE

What laws are relevant to the confidentiality of data shared with AI systems?

- Family Educational Rights & Privacy Act (and analogue in Education Code)
- Children's Online Privacy Protection Rule
- Protection of Pupil Rights Amendment (if applicable)
- Potentially applicable requirement related to contracts with technology providers (EC 49073.1)
- Individuals with Disabilities in Education Act (IDEA) for uses with students with disabilities



POTENTIAL USES OF AI SYSTEMS

- Student teaching (student-facing)
- Student supporting (student-facing)
- Teacher supporting (teacher-facing)
- System supporting (system-facing)



SHARING INFORMATION WITH AI SYSTEMS

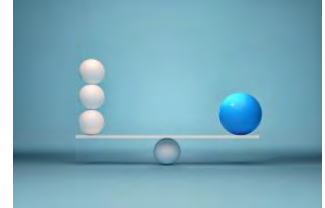
- **Assess application of FERPA**

- “Education record” to which FERPA applies are records that are:
 - Directly related to a student; and
 - Maintained by the school district or by a party acting for the school district.
- Until specific AI guidance promulgated, consider U.S. Department of Education approach in applying FERPA to new technologies (e.g., online educational services and video)



- **Authority to share education records with AI systems**

- **Consent**
 - Consent must be knowing and voluntary (i.e., cannot compel parents to waive FERPA rights)
- **“School officials” exception** authorizes sharing of PII from education records, without consent, if contractors:
 1. Perform **institutional service** or function for which the school or district would otherwise use employees;
 2. Meet the school district’s criteria for being considered a school official with a legitimate educational interest (as outlined in annual FERPA notification);
 3. Perform services under the **direct control** of the school district; and
 4. Are subject to limitations on use of **PII and redisclosure**.
- **Directory information** permits sharing of limited information that is generally considered less sensitive if it is properly designated as directory information



USE AND REDISCLOSURE OF EDUCATION RECORDS BY AI SYSTEM PROVIDERS



Limitations on use

- Providers may use data only for the purpose(s) for which the disclosure was made

Redisdisclosure limitation

- Redisdisclosure must be authorized by consent or an exception
 - Consent
 - School official exception
 - De-identified records and information
 - Removal of all personally identifiable information
 - Reasonable determination that student's identity is not identifiable through single or multiple releases and considering reasonably available information

Recordkeeping requirements

- Record names of additional parties to which information may be disclosed and the legitimate interest of each additional party

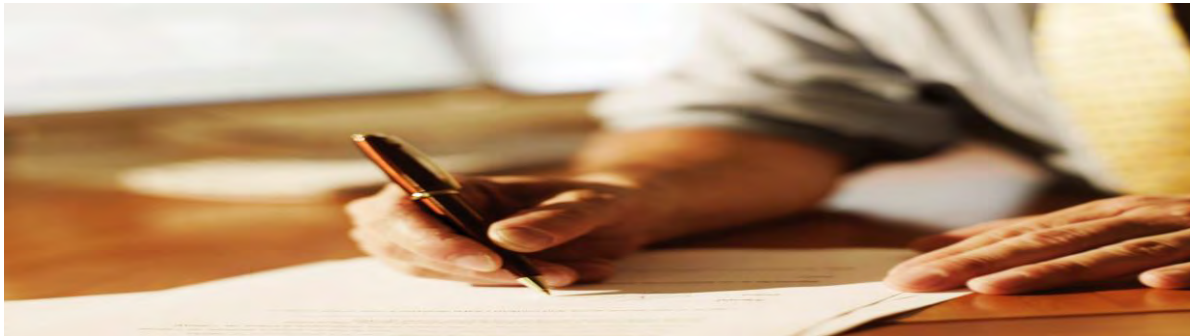
ENSURING LEGALLY REQUIRED ACCESS TO RECORDS

- Rights of parents to access education records
 - When education records will be held in an AI system, districts should also consider how they will comply with parents' right of access to education records Parents have the right to inspect and review education records
 - If circumstances effectively prevent inspection, district must either provide copies or make arrangement for parent to inspect and review
- What about access to non-education records?
 - Consider California Public Records Act application



CHILDREN'S ONLINE PRIVACY PROTECTION ACT

- Specific requirements for operators of websites or online services that collect, use, or disclose personal information from children under 13 years of age
- Providers must obtain verifiable parental consent
- Schools may consent on behalf of parents if the education technology service provides the school with COPPA-mandated data collection notices and practices



OTHER PLANNING RESOURCES & INSIGHTS FOR POTENTIAL FUTURE REGULATION

- White House Blueprint for AI Bill of Rights

- Outlines a framework for addressing privacy in sensitive domains, like education
- Ethical review and monitoring of any use of sensitive data or decision process that may limit rights, opportunities, or access
- **Narrow access:** Limit access to sensitive data and derived data: sensitive data, including any data that can be used to infer sensitive information, should not be sold, shared, or made public
 - Limit access to data based on necessity and local control (e.g., teacher granted access to daily progress data while district administrators (depending on role and need) may not have access
- **Data breach reporting:** require reporting of any breaches that resulted in sensitive data leaks or other data security lapses



CONSIDERATIONS FOR LIMITING RISK

- Data collection
 - Limited use of data: sensitive data should only be used for functions strictly necessary for that domain or that are necessary for administrative purposes
 - Data collection should be limited to extent feasible and clearly communicated to those whose data is collected
 - Data should only be collected for training or testing machine learning models if the collection and use is legal and consistent with the expectations of families
 - Data collection should be limited in scope and based on specific, narrow goals
 - Consider the availability of procedures to ensure that sensitive data is kept anonymous



CONSIDERATIONS FOR LIMITING RISK

- Data retention
 - Ensure clear timelines for retention of data, particularly student data
 - Data should be deleted as soon as possible (in alignment with any legal or policy-based limitations)
 - Document and justify data retention timelines
- Transparency
 - Are learners/families and teachers informed about what happens to their data, how it is used, and for what purposes?
- Privacy and data settings
 - Does the AI system make it possible to customize privacy and data settings?

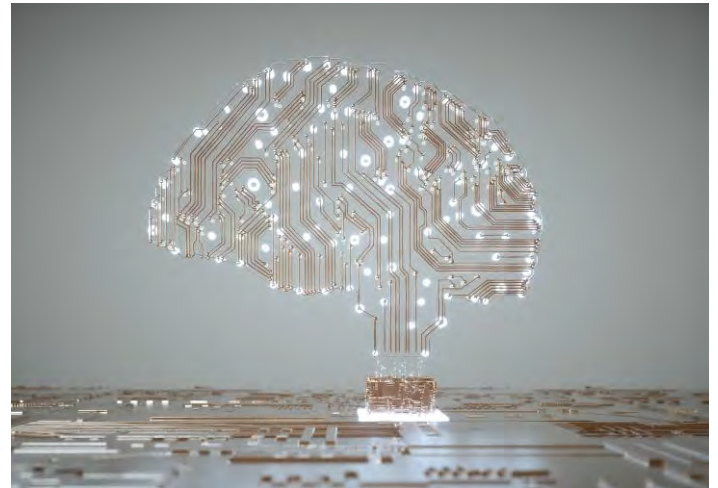
REVIEWING AI SYSTEM PROVIDERS

- Considerations for contractors to support LEA's compliance
 - Review the data that will be shared with AI systems
 - Categories of student records: review student data elements to be shared.
 - If there are education records, will directory information or the school officials exception authorize sharing? If not, will consent be voluntary and how will parents' withholding of consent impact educational services?
 - Sensitivity: consider the sensitivity of information to be shared.
 - Sources of student information: how is the information collected?
 - Redisclosure: what data will be redisclosed by the contractor and for what purpose?
 - Parent access to records
 - Does the AI system enable the school district to comply with the right of access to education records for parents (and right of public to access public records as applicable)?

PRIVACY AND DATA SECURITY

Generative AI

- Concern regarding use of prompts to train the model



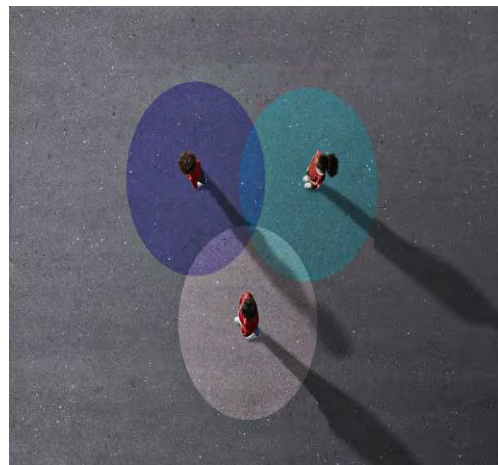
CAREFUL REVIEW OF TERMS OF USE

- **Highlighted terms**

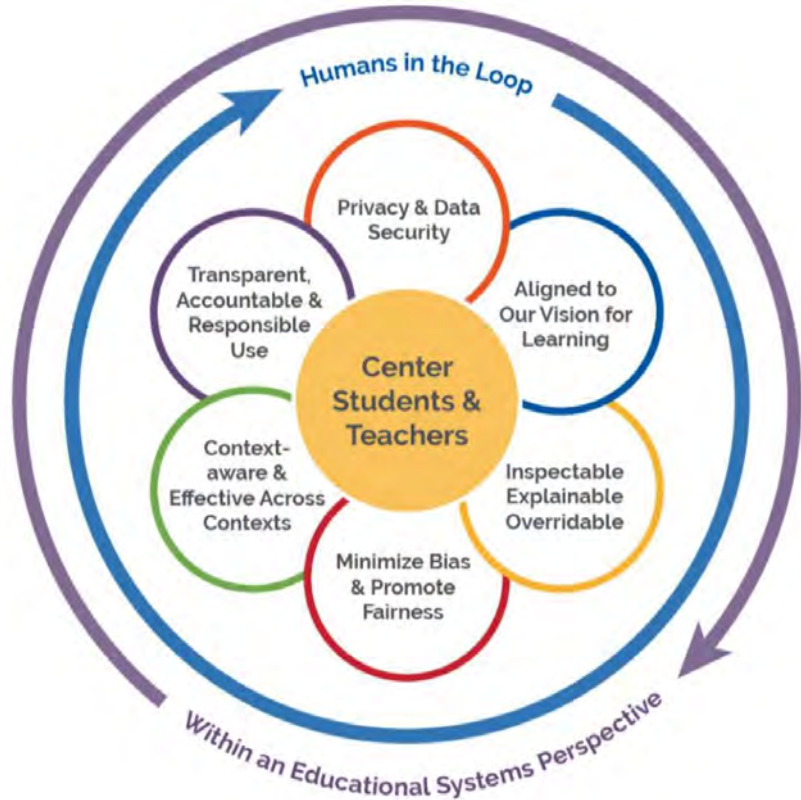
- Microsoft Copilot AI Experiences Terms: <https://www.bing.com/new/termsfuse>
- ChatGPT Terms of Use: <https://openai.com/policies/terms-of-use>
- Fetchy Blog: <https://www.fetchy.com/blog/fetchy-and-ai>
- Ivy Online Subscription Agreement: <https://ivy.ai/iosa>

- **Exercise**

- At your table, please review the terms of use on the printout at your table. Talk amongst your group:
 - What stands out from the different terms?
 - Compare and contrast the terms. What is similar? What is different across companies?
 - Share any other reactions to the terms



COORDINATED REVIEW OF NEW GENERATIVE AI TOOLS BEFORE PROCUREMENT AND USE





GENERATIVE AI SECURITY RISKS

- Create new and more complex malware that can bypass conventional detection methods and that adapts/evolves based on target environment
- Develop advanced evasion techniques to bypass security measures (e.g., intrusion detection systems and endpoint security)
- Create more convincing phishing campaigns, including pictures and video
- Launch distributed denial of service attacks
- Use previously leaked passwords to mimic patterns and guess password variants



GENERATIVE AI SECURITY RISKS

- Risk mitigation and response
 - Cyber insurance that covers third-party liability losses
 - Security review of new generative AI tools before procurement and use
 - Advanced endpoint protection – leverages machine learning AI within endpoint security to detect threats and anomalies
 - Recovery plans for data and computer systems



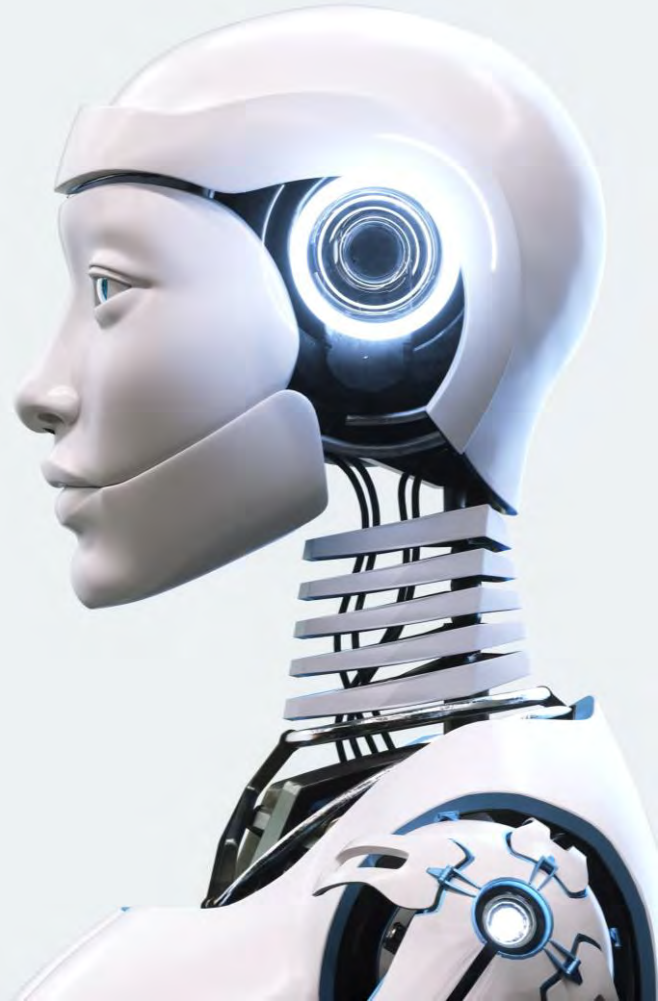
DEEPPFAKES

- Increasingly realistic mimicry of voice, image, and video
 - Face swap
 - Lip synching
 - Puppet technique
- Risks
 - Cyber bullying
 - Extortion
 - Financial fraud
 - Social engineering scams



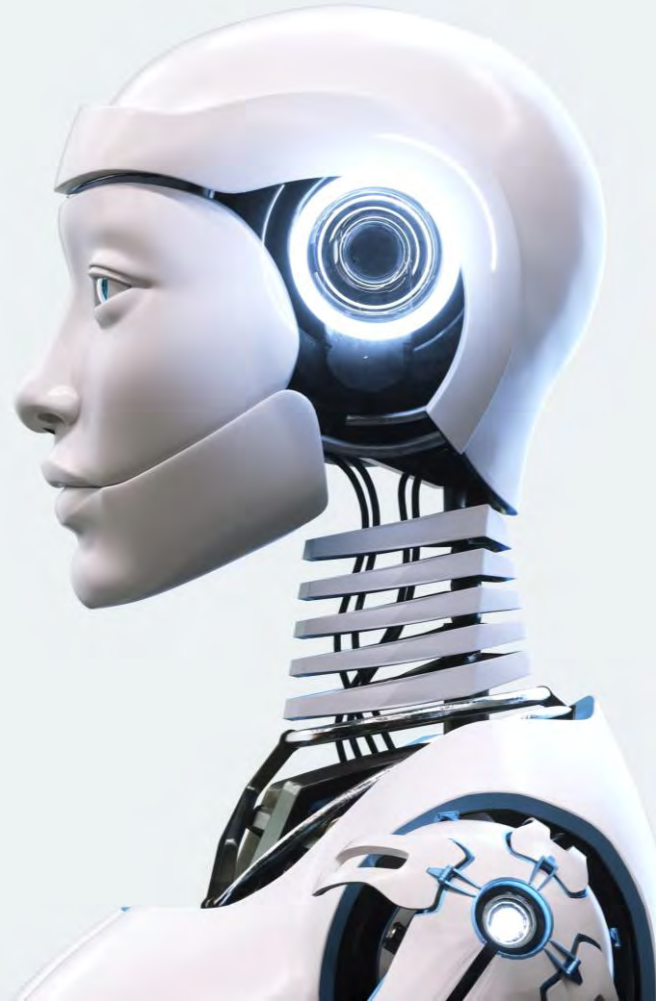
DEEPPFAKES

- Risk mitigation and response
 - Watermarks and security codes/passwords
 - Prohibition on replicating a person's voice or image
 - Independent verification before taking action
 - Training and awareness
 - Pending California legislation
 - AB 1873: criminalizes development, duplication, printing, and exchange of generative AI images depicting a person under 18 engaged in sexual conduct
 - AB 1872: criminalizes threatening to post, distribute, or create AI-generated images/videos of another
 - Cyber Civil Rights Initiative's Image Abuse Helpline



OTHER GENERATIVE AI RISKS/CONCERNS

- Hallucinations – inaccurate/false information
- Outdated information
- Bias and discrimination
- Copyright and other IP infringement
- Public records



RISK MITIGATION FOR GENERATIVE AI

- Human review for accuracy and bias/discrimination and acceptance of responsibility for use of generative AI
- Prohibition on using generative AI for decision-making
- Transparency – disclose whenever generative AI is used (e.g., by adding a disclaimer or watermark)
- Review terms of use related to ownership of output and indemnification for copyright infringement
- Establish retention and disclosure policies for prompts and outputs consistent with relevant laws governing records



POLICY AND USE GUIDELINES

- Jurisdictions in California and across the United States have adopted policies/guidelines for their staff on the proper use of generative AI following the release of ChatGPT in November 2022
- Some have adopted internal processes to review new generative AI use cases and tools prior to procurement and/or use
- Others allow for use of public generative AI tools subject to the terms of the policies/guidance

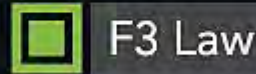
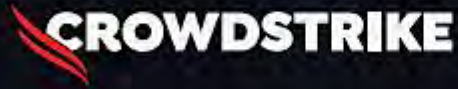


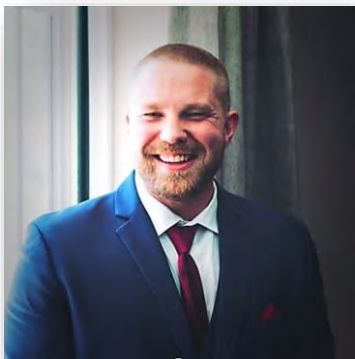
QUESTIONS?

Networking Lunch

Sponsored by

proofpoint.





CISA – Safeguarding K-12

Scott Alford, Cybersecurity Advisor
CISA

CYBERSECURITY SERVICES FOR BUILDING CYBER RESILIENCE

Scott Alford

CISA Cybersecurity Advisor – Monterey, San Benito,
South Bay & Santa Cruz County
Cybersecurity Advisor Program
Cybersecurity and Infrastructure Security Agency

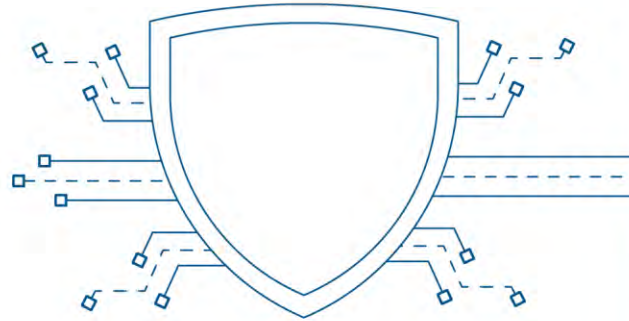
Cell: +1 (202) 285-9621
Teams: +1 (771) 208-1989
Email: scott.alford@cisa.dhs.gov

Spring 2024





Cybersecurity Mission

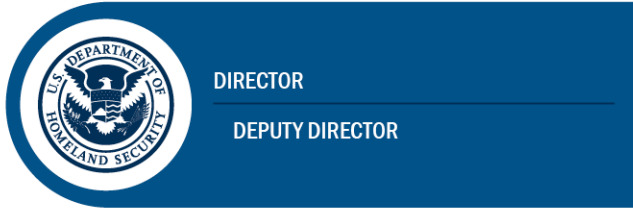


CISA's Cybersecurity Division leads the national effort to reduce the prevalence and impact of cyber incidents by providing services, guidance, and capabilities that address immediate risks and advance toward a secure cyber ecosystem.

HOW CISA IS CARRYING OUT ITS CYBERSECURITY MISSION:

- ▶ Catalyze Persistent Collaboration Across Government and the Private Sector
- ▶ Expand Operational Visibility into Threats and Vulnerabilities
- ▶ Drive Prioritization and Measure Adoption of the Most Effective Security Measures
- ▶ Serve as the Operational Lead for Federal Civilian Cybersecurity
- ▶ Advance a Technology Product Ecosystem that is Secure by Design and Default

Cybersecurity & Infrastructure Security Agency



EMERGENCY COMMUNICATIONS
DIVISION



NATIONAL RISK MANAGEMENT
CENTER (NRMCC)






CYBERSECURITY DIVISION



INFRASTRUCTURE
SECURITY DIVISION

16 Critical Infrastructure Sectors & Corresponding Sector Risk Management Agencies

 CHEMICAL	CISA	 FINANCIAL	Treasury
 COMMERCIAL FACILITIES	CISA	 FOOD & AGRICULTURE	USDA & HHS
 COMMUNICATIONS	CISA	 GOVERNMENT FACILITIES	GSA & FPS
 CRITICAL MANUFACTURING	CISA	 HEALTHCARE & PUBLIC HEALTH	HHS
 DAMS	CISA	 INFORMATION TECHNOLOGY	CISA
 DEFENSE INDUSTRIAL BASE	DOD	 NUCLEAR REACTORS, MATERIALS AND WASTE	CISA
 EMERGENCY SERVICES	CISA	 TRANSPORTATIONS SYSTEMS	TSA & USCG
 ENERGY	DOE	 WATER	EPA

CISA Central

CISA Central is CISA's hub for staying on top of threats and emerging risks to our nation's critical infrastructure, whether they're of cyber, communications or physical origin:

CYBER RESOURCE HUB

- RVA Mapped to the MITRE ATT&CK Framework Infographic
- Vulnerability Scanning
- Phishing Campaign Assessment
- Risk and Vulnerability Assessment
- Cyber Resilience Review (CRR)
- CRR Downloadable Resources
- External Dependencies Management Assessment (EDM)
- EDM Downloadable Resources
- Cyber Infrastructure Survey
- Remote Penetration Testing
- Web Application Scanning
- Cyber Security Evaluation Tool (CSET®)
- Validated Architecture Design Review (VADR)



Protective Security Advisors



SURVEYS AND ASSESSMENTS

PSAs conduct voluntary, non-regulatory security surveys and assessments on critical infrastructure assets and facilities within their respective regions.



OUTREACH ACTIVITIES

PSAs conduct outreach activities with critical infrastructure owners and operators, community groups, and faith-based organizations in support of CISA priorities.



SPECIAL EVENT SUPPORT

PSAs support Federal, State, and local officials responsible for planning, leading, and coordinating NSSE and SEAR events.



INCIDENT RESPONSE

PSAs plan for and, when directed, deploy in response to natural or man-made incidents.



BOMBING PREVENTION AND AWARENESS

PSAs work in conjunction with CISA's Office for Bombing Prevention by coordinating training and materials for partners to assist in deterring, detecting, preventing, protecting against, and responding to improvised explosive device threats.



Edgar S. Castor, CPP

Protective Security Advisor
Region 9: San Francisco District
Phone/Text: (202) 309-0715
Email: edgar.castor@hq.dhs.gov

Justin L. Brooks

Protective Security Advisor
Region 9: San Jose District
Phone/Text: (202) 819-6511
Email: justin.brooks@hq.dhs.gov

Christopher Reidel

Protective Security Advisor
Region 9: Sacramento District
Phone/Text: (207) 400-2769
Email: christopher.reidel@cisa.dhs.gov

Cybersecurity Advisor

To provide direct coordination, outreach, and regional support and assistance in the protection of cyber components essential to the Nation's Critical Infrastructure.

- **Assess:** Evaluate critical infrastructure cyber risk
- **Promote:** Encourage best practices and risk mitigation strategies
- **Build:** Initiate, develop capacity, & support cyber communities
- **Educate:** Inform and raise awareness
- **Listen:** Collect stakeholder requirements
- **Coordinate:** Bring together incident support and lessons learned



CISA CYBERSECURITY ADVISOR PROGRAM



Cybersecurity Services

- Cybersecurity Advisors
- State, Local, Tribal, and Territorial engagements
- Cyber Education and Awareness
- Federal Virtual Training Environment (Fed VTE)
- National Initiative for Cybersecurity Careers and Studies (NICCS)
- Stop. Think. Connect.™
- Cybersecurity Awareness Month
- .gov Domain
- Request a CISA Speaker
- Biweekly Threat Briefing
- Information / Threat Indicator Sharing
- Known Exploited Vulnerabilities Catalog
- Resource Guides
- Cyber Incident Response Tabletop Exercise (TTX)
- Advanced Malware Analysis Center
- Cyber Performance Goals (CPG)
- Ransomware Readiness Assessment (RRA)
- Cyber Resilience Reviews (CRR™)
- External Dependencies Management (EDM) Assessments
- Cyber Infrastructure Survey
- Cyber Security Evaluation Tool (CSET™)
- Cyber Hygiene Services
 - Vulnerability Scanning
 - Web Application Scanning (WAS)
 - Ransomware Vulnerability Warning Pilot (RVWP)
- Risk and Vulnerability Assessment (RVA)
- Validated Architecture Design Review (VADR)
- CyberSentry*
- Protective DNS*
- Secure Cloud Business Applications (SCuBA)
- Logging Made Easy (LME)



Sampling of Cybersecurity Offerings

• Preparedness Activities

- Information / Threat Indicator Sharing
- Cybersecurity Training and Awareness
- Cyber Exercises and “Playbooks”
- National Cyber Awareness System
- Vulnerability Notes Database
- Information Products and Recommended Practices
- Cybersecurity Evaluations
 - Cyber Resilience Reviews (CRR™)
 - Cyber Infrastructure Surveys
 - Phishing Campaign Assessment
 - Vulnerability Scanning
 - Risk and Vulnerability Assessments (aka “Pen” Tests)
 - External Dependencies Management Reviews
 - Cyber Security Evaluation Tool (CSET™)
 - Validated Architecture Design Review (VADR)

• Response Assistance

- Remote / On-Site Assistance
- Malware Analysis
- Hunt and Incident Response Teams
- Incident Coordination

• Cybersecurity Advisors

- Assessments
- Working group collaboration
- Best Practices private-public
- Incident assistance coordination

• Protective Security Advisors

- Assessments
- Incident liaisons between government and private sector
- Support for National Special Security Events



CISA Cybersecurity Offerings

Cybersecurity Advisor Facilitated

Cybersecurity Assessments

- Cyber Performance Visit (**CPV**)
- Cyber Performance Goals (**CPG**)
- Cyber Infrastructure Survey (**CIS**)
- External Dependencies Management (EDM)/Cyber Resilience Review (**EDM/CRR**)
- CISA Tabletop Exercise Package (**CTEP**)
- Cyber Hygiene (**CyHy**):
 - Vulnerability Scanning (**VS**)
 - Web Application Scanning (**WAS**)
- Cybersecurity Evaluation Tool (**CSET**)
 - Ransom Readiness Assessment (**RRA**)

HQ Vulnerability Team Facilitated

- Validated Architecture Design (**VADR**)
 - Remote Penetration Testing (**RPT**)
 - Risk & Vulnerability Assessment (**RVA**)
 - Phishing Campaign Assessment (**PCA**)
- No longer available**

CISA HQ Response Assistance

- Remote / On-Site Assistance
- Malware Analysis
- Hunt and Incident Response Teams
- Incident Coordination

California Based Protective Security Advisors

- Physical Security Assessments
- Incident liaisons between government and private sector for CI protection



Process Management and Improvement

Cybersecurity and Infrastructure Security Agency (**CISA**)

EMAIL: vulnerability@cisa.dhs.gov

ASSESSMENTS



Criticality of Periodic Assessments

- Periodic assessments are essential for resilience
- Can't protect if you don't know what needs protection
- Can't fix what needs if you don't know what's wrong



Range of Cybersecurity Assessments



Protected Critical Infrastructure Information Program

Protected Critical Infrastructure Information (PCII) Program Guards Your Information


- Sensitive critical infrastructure information voluntarily given to CISA is protected by law from
 - Public release under Freedom of Information Act requests,
 - Public release under State, local, tribal, or territorial disclosure laws,
 - Use in civil litigation and
 - Use in regulatory purposes.




CYBER PERFORMANCE GOALS



CPG's



CPG
Cross-Sector Cybersecurity
Performance Goals
2022



**PERFORMANCE
GOALS**

IDENTIFY (1)				
CPG Identifier	CPG Title	Current Assessment	Year 1 Assessment	Notes
5.A Asset Inventory	5.A.M.1, 5.A.M.2, 5.A.M.3, 5.A.M.4, 5.A.M.5, 5.A.M.6, 5.A.M.7			
GOALS: 5.A.1 - IMPACT HIGH COMPLEXITY LOW	TOP 20 RISK ADDRESSED: INTEGRAL, TECHNICAL, AND PROCEDURAL (IT) RISK ADDRESSED: Insecure Software (75.00%) Paper/Pencil/Handwritten Approvals (7.00%) Data Breach/Leak (6.00%) System Outage (5.00%)	DATE: _____	DATE: _____	
RECOMMENDED ACTION: Assess or regularly update inventory of all organizational assets and state of systems providing this inventory. This inventory is updated on a recurring basis on the responsibility for Item (7) and (8).	FOUR KEYWORDS AND REFERENCE: Color: Light Blue, Severity: "Low", (2) - Information Security in www.gsa.gov/asset-inventory	<input type="checkbox"/> IMPLEMENTED <input type="checkbox"/> IN PROGRESS <input type="checkbox"/> SCOPED <input type="checkbox"/> NOT STARTED	<input type="checkbox"/> IMPLEMENTED <input type="checkbox"/> IN PROGRESS <input type="checkbox"/> SCOPED <input type="checkbox"/> NOT STARTED	
5.B Organizational Cybersecurity Leadership	5.B.1, 5.B.2			
GOALS: 5.B.1 - IMPACT HIGH COMPLEXITY LOW	TOP 20 RISK ADDRESSED: Lack of sufficient cybersecurity resources, expertise, or effectiveness.	DATE: _____	DATE: _____	
RECOMMENDED ACTION: Assess organizational cybersecurity resources, expertise, and effectiveness for planning, measuring, and monitoring of organizational priorities. This may include activities such as reviewing cybersecurity capabilities at the service level, measuring and monitoring progress, or leading strategic development of cyber force planning.		<input type="checkbox"/> IMPLEMENTED <input type="checkbox"/> IN PROGRESS <input type="checkbox"/> SCOPED <input type="checkbox"/> NOT STARTED	<input type="checkbox"/> IMPLEMENTED <input type="checkbox"/> IN PROGRESS <input type="checkbox"/> SCOPED <input type="checkbox"/> NOT STARTED	
5.C IT Cybersecurity Leadership	5.C.1.A, 5.C.1.B			
GOALS: 5.C.1 - IMPACT HIGH COMPLEXITY LOW	TOP 20 RISK ADDRESSED: Lack of accountability, ownership, or effectiveness of IT cybersecurity program.	DATE: _____	DATE: _____	
RECOMMENDED ACTION: Assess cybersecurity program to determine responsibility and accountability for planning, measuring, and monitoring of cybersecurity priorities. This may include activities such as reviewing cybersecurity capabilities at the service level, measuring and monitoring progress, or leading strategic development of cyber force planning.		<input type="checkbox"/> IMPLEMENTED <input type="checkbox"/> IN PROGRESS <input type="checkbox"/> SCOPED <input type="checkbox"/> NOT STARTED	<input type="checkbox"/> IMPLEMENTED <input type="checkbox"/> IN PROGRESS <input type="checkbox"/> SCOPED <input type="checkbox"/> NOT STARTED	
5.D Improving IT and OT Cybersecurity Relationships	5.D.1.C, 5.D.1.D, 5.D.1.E			
GOALS: 5.D.1 - IMPACT HIGH COMPLEXITY LOW	TOP 20 RISK ADDRESSED: Poor working relationships with a lack of shared understanding, respect, trust, or information for cyber risk to be managed.	DATE: _____	DATE: _____	
RECOMMENDED ACTION: Organizational members at least "look out for" or "work together" to get the job done. This includes understanding working relationships between IT and OT security personnel, and is not a working relationship as a primary focus during an incident response.		<input type="checkbox"/> IMPLEMENTED <input type="checkbox"/> IN PROGRESS <input type="checkbox"/> SCOPED <input type="checkbox"/> NOT STARTED	<input type="checkbox"/> IMPLEMENTED <input type="checkbox"/> IN PROGRESS <input type="checkbox"/> SCOPED <input type="checkbox"/> NOT STARTED	



Cyber Performance Goals

- Voluntary self-assessment
- Baseline set of cybersecurity practices
- Broadly applicable across critical infrastructure
- Known risk-reduction value
- Recommended practices for IT and OT owners
- Guided self-assessment
- Not a full cybersecurity program



IDENTIFY (1)				
1.A Asset Inventory ID.AM-1, ID.AM-2, ID.AM-4, DE.CM-1, DE.CM-7	CURRENT ASSESSMENT	YEAR 1 ASSESSMENT	NOTES	
CODE: 8 (0) IMPACT: HIGH RISK: HIGH COMPLEXITY: MEDIUM FACTS, TECHNIQUE, AND PROCEDURE (TFP) OR RISK ADDRESSED: Inventory Addition (1.2.20) Equifax Public Facing Application (CVE-2016, CVE-2016-5329) Insecure Accession (CVE-2016-7029) RECOMMENDED ACTION: Maintain a regularly updated inventory of all organizational assets with an IP address (including IPv6), including OT. This inventory is updated on a recurring basis, not less than monthly for SOI/CI and CI. FREE SERVICES AND REFERENCES: Cisco Umbrella Services , Qualys OT Discovery/Probe or VMware vSphere Security Tools	DATE:	DATE:		
	<input type="checkbox"/> IMPLEMENTED <input type="checkbox"/> IN PROGRESS <input type="checkbox"/> SCOPED <input type="checkbox"/> NOT STARTED	<input type="checkbox"/> IMPLEMENTED <input type="checkbox"/> IN PROGRESS <input type="checkbox"/> SCOPED <input type="checkbox"/> NOT STARTED		
1.B Organizational Cybersecurity Leadership ID.OV-1, ID.OV-2	CURRENT ASSESSMENT	YEAR 1 ASSESSMENT	NOTES	
CODE: 8 (0) IMPACT: HIGH RISK: HIGH COMPLEXITY: LOW TFP OR RISK ADDRESSED: Lack of sufficient cybersecurity accountability, investment, or effectiveness. RECOMMENDED ACTION: A named role/responsibility is identified as responsible and accountable for planning, executing, and execution of cybersecurity activities. This role may undertake activities, such as managing cybersecurity operations at the sector level, responding and securing bought-in resources, or leading strategic development to inform future planning.	DATE:	DATE:		
	<input type="checkbox"/> IMPLEMENTED <input type="checkbox"/> IN PROGRESS <input type="checkbox"/> SCOPED <input type="checkbox"/> NOT STARTED	<input type="checkbox"/> IMPLEMENTED <input type="checkbox"/> IN PROGRESS <input type="checkbox"/> SCOPED <input type="checkbox"/> NOT STARTED		
1.C OT Cybersecurity Leadership ID.OV-1, ID.OV-2	CURRENT ASSESSMENT	YEAR 1 ASSESSMENT	NOTES	
CODE: 8 (0) IMPACT: HIGH RISK: HIGH COMPLEXITY: LOW TFP OR RISK ADDRESSED: Lack of accountability, investment, or effectiveness of OT cybersecurity program. RECOMMENDED ACTION: A named role/responsibility is identified as responsible and accountable for planning, executing, and execution of OT-specific cybersecurity activities. In some organizations this may be the same position as identified in 1.B.	DATE:	DATE:		
	<input type="checkbox"/> IMPLEMENTED <input type="checkbox"/> IN PROGRESS <input type="checkbox"/> SCOPED <input type="checkbox"/> NOT STARTED	<input type="checkbox"/> IMPLEMENTED <input type="checkbox"/> IN PROGRESS <input type="checkbox"/> SCOPED <input type="checkbox"/> NOT STARTED		
1.D Improving IT and OT Cybersecurity Relationships ID.OV-2, PR.AT-5	CURRENT ASSESSMENT	YEAR 1 ASSESSMENT	NOTES	
CODE: 8 (0) IMPACT: MEDIUM RISK: MEDIUM COMPLEXITY: LOW TFP OR RISK ADDRESSED: Poor working relationships and a lack of mutual understanding between IT and OT cybersecurity can often result in increased risk for OT cybersecurity. RECOMMENDED ACTION: Organizations across all asset use "table top" or simulated exercise (getting out year that is focused on strengthening working relationships between IT and OT security personnel, and to a working event, such as planning, table toping an incident response).	DATE:	DATE:		
	<input type="checkbox"/> IMPLEMENTED <input type="checkbox"/> IN PROGRESS <input type="checkbox"/> SCOPED <input type="checkbox"/> NOT STARTED	<input type="checkbox"/> IMPLEMENTED <input type="checkbox"/> IN PROGRESS <input type="checkbox"/> SCOPED <input type="checkbox"/> NOT STARTED		

CYBER INFRASTRUCTURE SURVEY



Cyber Infrastructure Survey (CIS) Highlights

- **Overview:** CIS focuses on a service-based-view versus a programmatic-view of cybersecurity. Critical services are assessed against more than 80 cybersecurity controls grouped under five top-level domains: cybersecurity management, cybersecurity forces, cybersecurity controls, cyber incident response, and cyber dependencies.
- **Delivery:** CSA-facilitated
- **Benefits:**
 - Effective assessment of cybersecurity controls in place for a critical service,
 - Easy-to-use interactive dashboard (to support cybersecurity planning and resource allocation), and
 - Access to peer performance data visually depicted on the dashboard.



Example of CIS Dashboard

CISA
CYBER-INFRASTRUCTURE SECURITY AGENCY

Home Logout

Cyber Infrastructure Survey for

Cyber Protection Resilience Index

- Point Of Contact and Participants
- Critical Service Information
- Cybersecurity Management**
- Cybersecurity Leadership
- Inventory
- System Architecture
- Security Architecture
- Change Management
- Lifecycle Tracking
- Accreditation and Assessment
- Cybersecurity Plan
- Cybersecurity Exercises
- External Information Sharing

Threat Overlay: General Scenario: General

Cyber Protection Resilience

Cyber Protection Resilience

Your Score: ~15
Comparison High: ~45
Comparison Median: ~35
Comparison Low: ~15

Threat-based PMI:

- Natural Disaster
- Distributed Denial-of-Service
- Remote Access Compromise
- System Integrity Compromise

Scenario:

- Where should we to invest?
- Weakest area in comparison to peers
- Show management improvement

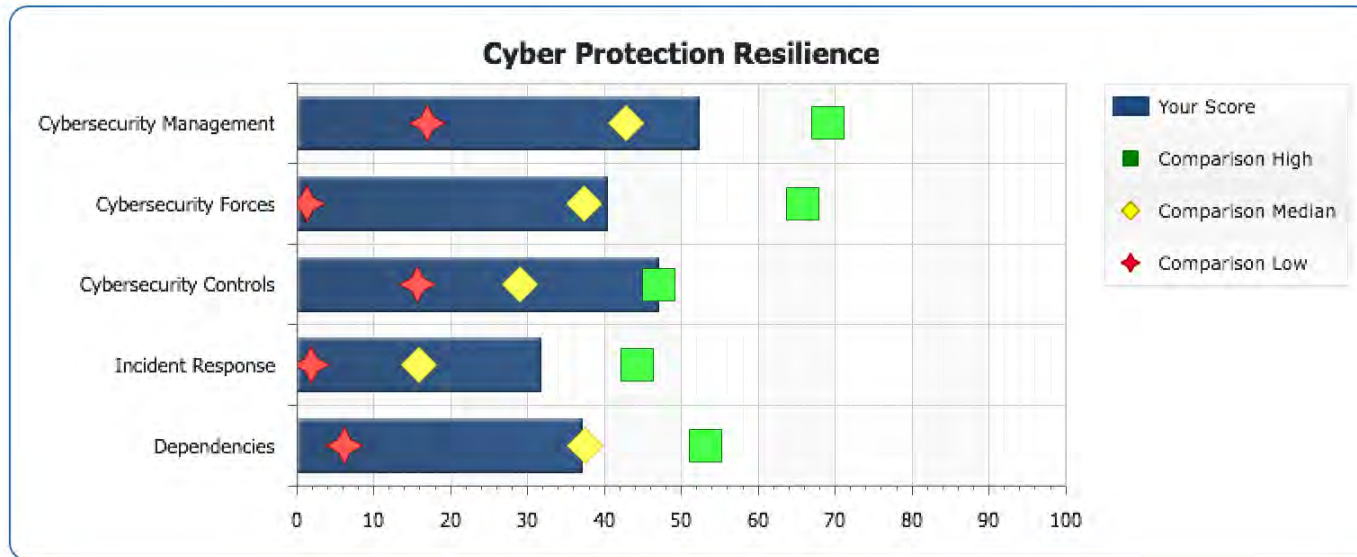
Comparison:

- Low Performers
- Median Performers
- High Performers



CIS Dashboard - Comparison

- Shows the low, median, and high performers
- Compares your organization to the aggregate





EXTERNAL DEPENDENCIES MANAGEMENT ASSESSMENTS

External Dependencies Management Highlights

- **Purpose:** Evaluate the activities and practices your organization uses to manage risks arising from external dependencies. Through an EDM Assessment, your organization will gain a better understanding of your cybersecurity posture relating to external dependencies.
- **Delivery:** CSA-facilitated
- **Through the EDM Assessment, your organization will evaluate:**
 - Relationship Formation – how your organization considers third-party risks, selects external entities, and forms relationships with them so that risk is managed from the start.
 - Relationship Management and Governance – how your organization manages ongoing relationships with external entities to support and strengthen your critical services at a managed level of risk and costs.
 - Service Protection and Sustainment – how your organization plans for, anticipates, and manages disruption or incidents related to external entities.



External Dependencies Management

- **Purpose:** Evaluate an entity's management of their dependencies on third-party entities
- **Delivery:** CSA-facilitated
- **Benefits:**
 - Better understanding of the entity's cyber posture relating to external dependencies
 - Identification of improvement areas for managing third parties that support the organization



EDM process outlined per the External Dependencies Management Resource Guide

Note: graphic edits will need time to be recreated and adjusted.



EDM Assessment Organization and Structure

- ❑ Structure and scoring similar to Cyber Resilience Review
- ❑ Uses one Maturity Indicator Level (MIL) scale with three lifecycle domains.

Relationship Formation

Assesses whether the acquirer evaluates and controls the risks of relying on external entities before entering into relationships with them.

Relationship Management and Governance

Assesses whether the acquirer manages ongoing relationships to maintain the resilience of the critical service, and mitigate dependency risk.

Service Protection and Sustainment

Assesses whether the acquirer accounts for its dependence on external entities as part of its operational activities around managing incidents, disruptions, and threats.



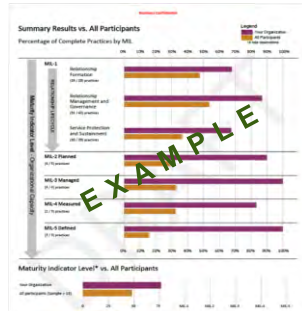
EDM Assessment Report

Each EDM report includes:

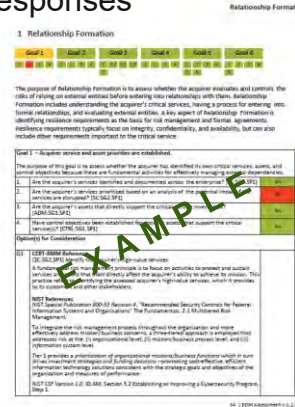
- Performance summary of existing capability managing external dependencies



- Comparison data with other EDM participants



- Sub-domain performance of existing capability managing external dependencies and options for consideration for all responses



CYBER RESILIENCE REVIEW



Cyber Resilience Review

- **Purpose:** Evaluates that maturity of an organization's capacities and capabilities in performing, planning, managing, measuring, and defining cybersecurity capabilities across the following 10 domains:

Asset Management	Service Continuity Management
Controls Management	Risk Management
Configuration and Change Management	External Dependency Management
Vulnerability Management	Training and Awareness
Incident Management	Situational Awareness

- **Benefits include:** Helps public and private sector partners understand and measure cybersecurity capabilities as they relate to operational resilience and cyber risk



CYBER RESILIENCE REVIEW (CRR)

Question Set with Guidance

April 2020

U.S. Department of Homeland Security
Cybersecurity and Infrastructure Security Agency

Cyber Resilience Review Domains

Asset Management

Know your assets being protected & their requirements, e.g., CIA

Risk Management

Know and address your biggest risks that considers cost and your risk tolerances

Configuration and Change Management

Manage asset configurations and changes

Service Continuity Management

Ensure workable plans are in place to manage disruptions

Controls Management

Manage and monitor controls to ensure they are meeting your objectives

Situational Awareness

Discover and analyze information related to immediate operational stability and security

External Dependencies Management

Know your most important external entities and manage the risks posed to essential services

Training and Awareness

Ensure your people are trained on and aware of cybersecurity risks and practices

Incident Management

Be able to detect and respond to incidents

Vulnerability Management

Know your vulnerabilities and manage those that pose the most risk

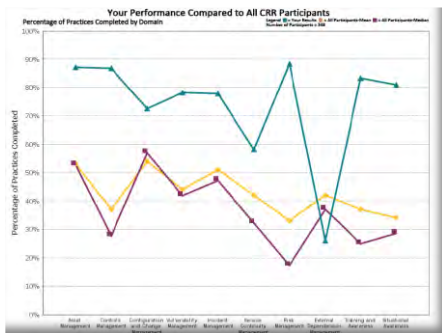
For more information: <https://www.cisa.gov/cisa-cybersecurity-resources>



CRR Sample Report



Each CRR report includes:



Comparison data with other CRR participants
*facilitated only



A summary “snapshot” graphic, related to the **NIST Cyber Security Framework**.

Domain performance of existing cybersecurity capability and options for consideration for all

Responses

Domain 1: ASSET MANAGEMENT

ML-1	ML-2	ML-3	ML-4	ML-5	ML-6	ML-7
GI	CG	CA	CE	CF	CS	CT

The purpose of Asset Management (AM) is to identify, document, and manage assets during their life cycle to ensure sustained productivity to support critical services. There are seven goals in Asset Management:

- Goal 1 – Identify & prioritize critical services
- Goal 2 – Inventory assets, and establish the authority and responsibility for these assets
- Goal 3 – Establish the relationship between assets and the services they support
- Goal 4 – Manage the asset inventory
- Goal 5 – Manage access to assets
- Goal 6 – Prioritize & manage information assets
- Goal 7 – Prioritize & manage facility assets

The following contains questions asked during the CRR for each goal in the Asset Management domain, and your organization's response to these questions. In cases where the response is noted as "Incomplete" or "No", there is an accompanying Option for Consideration addressing that question.

Goal 1 – Identify & prioritize critical services:		
1.	Are critical services identified? [SC-SG1.SF.1]	Incomplete
2.	Are critical services prioritized based on an analysis of potential impact if these services are disrupted? [SC-SG1.SF.1]	Incomplete
Q2	CERT-RBM Reference: [SC-SG1.SF.1] Identify and inventory critical services, associated assets, and activities. A fundamental risk management principle is to focus on activities to protect and sustain services and assets that most directly affect the organization's ability to achieve its mission. Additional Reference: NIST SP 800-34, Revision 1 "Contingency Planning Guide for Federal Information Systems" (pages 15-19)	Incomplete
Goal 2 – Inventory assets, and establish the authority and responsibility for these assets:		
1.	Are the assets that directly support the critical service inventoried? [ADM-SG1.SF.1]	People: Incomplete Information: Incomplete Technology: Incomplete Facilities: Complete
Q1	CERT-RBM Reference: [ADM-SG1.SF.1] Identify and inventory critical assets. An organization must be able to identify its critical assets, document them, and establish their value in order to develop strategies for protecting and sustaining assets commensurate with their value to the services they support. Additional Reference: NIST SP 800-18, Revision 1, "Guide for Developing Security Plans for Federal Information Systems" (pages 2-3)	Incomplete



TABLETOP EXERCISES



Cyber or Physical Tabletop Exercises

- Develop and conduct preparedness exercises for a variety of resilience disciplines
- Customized and facilitated exercises
- Off-the-shelf, do it yourself, Tabletop Exercise Packages (CTEPs)
- Small-scale, discussion-based
- Large-scale, operations-based exercises



CTEP Scenarios

Active Threat

- COVID-19 Active Shooter
- COVID-19 Sensitive Information
- Hazardous Materials
- Potential Civil Unrest
- **Chemical Sector** – Active Shooter, Active Threat, Domestic Threat, Edged Weapon, Improvised Explosive Device (IED), Vehicle-Borne Improvised Explosive Device (VBIED), Vehicle Ramming, Fire as a Weapon, Unmanned Aerial System (UAS), Civil Unrest
- **Commercial Facilities** – Outdoor Events Edged Weapon, Outdoor Events Active Shooter, Outdoor Events VBIED & Hostage, Outdoor Events Hostage, Cruise Ship Incident, Indoor Performing Arts Theater
- **Critical Manufacturing** – Supply Chain Terrorist Threat, Supply Chain Border Closing
- **Dams** – Active Shooter
- **Defense Industrial Base** – VBIED
- **Education** – K-12 Education Active Threat
- **Energy** – Electricity Substation
- **Food & Agriculture** – Food Manufacturing Facility (Processing/Packaging/Production)
- **Government Facilities** – National Monuments & Icons
- **Healthcare & Public Health** – Suicide Bomber, Suspicious Package, VBIED
- **Transportation** – Maritime Domestic Terror

Cyber

- Insider Threat
- Elections: Early Voting Same Day or Election Day Registration
- Elections: Election Day Voting Machines
- Elections: Vote by Mail
- Ransomware: Industrial Controls
- Ransomware: Ransomware Third Party Vendor
- Ransomware: Vendor Phishing
- **Chemical Sector** – Cyber Attack
- **Water & Wastewater Systems** – Cyber Attack

Natural Disaster

- Hurricane
- Pandemic Recovery
- Wildfire
- **Critical Manufacturing** – Hurricane Supply Chain, Pandemic Supply Chain Disruption, Severe Flooding Supply Chain, Supply Chain Severe Winter Weather
- **Emergency Services** – ESS Disaster Access Management/Re-entry

Complex Coordinated Attack

- Violent Extremist
- **Chemical Sector** – Complex Coordinated Attack
- **Commercial Facilities** – Large Box Store, Gaming Industry
- **Dams** – Adversarial Threat
- **Education** – Higher Education Active Threat
- **Food & Agriculture** – Supply Chain



Available at [CISA Tabletop Exercises Packages](#)

CTEP Facilitation

- Timeline:
 - 1 – 2 month planning cycle
 - 1 formal planning meeting (*CISA and Stakeholder*)
- Planning Activities:
 - Modify CTEP scenario (*CISA modifies and Stakeholder reviews*)
 - Modified CTEP discussion questions (*CISA modifies and Stakeholder reviews*)
 - Facilitation (*CISA facilitates and Stakeholder provides venue and participants*)
 - In-person, virtual, or hybrid
 - 3 – 6 hour exercises
 - Key Takeaways (*CISA develops*)



Custom Built Exercise

- Timeline:
 - 3 – 4 month planning cycle
 - 4 – 5 formal planning meetings (*CISA and Stakeholder*)
- Planning Activities:
 - Document development (*CISA develops and Stakeholder reviews*)
 - Scenario development (*CISA develops and Stakeholder reviews*)
 - Facilitation (*CISA facilitates and Stakeholder provides venue and participants*)
 - In-person, virtual, or hybrid
 - 3 – 6 hour exercises
 - After Action Report/Summary development (*CISA develops*)





CYBER HYGIENE: VULNERABILITY SCANNING

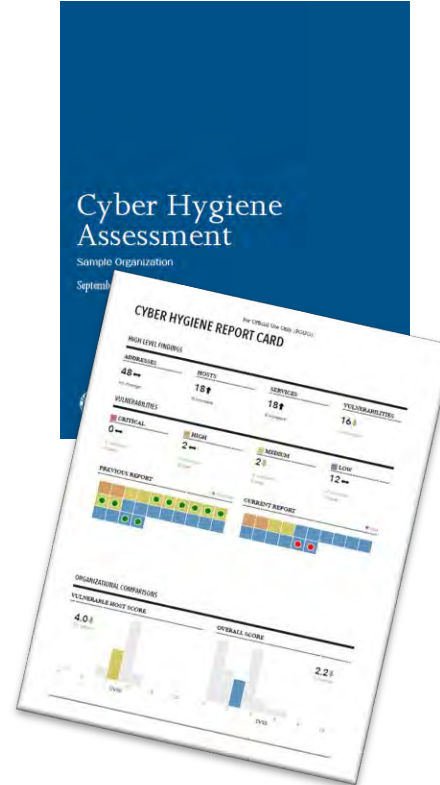
Vulnerability Scanning

Purpose: Assess Internet-accessible systems for known vulnerabilities and configuration errors.

Delivery: Online by CISA

Benefits:

- Continual review of system to identify potential problems
- Weekly reports detailing current and previously mitigated vulnerabilities
- Recommended mitigation for identified vulnerabilities
- **Network Vulnerability & Configuration Scanning**
 - Identify network vulnerabilities and weakness



Reports

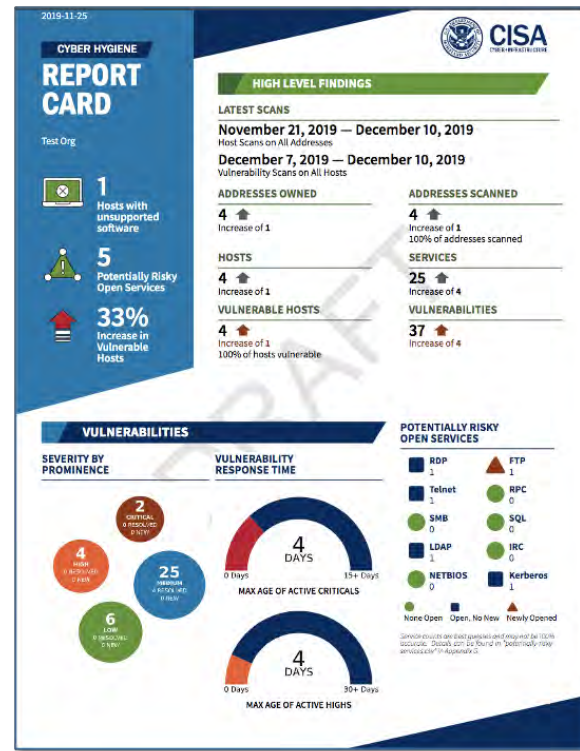


Weekly Reports

- Password-protected PDF
- High-level summary “Report Card”
- Filterable/ingestible CSV attachments
- Sub-organization breakdown (if requested)

Ad-Hoc Alerts within 24 hours of detecting:

- New critical/high vulnerabilities
- New known exploited vulnerabilities
- Newly available potentially risky services



We recommend creating a distribution list to receive reports so that you can control who receives them.

Known Exploited Vulnerabilities Catalog



**CYBERSECURITY
& INFRASTRUCTURE
SECURITY AGENCY**



Search



cisa.gov/uscert

[Report Cyber Issue](#)



KNOWN EXPLOITED VULNERABILITIES CATALOG

[Download CSV version](#)

[Download JSON version](#)

[Download JSON schema](#)

[Subscribe to the Known Exploited Vulnerabilities Catalog Update Bulletin](#)

[Back to previous page for background on known exploited vulnerabilities](#)



CYBER HYGIENE: WEB APPLICATION SCANNING (WAS)



Cyber Hygiene: Web Application Scanning (WAS)

The CISA Assessments team supports Federal, State, Local, Tribal and Territorial Governments and Critical Infrastructure partners by providing proactive testing and assessment services. CISA's Cyber Hygiene Web Application Scanning is "internet scanning-as-a-service." This service assesses the "health" of your publicly accessible web applications by checking for known vulnerabilities and weak configurations. Additionally, we can recommend ways to enhance security in accordance with industry and government best practices and standards.



SCANNING OBJECTIVES

- Maintain enterprise awareness of your publicly accessible web-based assets
- Provide insight into how systems and infrastructure appear to potential attackers
- Drive proactive mitigation of vulnerabilities to help reduce overall risk

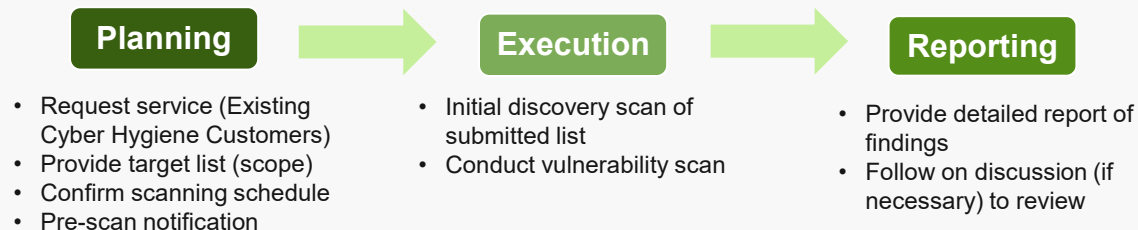


SCANNING PHASES AND OVERALL PROCESS

Scanning Phases

- **Discovery Scanning:** Identify active, internet-facing web applications
- **Vulnerability Scanning:** Initiate non-intrusive checks to identify potential vulnerabilities and configuration weaknesses

OVERALL PROCESS



CYBER SECURITY EVALUATION TOOL



Cyber Security Evaluation Tool

- **Purpose:** Assesses control system and information technology network security practices against industry standards.
- **Facilitated:** Self-Administered, undertaken independently
- **Benefits:**
 - Immediately available for download upon request
 - Understanding of operational technology and information technology network security practices
 - Ability to drill down on specific areas and issues
 - Helps to integrate cybersecurity into current corporate risk management strategy



RANSOMWARE READINESS ASSESSMENT



Ransomware Incident Response

- Guidance for preparation and response for ransomware
- This guide was developed through the U.S. Joint Ransomware Task Force (JRTF)
- Part 1: Ransomware and Data Extortion Prevention Best Practices
- Part 2: Ransomware and Data Extortion Response Checklist



VALIDATED ARCHITECTURE DESIGN REVIEW



Validated Architecture Design Review

Purpose: Analyze network architecture, system configurations, log file review, network traffic and data flows to identify abnormalities in devices and communications traffic.

Delivery: CISA staff working with entity staff

Benefits:

- In-depth review of network and operating system
- Recommendations to improve an organization's operational maturity and enhancing their cybersecurity posture
- Evaluation of network architecture





RISK AND VULNERABILITY ASSESSMENT [PENETRATION TEST]

Risk and Vulnerability Assessment

- **Purpose:** Perform network penetration and deep technical analysis of enterprise IT systems and an organization's external resistance to specific IT risks
- **Delivery:** Onsite by CISA
- **Benefits:**
 - Identification of vulnerabilities
 - Specific remediation recommendations
 - Improves an entity's cyber posture, limits exposure, reduces rates of exploitation
 - Increases speed and effectiveness of future cyber attack responses.



RVA team with Federal Lead Miguel Rios (far left) on a pentest for a stakeholder

Remote Penetration Testing

SCENARIOS



External Penetration Test: Verifying if the stakeholder network is accessible from the public domain by an unauthorized user by assessing open ports, protocols, and services.



External Web Application Test: Evaluating web applications for potential exploitable vulnerabilities; the test can include automated scanning, manual testing, or a combination of both methods.



Phishing Assessment: Testing the stakeholder email infrastructure through carefully crafted phishing emails containing a variety of malicious payloads to the trusted point of contact.



Open-Source Information Gathering: Identify publicly available information about the stakeholder environment which may be useful in preparing for an attack.

ASSESSMENT OBJECTIVES

- Conduct assessments to identify vulnerabilities and work with customers to eliminate exploitable pathways.
- Simulate the tactics and techniques of real-world threats and malicious adversaries.
- Test centralized data repositories and externally accessible assets/resources.
- Avoid causing disruption to the customer's mission, operation, and network infrastructure.

ASSESSMENT TIMELINE

Pre-Planning

- Request RPT
- Receive RPT Capabilities Brief
- Sign and return RPT Rules of Engagement
- Determine RPT services, scope, and logistics during pre-assessment call(s)

Planning

- Confirm schedule
- Establish trusted points of contact

Execution (Up to Six Weeks)

- Dependent on resource availability
- Critical findings are immediately disclosed

Reporting

- Briefing and initial recommendations
- Final report review and receipt – 10 days



Risk and Vulnerability Assessment

Assessment Aspects

Service	Description
Vulnerability Scanning and Testing	Conduct Vulnerability Assessments
Penetration Testing	Exploit weakness, test responses in systems, applications, network, and security controls
Social Engineering	Craft e-mail at targeted audience to test security awareness, used as an attack sector to internal network
Wireless Discovery & Identification	Identify wireless signals and rogue wireless devices, and exploit access points
Web Application Scanning and Testing	Identify web application vulnerabilities
Database Scanning	Security Scan of database settings and controls
Operating System Scanning	Security Scan of operating system to do compliance checks



CISA Cyber Assessments in Brief, 1 of 2

Name	Cyber Resilience Review	Cyber Infrastructure Survey	External Dependencies Management Review	Cybersecurity Evaluation Tool Assessment
Purpose	Identify cybersecurity management capabilities and maturity	Calculate a comparative analysis and valuation of protective measures in-place	Assess the activities and practices utilized by an organization to manage risks arising from external dependencies	Provide detailed, effective, and repeatable methodology for assessing control systems security encompassing the organization's infrastructure, policies, and procedures
Scope	Critical service view	Critical service view	Critical service view	Information Technology and Operational Technology systems
Time to Execute	8 Hours (1 business day)	2 ½ to 4 Hours	2 ½ to 4 Hours	Varies greatly (min 2 Hours), unknown for self-assessment
Information Sought	Capabilities and maturity indicators in 10 security domains	Protective measures in-place	Capabilities and maturity indicators across third-party relationship management lifecycle domains	Architecture diagrams, infrastructure, policies, and procedures documents
Preparation	1-hour questionnaire and planning call(s)	Planning call to scope evaluation	Planning call to scope evaluation	Self-assessment available from web site and used locally
Participants	IT / Security Manager, Continuity Planner, and Incident Responders	IT / Security Manager	IT / Security Manager with Continuity Planner and Contract Management	Operators, engineers, IT staff, policy / management personnel, and subject matter experts
Delivered By	CSAs iodregionaloperations@cisa.dhs.gov	CSAs iodregionaloperations@cisa.dhs.gov	CSAs iodregionaloperations@cisa.dhs.gov	Self-administered / CSAs https://ics-cert.us-cert.gov/



CISA Cyber Assessments in Brief, 2 of 2

Name	Validated Architecture Design Review	Phishing Campaign Assessment	Risk and Vulnerability Assessment	Vulnerability Scanning
Purpose	Provide analysis and representation of asset owner's network traffic, data flows, and relationships between devices and identifies anomalous communications flows.	Measure the susceptibility of an organization's personnel to social engineering attacks, specifically email phishing attacks.	Perform penetration and deep technical analysis of enterprise IT systems and an organization's external resistance to specific IT risks	Identify public-facing Internet security risks, at a high-level, through service enumeration and vulnerability scanning
Scope	Industrial Control Systems / Network Architecture, Traffic	Organization / Business Unit / Email Exchange Service	Organization / Business Unit / Network-Based IT Service	Public-Facing, Network-Based IT Service
Time to Execute	Variable (Hours to Days)	Approximately 6 Weeks	Variable (Days to Weeks)	Variable (Hours to Continuous)
Information Sought	Network design, configurations, log files, interdependencies, data flows and its applications	Click rate metrics gathered during phishing assessment	Low-level options and recommendations for improving IT network and system security	High-level network service and vulnerability information
Preparation	Coordinated via Email. Planning call(s).	Formal rules of engagement and pre-planning	Formal rules of engagement and extensive pre-planning	Formal rules of engagement and extensive pre-planning
Participants	Control system operators/ engineers, IT personnel, and ICS network, architecture, and topologies SMEs	IT/Security Manager and Network Administrators, end users	IT/Security Manager and Network Administrators	IT/Security Manager and Network Administrators
Delivered By	VM VM@CISA.DHS.GOV	VM VM@CISA.DHS.GOV	VM VM@CISA.DHS.GOV	VM VM@CISA.DHS.GOV



INFORMATION SHARING



ISACs

The EI-ISAC is federally funded by CISA and a division of the Center for Internet Security (CIS).
The EI-ISAC is autonomously guided by the Executive Committee and member organizations.



CISA focuses on the cybersecurity of all critical infrastructure within the United States (including election offices).



The MS-ISAC is a trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial (SLTT) government entities.



The EI-ISAC supports the rapidly changing cybersecurity needs of U.S. SLTT election offices.



CIS is home to the MS-ISAC and the EI-ISAC

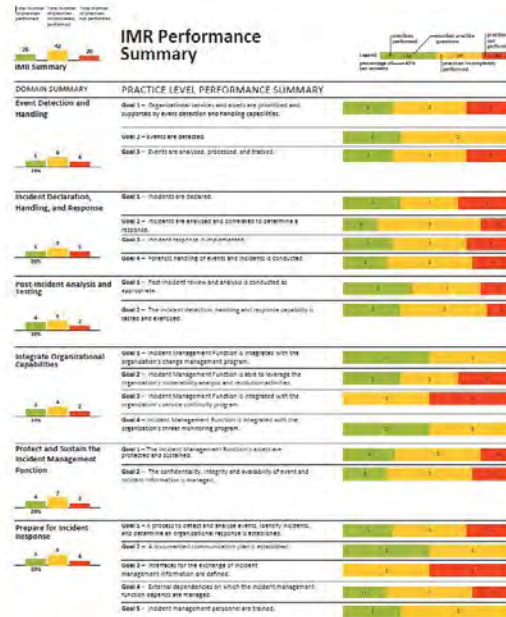


INCIDENT MANAGEMENT REVIEW



INCIDENT MANAGEMENT REVIEW

SEPTEMBER 2020



Incident Management Planning Helps Mitigate Effects

1. Get leadership support for incident management planning.
2. Establish an event-detection process.
3. Establish a triage-and-analysis process.
4. Establish an incident-declaration process.
5. Establish an incident-response and recovery process.
6. Establish an incident-communications process.
7. Assign roles and responsibilities for incident management.
8. Establish a post-incident analysis and improvement process.

Resource: Google Mandiant, CRR Supplemental Resource Guide, Incident Management.

CRR Supplemental Resource Guide



Volume 5

Incident Management

Version 1.1



Federal Incident Response, 1 of 2

Federal Incident Response

- **Threat Response:** Attributing, pursuing, and disrupting malicious cyber actors and malicious cyber activity. Conducting criminal investigations and other actions to counter the malicious cyber activity.
- **Asset Response:** Protecting assets and mitigating vulnerabilities in the face of malicious cyber activity, reducing the impact to systems and data; strengthening, recovering, and restoring services; identifying other entities at risk; and assessing potential risk to broader community.



Federal Incident Response, 2 of 2

Threat Response

Federal Bureau of Investigation

855-292-3937 or cywatch@ic.fbi.gov

U.S. Secret Service

secretsservice.gov/contact/field-offices

Immigration and Customs

Homeland Security Investigations

866-347-2423 or ice.gov/contact/hsi

Asset Response

CISA Central

888-282-0870 or central@cisa.DHS.gov

Report suspected or confirmed cyber incidents, including when the affected entity may be interested in government assistance in removing the adversary, restoring operations, and recommending ways to further improve security.

Report Internet Crimes:

FBI Internet Crime Complaint Center

ic3.gov



Malware Analysis

To submit malware:

- Email submissions to CISA Central at: submit@malware.us-cert.gov
 - Send in password-protected zip file(s). Use password "infected."
- Upload submission online: <https://malware.us-cert.gov>

US-CERT AMAC Malware Analysis Submissions

Job Disclaimer

By submitting malware artifacts to the Department of Homeland Security's (DHS) United States Computer Emergency Readiness Team (US-CERT), submitter agrees to the following:

Submitter requests that DHS provide analysis and warnings of threats to and vulnerabilities of its systems, as well as mitigation strategies as appropriate.

Submitter has obtained the data, including any electronic communications, and is disclosing it to DHS consistent with all applicable laws and regulations.

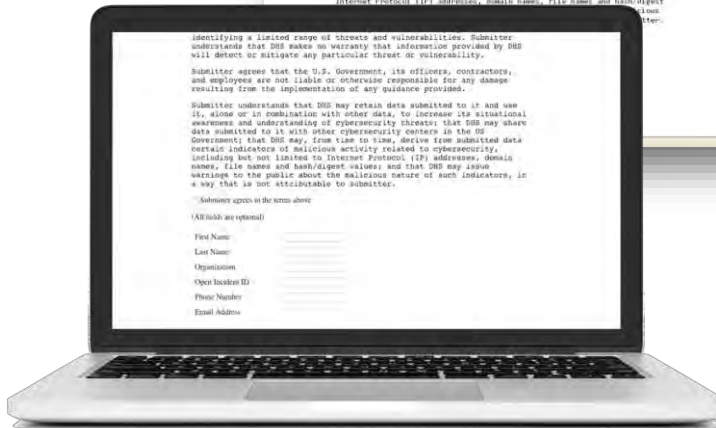
Submitter acknowledges that DHS's analysis is for the purpose of identifying a limited range of threats and vulnerabilities. Submitter understands that DHS makes no warranty that information provided by DHS will detect or mitigate any particular threat or vulnerability.

Submitter agrees that the U.S. Government, its officers, contractors, and employees are not liable or otherwise responsible for any damage resulting from the implementation of any guidance provided.

Submitter understands that DHS may retain data submitted to it and use it, alone or in combination with other data, to increase its situational awareness and understanding of cybersecurity threats; that DHS may share data submitted to it with other cybersecurity centers in the US Government; that DHS may, from time to time, derive from submitted data certain indicators of malicious activity related to cybersecurity, including but not limited to Internet Protocol (IP) addresses, domain names, file names and hash/digest values.

Submitter agrees to the terms above
(All fields are optional)

First Name: _____
Last Name: _____
Organization: _____
Open Incident ID: _____
Phone Number: _____
Email Address: _____





ADDITIONAL CYBERSECURITY RESOURCES

Cybersecurity Awareness Month

The National Cybersecurity Alliance creates strong partnerships between governments and corporations to amplify our message and to foster a greater “digital” good.

Each and every one of us needs to do our part to make sure that our online lives are kept safe and secure. That’s what Cybersecurity Awareness Month is all about!



Established in 2001
2.1 Mil page views in 2021
30k Newsletter subscribers
360k Social media followers



Cybersecurity Awareness Month Partner

- Partnering with CISA for Cybersecurity Awareness Month is a great way for us to work together and share the importance of reducing risks when we are online or using devices connected to the internet.
- As a partner your organization will receive free resources to help it create its own campaign and promote participation in Cybersecurity Awareness Month by employees, customers, the public, friends, and family.
- Become one of our partners and help promote a safer, more secure, and more trusted internet.
- For more information, and to become a Cybersecurity Awareness Month partner, email us at AwarenessCampaigns@cisa.dhs.gov



Request a CISA Speaker

- CISA maximizes its resources through unified integrated and cohesive stakeholder activities by engaging in speaking events and conferences.
- Follow the steps at the “Request a CISA Speaker” page to request a CISA speaker for your Cybersecurity Awareness Month event.
- <https://www.cisa.gov/news-events/request-speaker>



City of Orinda Council Meeting

Get .gov Domain

- Get .gov Domain. It should be easy to identify governments on the internet.
- The public shouldn't have to guess whether the site they're on or the email that hits their inbox is genuine.
- .gov is the top-level domain for U.S.-based government organizations.
- CISA sponsors the .gov TLD and makes it available solely to U.S.-based government organizations and publicly controlled entities.
- For those that qualify for a .gov domain, it's available without a fee. For more information or to register go to <https://get.gov/>
- For questions email registrar@dotgov.gov



CYBERSECURITY TRAINING



Free Federal Cyber Training

FedVTE enables cyber professionals to continue growing skills.

FedVTE is an online, on-demand training center that provides **free** cybersecurity training for U.S. veterans and federal, state, local, tribal, and territorial government employees. **As of January 2017**, there are:

- Over 140,000 registered users, including employees at all levels of government
- Over 18,000 veteran users (through non-profit partner, Hire Our Heroes™)
- Over 5,000 SLTT registered users

The logo for FedVTE (Federal Virtual Training Environment) is displayed. It features the text "FedVTE" in a large, bold, blue font, with "FEDERAL VIRTUAL TRAINING ENVIRONMENT" in a smaller, blue, sans-serif font stacked to its right.

CYBER WORKFORCE

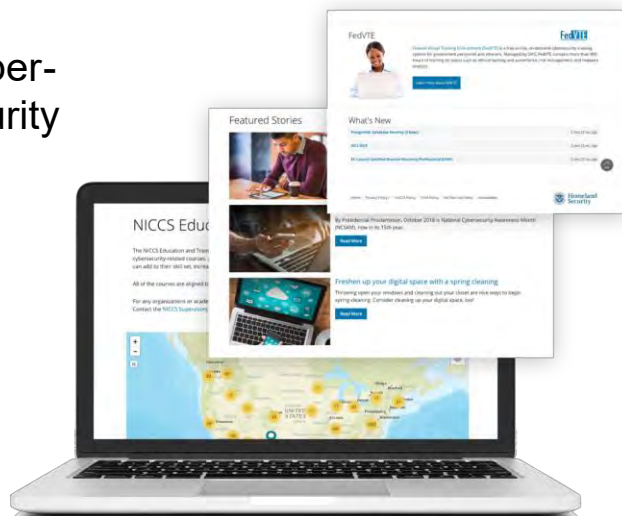


Cybersecurity Training Resources

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



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

Our Nation's Cyber Workforce Foundation

The **National Cybersecurity Workforce Framework** is a collection of definitions that describe types of cybersecurity work and skills requires to perform it.

- ✓ When used nationally, the definitions help establish universally applicable cybersecurity skills, training/development, and curricula
- ✓ 7 Categories, 30+ Specialty Areas
- ✓ Baselines knowledge, skills, and abilities & tasks



Operate
&
Maintain



Securely
Provisio
n



Analyze



Collect
&
Operate



Oversight &
Developmen
t



Protect
&
Defend



Investigat
e



CISA Cybersecurity Resources

- National Cybersecurity Assessments

- Cyber Resilience Review (CRR™)
- External Dependencies Management (EDM)
- Cyber Infrastructure Review (CIS)
- Incident Management Review (IMR)
- Cyber Resilience Essentials (CRE)
- Cyber Protection Goals (CPG's)

<https://www.cisa.gov/cyber-resource-hub>

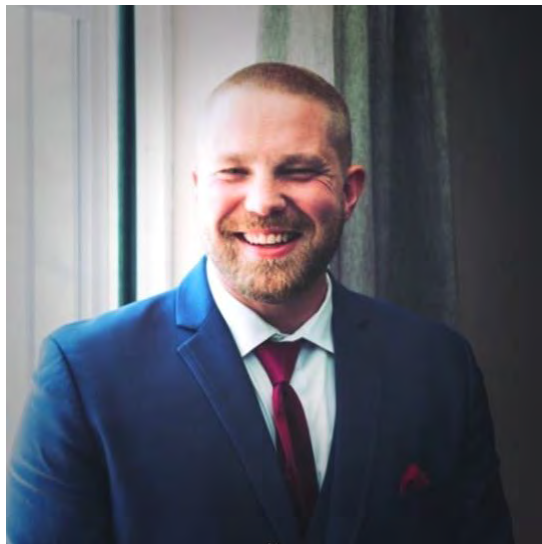
- Cyber Hygiene: Vulnerability Scanning

- Other Cyber resources

- Cyber Security Evaluation Tool (CSET)
- Malware Analysis
- National Cyber Exercise and Planning Program
- Federal Virtual Training Environment (FedVTE)
- Information Sharing and Analysis Centers (ISACs)
- STOP.THINK.CONNECT
- STOPRANSOMWARE
- Cyber Protective Visit (CPV)
- CISA.Gov



Contact



General Inquiries

iodregionaloperations@cisa.dhs.gov

CISA Contact Information

Scott Alford
Cybersecurity Advisor

Scott.alford@cisa.dhs.gov
+1 (202) 315-8091

Mario F. Garcia
Supervisory Cybersecurity Advisor

Mario.Garcia@cisa.dhs.gov
+1 (202) 309-1847

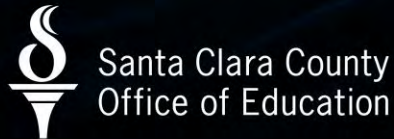
Cybersecurity and Infrastructure Security Agency





SECOND ANNUAL
CYBERSECURITY
SUMMIT 2024

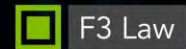
APRIL 25 • 9:00 A.M. - 3:30 P.M.



In Partnership with



Sponsored by



Adjourn to Breakout Sessions

- Community Leaders | remain in the Bowers Hall
- HR Leaders | Marilyn Pratt Lab, The Tech Interactive
- Business Leaders | Large Group Meeting Room, The Tech Interactive



Closing Remarks

David Wu, Head of Technology

Some additional advice

- Staff creatively to meet cybersecurity needs as small to mid-size organizations
- Upgrade, train, and retain your workforce
- Develop a human-centric approach to cybersecurity
- Take advantage of industry consolidation to reduce costs.



Thank you!

Event Survey QR Code:

sccoe.to/CybersecuritySummit



Toolkit QR Code:

sccoe.to/CyberToolkit



Santa Clara County Office of Education

Working collaboratively with school and community partners, the **Santa Clara County Office of Education (SCCOE)** is a regional service agency committed to serving, inspiring, and promoting student and public school success. The SCCOE is a premier service organization driven by the core principles of equity, diversity, inclusion, and partnership.

For more information about the Santa Clara County Office of Education, please visit www.sccoe.org



@SCCOE



@santaclarasccoe



@santa-clara-county-office-of-education