Albany InfraGard Members Alliance

Ransomware Tabletop Exercise

Welcome

- □ Pledge of Allegiance
- □ Recognition
- □ Team USA

Sponsors

- □ Thank you to our most recent sponsor:

NORTHERN

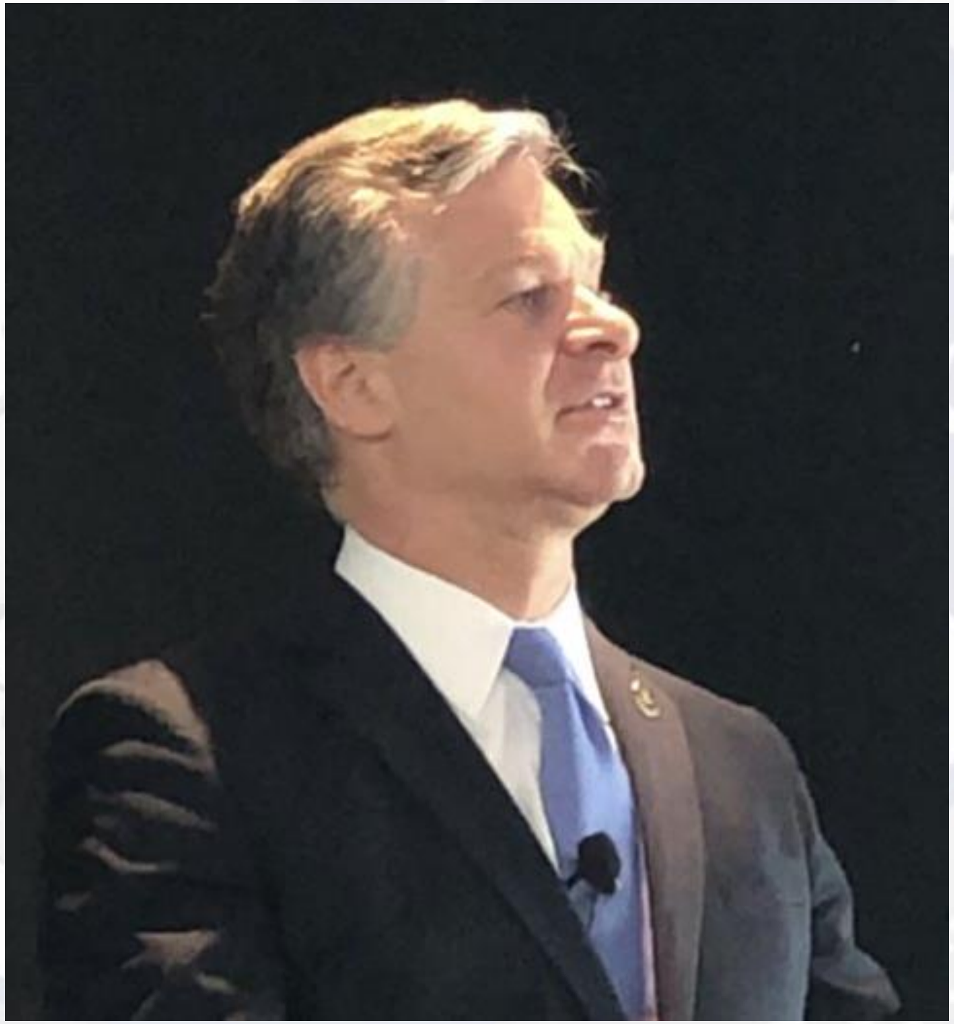
EST. N 1930

INSURING AGENCY

InfraGard Mission

- The mission of InfraGard is to promote ongoing dialogue and timely communication between members and the FBI specifically concerning the security of, vulnerabilities in, and threats to critical infrastructure entities.

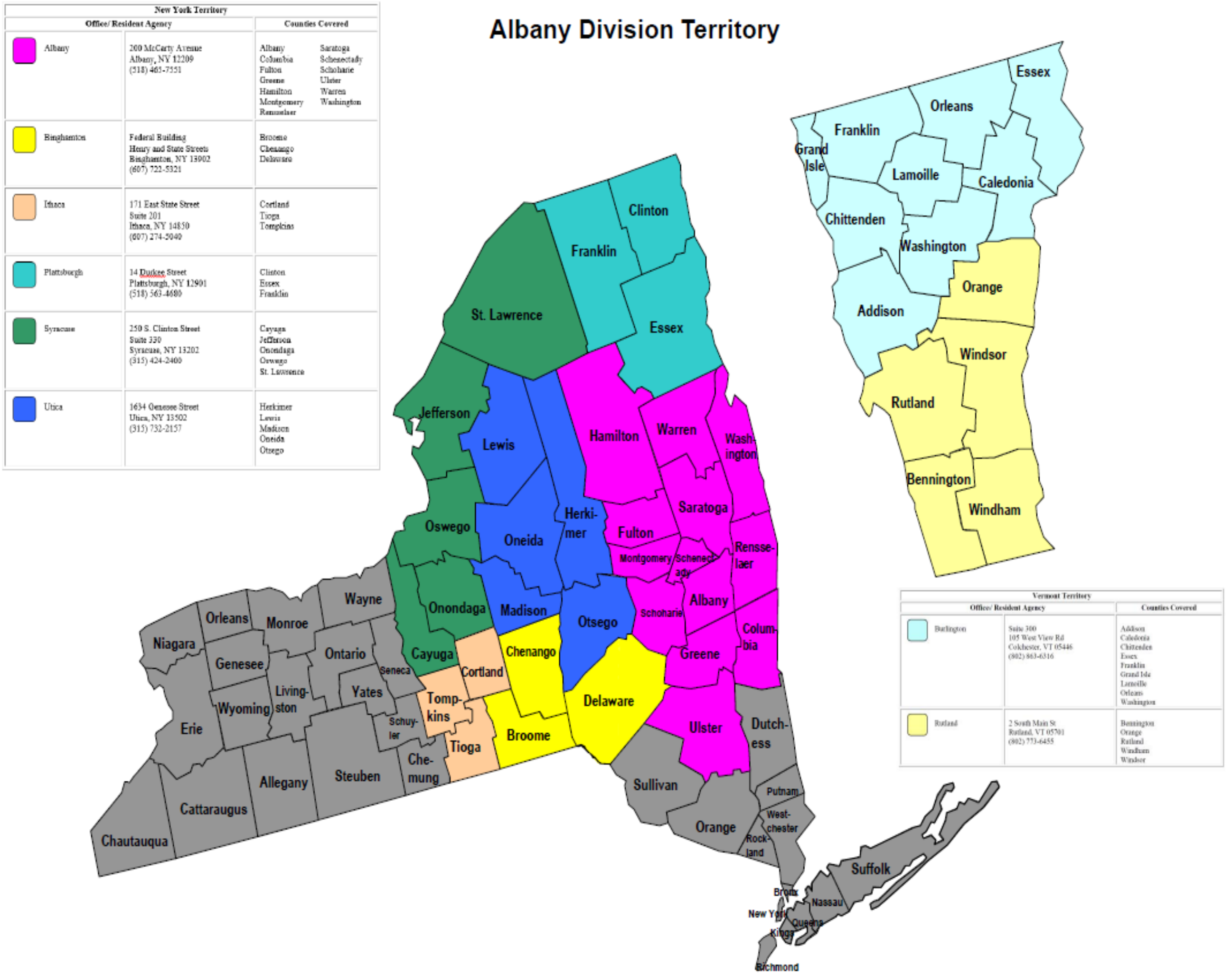
FBI Director Wray



- □ Four Pillars
  - ◘ Process
  - ◘ Brand
  - ◘ Innovation
  - ◘ Partnership

Albany InfraGard Members Alliance

- Over 40,000 square miles
- 2 states, 46 counties
- 425 members



New York Territory		
Office/ Resident Agency		Counties Covered
🟪 Albany	200 McCarty Avenue Albany, NY 12209 (518) 465-7551	Albany Columbia Fulton Greene Hamilton Montgomery Rensselaer Saratoga Schenectady Schoharie Ulster Warren Washington
🟨 Binghamton	Federal Building Henry and State Streets Binghamton, NY 13902 (607) 722-5321	Broome Chenango Delaware
🟧 Ithaca	171 East State Street Suite 201 Ithaca, NY 14850 (607) 274-5040	Cortland Tioga Tompkins
🟦 Plattsburgh	14 Durkee Street Plattsburgh, NY 12901 (518) 563-4680	Clinton Essex Franklin
🟩 Syracuse	250 S. Clinton Street Suite 330 Syracuse, NY 13202 (315) 424-2400	Cayuga Jefferson Onondaga Oswego St. Lawrence
🟦 Utica	1634 Genesee Street Utica, NY 13502 (315) 732-2157	Herkimer Lewis Madison Oneida Otsego

Albany Division Territory

Vermont Territory		
Office/ Resident Agency		Counties Covered
🟦 Burlington	Suite 300 105 West View Rd Colchester, VT 05446 (802) 863-6316	Addison Caledonia Chittenden Essex Franklin Grand Isle Lamoille Orleans Washington
🟨 Rutland	2 South Main St Rutland, VT 05701 (802) 773-6455	Bennington Orange Rutland Windham Windsor

Get Involved

- Join the Chapter – Look for InfraGard Members Today
  - www.InfraGard.org
- Become a Member of the Patriots Circle
  - InfraGard Patriots Circle (infragardnational.org)
- Sponsor our Chapter – Ensure greater access to Information to all to help defend out Nation.
  - 2020-Sponsorship-Guide.pdf (infragardalbany.org)
- InfraGard Pins here today --

Albany IMA Board of Directors

Devi Momot — President

Gary Hoover — Vice President

Jeffrey Wilson — Secretary

Michael Britton — Treasurer

John Griffin — Member at Large
Corey Hovak — Member at Large

SSA Michael Dwyer, FBI PSC and InfraGard Coordinator

Email Us at: Board@InfraGardAlbany.org

TEAM USA

- When any organization suffers, we all suffer.

Successful cyber defense requires all of us

"We are used to defending our Country in kinetic war primarily with Gov defense…today we are defending the country in cyber too…we are all part of that defense."

-Dr. Ron Ross

NIST Fellow, Information Technology Laboratory, NIST

Incident Response methodology

The mnemonic 'PICERL' consists of six steps:

1. Preparation
2. Identification
3. Containment
4. Eradication
5. Recovery
6. Lessons Learned

Prepare

- Preparation Phase Prepare for major incidents before they occur to mitigate any impact on the organization.

Are you prepared?

- Security incidents are often attributed to inadequate time spent *Preparing* -

- Today we will help you to begin or continue your preparation….enjoy the day!

INFRAGARD AND PRIVATE SECTOR COORDINATOR

FBI – InfraGard

SPONSORSHIPS

Thank you to our InfraGard Albany Sponsors

Panelists

□**Johnny Griffin,** Board Member-at-Large and Sector Chief Coordinator, InfraGard Albany Members Alliance , IT Sector Chief

□**David Hinsdale, Special Agent, FBI Cyber Squad Albany Field Office**

□**Corey Hovak,** Board Member-at-Large, InfraGard Albany Members Alliance, New York State Intelligence Center, Cyber Analysis Unit

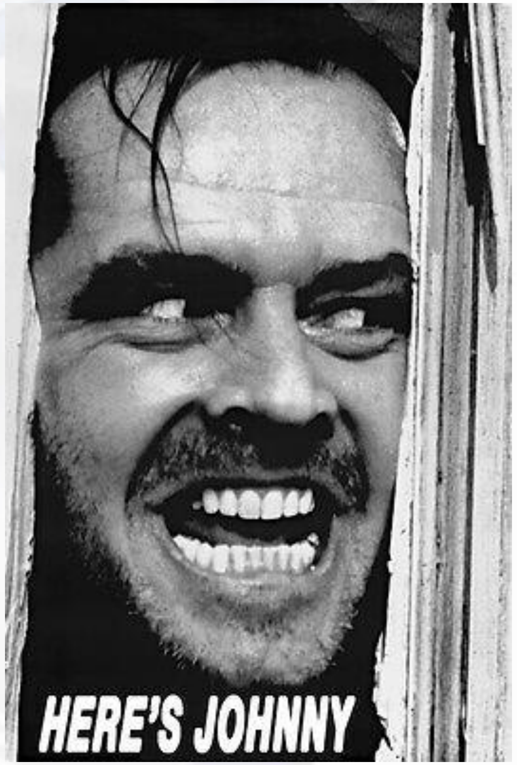
□**Rich Ingersoll,** Health Sector Chief, InfraGard Albany

□**Devi Momot,** Communications Sector Chief, President InfraGard Albany Members Alliance

□**Alex Vargas,** FBI Computer Scientist

□**Brian Gregoire**, NYS Troopers Investigator, Task Force Officer, FBI, InfraGard Albany Members Alliance Emergency Services Sector Chief

And here's Johnny!!



- This presentation has several components – tabletop-style cyber security walkthroughs and participation scenarios and a panel discussion.
- These are intended **solely to provoke discussion** among the attendees
- It’s perfectly fine (even optimal) if we don’t complete them due to an enormous volume of questions and comments from the attendees as we go along.
- The panel and support group today is composed of FBI agents and computer scientists. New York State Police investigators and intelligence analysts. FBI Cyber Task Force Officers. New York state cyber incident response team members. Private sector cyber security experts.

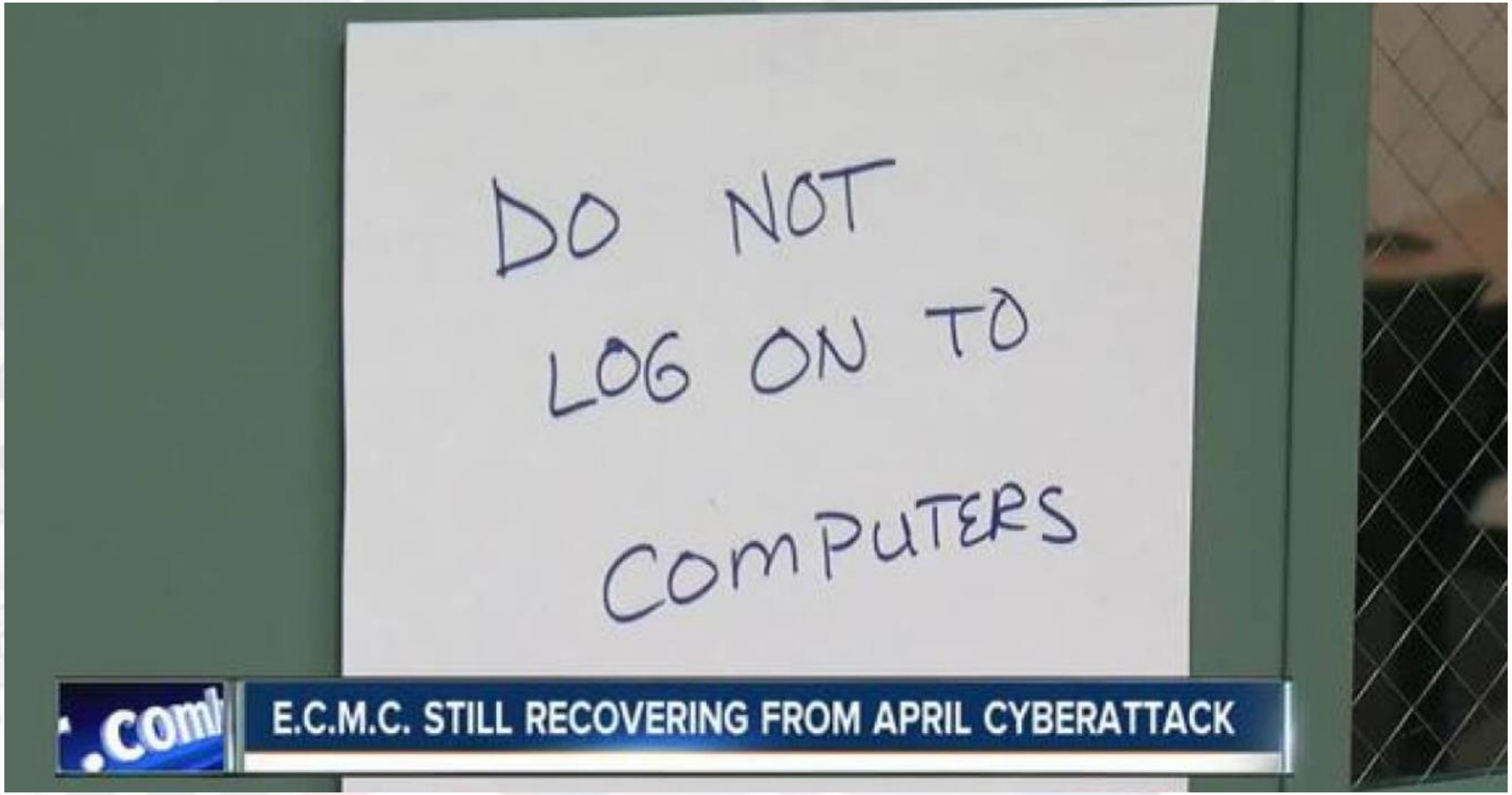
- All are here today as the vanguard for the Albany chapter of InfraGard.
- All are here today to share their time and experience.
- Please take full advantage of this opportunity to participate, ask questions, and share concerns.
- And join InfraGard. Become part of the community of practice.

ERIE COUNTY MEDICAL CENTER

April 9, 2017

ECMC spent nearly $10 million recovering from massive cyberattack

Erie County Medical Center: Anatomy of a ransomware attack


DO NOT
LOG ON TO
COMPUTERS
.com
E.C.M.C. STILL RECOVERING FROM APRIL CYBERATTACK

Erie County Medical Center

- At the time, ECMC shut down its computer network and implemented a backup plan, that was developed in case of a massive power outage, where **staff switched to using paper files in order to keep operations under way**. ECMC officials felt no patient information was compromised but admitted that **having to use the paper system did slow down hospital operations**.

SOB
ETOH
Foreign Body Inj
Overdose
Ankle Pain
AMS
HTN
GU
ETOH
LUE Burn
ETOH.
Head Injury
JD
NT
MM/DS
MM/ER
GI/ER
MM/DS
GI/NT
GI/JD
ANDY

Schuyler County

□ Schuyler County lateSEPTEMBER 9, 2017

□ Schuyler County **latest victim** to cyber hack

“The **Schuyler County Sheriff’s Department**, headquartered in Watkins Glen, had to get support from surrounding counties after the **hacking temporarily crippled its 911 emergency system** and **ability to dispatch deputies to calls**,”

City of Albany

March 30 2019

- Albany's **repair cost** after ransomware attack: **$300,000**
- **Albany, N.Y. hit with ransomware attack, mayor says**
- Computer systems in the City of Albany hit in **Ransomware Attack**

Albany County Airport

December 25 2020

- **Albany Airport Pays Ransom After Its MSP Was Hit By Ransomware**
- *The attack came to light after MSP LogicalNet reported its own management services network had been **breached**, with the ransomware **virus spreading** to the Albany (N.Y.) County Airport Authority's **servers and backup servers**.*
- The Albany (N.Y.) International Airport **paid a five-figure ransom** to restore data access after getting hit with Sodinokibi Ransomware **over Christmas** through its managed service provider.

Town of Colonie

January 17, 2020

Town of Colonie falls **victim** to **ransomware attack**

Town of Colonie got hacked; looks to avoid paying ransomware demand of about $400,000

presenter1

password

sheriff

sheriff

toshiba

toshiba

mailman

goldie

barracuda

barracuda

administrator

police123

Ryuk - October 29, 2020

- **Russian-speaking cybercriminals** in recent days have launched a **coordinated attack targeting U.S. hospitals** already stressed by the coronavirus pandemic with ransomware that analysts worry **could lead to fatalities**.
- In the space of **24 hours** beginning Monday, six hospitals from California to **New York** have been **hit by the Ryuk ransomware**, which encrypts data on computer systems, forcing the hospitals in some cases to **disrupt patient care** and **cancel** noncritical **surgeries**, analysts said.

JBS Meat Plant

June 1, 2021

- The company was **hacked** in May by **REvil**, one of a number of **Russian-speaking hacker gangs**
- **Meat supplier JBS paid ransomware hackers $11 million**
- ***Ransomware Disrupts Meat Plants in Latest Attack on Critical U.S. Business***
- **All** of JBS's beef **plants in the U.S**. were **shuttered** on Tuesday
- The **breach** at JBS was a **ransomware attack**, the White House said

Colonial Pipeline

- The Colonial **Pipeline attack** was the work of a ransomware operator called **DarkSide**, which Mr. Biden said was **based in Russia**.

- **DarkSide**, Blamed for **Gas Pipeline Attack**, Says It Is Shutting Down

Colonial Pipeline

□ **One password** allowed **hackers to disrupt** Colonial **Pipeline**, CEO tells senators

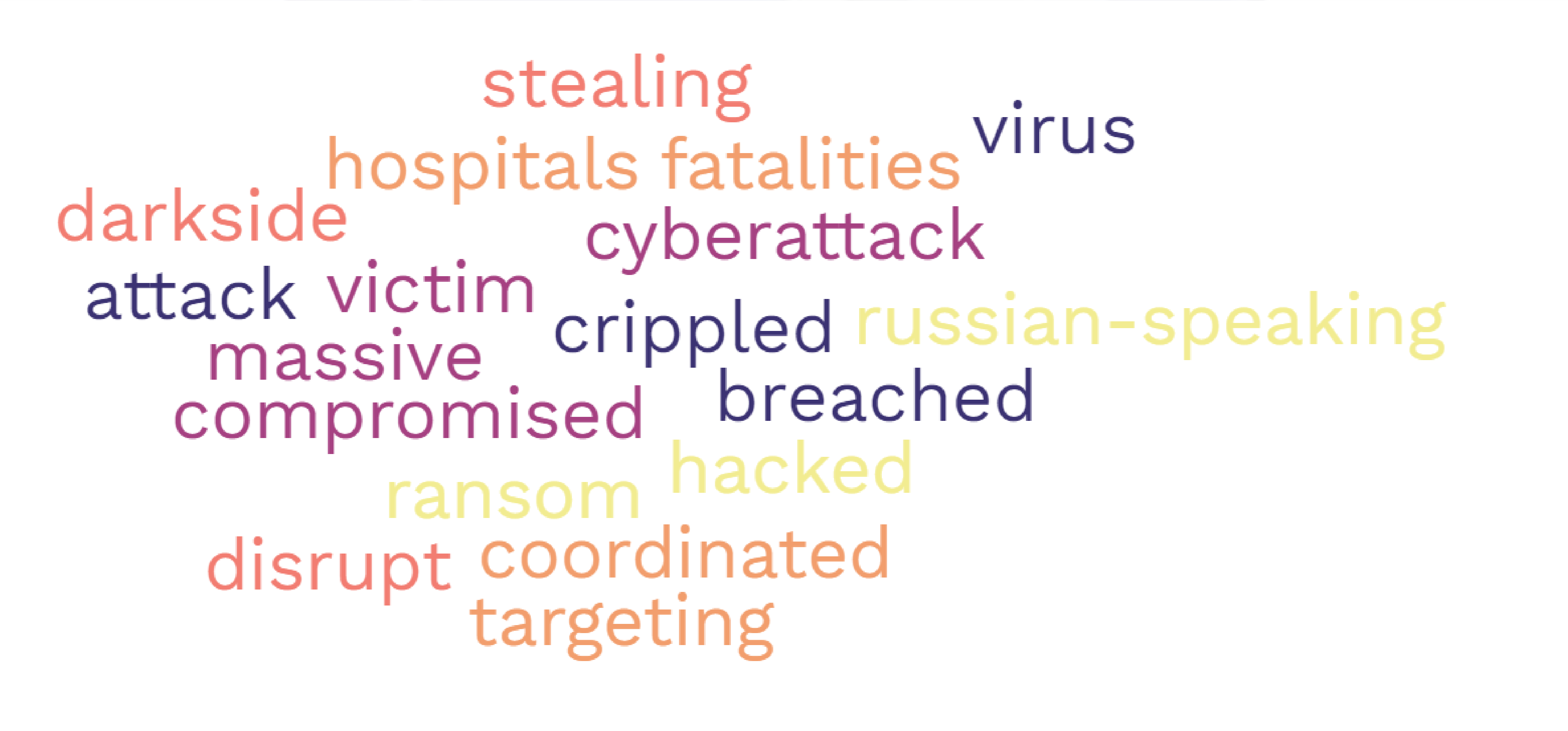
Colonial Pipeline

- The head of Colonial Pipeline told U.S. senators on Tuesday that **hackers** who launched last month’s cyber attack against the company and **disrupted fuel supplies to the U.S.** Southeast were able to **get into the system** by **stealing a single password.**

“stealing a single password”

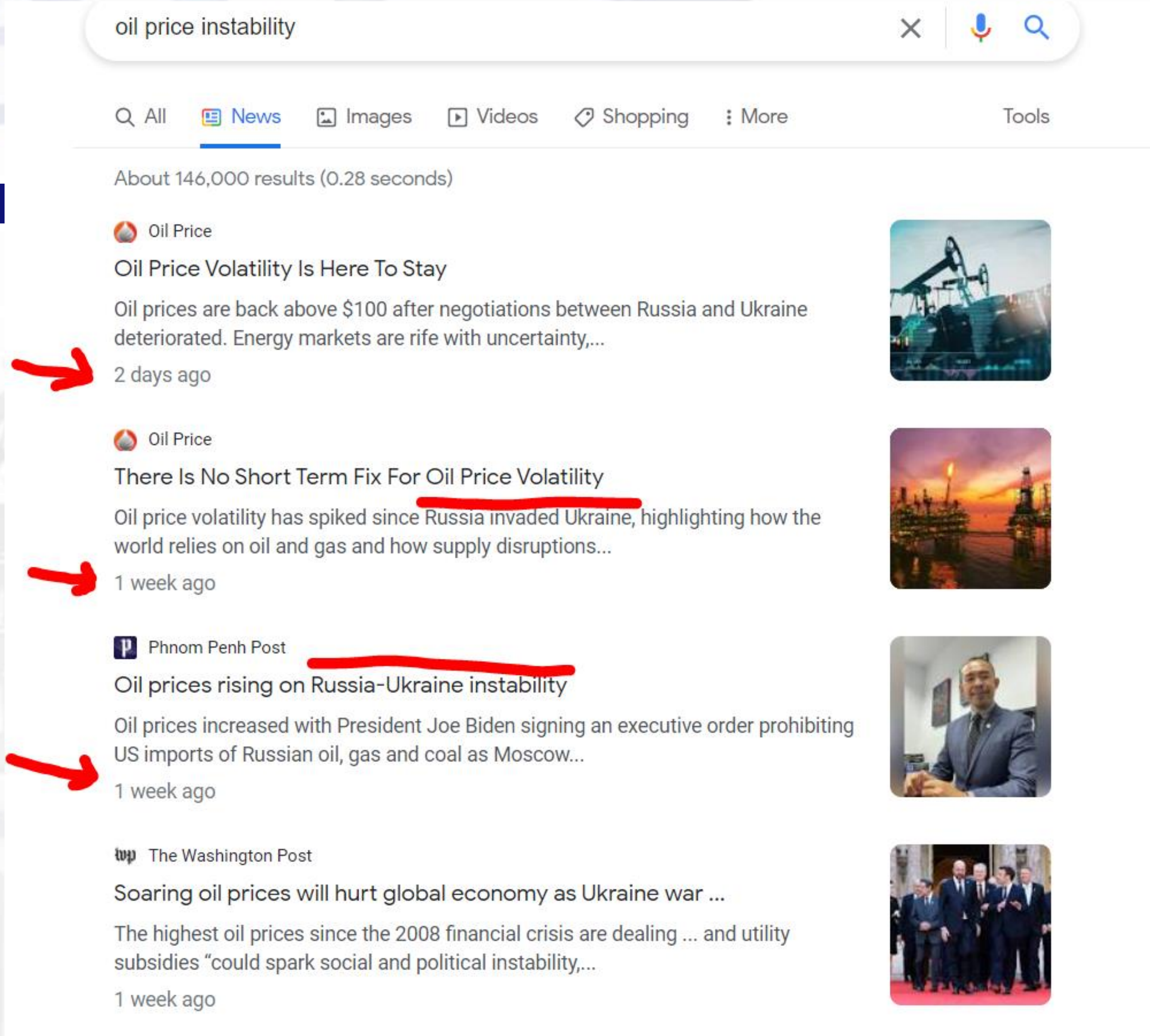
- toshiba:toshiba
- sheriff:sheriff
- presenter1:password
- barracuda:barracuda
- mailman:goldie
- administrator:police123

News Article Wordcloud



More Critical Today Than Ever…

- Russia/Ukraine War Increases Spillover Risks of Global Cyberattacks
- The world is bracing for a global cyberwar as Russia invades Ukraine
- The Cybersecurity Risks of an Escalating Russia-Ukraine Conflict
- Officials urge New Yorkers to protect themselves from Russian cyber attacks
- US warns of cyberattacks amid Russia-Ukraine war



oil price instability

About 146,000 results (0.28 seconds)

Oil Price

Oil Price Volatility Is Here To Stay

Oil prices are back above $100 after negotiations between Russia and Ukraine deteriorated. Energy markets are rife with uncertainty,...

2 days ago

Oil Price

There Is No Short Term Fix For Oil Price Volatility

Oil price volatility has spiked since Russia invaded Ukraine, highlighting how the world relies on oil and gas and how supply disruptions...

1 week ago

Phnom Penh Post

Oil prices rising on Russia-Ukraine instability

Oil prices increased with President Joe Biden signing an executive order prohibiting US imports of Russian oil, gas and coal as Moscow...

1 week ago

The Washington Post

Soaring oil prices will hurt global economy as Ukraine war ...

The highest oil prices since the 2008 financial crisis are dealing ... and utility subsidies “could spark social and political instability,...

1 week ago

This Slide Intentionally Blank

Scenario: Ransomware

- Small, rural upstate public-safety entity.
- Users report applications behaving strangely, folders unavailable
- Users observe files all have an odd extension
- Entity calls intermittent IT consultant, shares observations.

Scenario: Ransomware

- Consultant states:

“That sounds like Ransomware. That’s way over my head. I can’t help you…”

Scenario: Ransomware

- Entity calls Albany FBI
- Outline standard on-scene evidence collection, triage.
- Considerations for imaging onsite, versus collecting devices and carrying back to Albany.
- Impact and potential service interruptions.
- FBI case office model for known variants.
- Difference between incident response and evidence collection, processing a cyber crime scene.

Scenario: Ransomware

- No Managed Security Services (MSS)
- No logging
- Firewall is a Sonic Firewall dangling above head-level by an ethernet cable. From a hole in the ceiling.
- 16 of 20 user devices (laptops, workstations) are encrypted, including the sole domain controller.
- Computer-assisted dispatch (CAD) system is impacted.
- Records search is impacted
- Entity’s Internet Service Provider (ISP) is Spectrum.

Scenario: Ransomware

□ What evidence sources are available?

□ What are possible steps to start recovery and restoration?

□ Flatten everything and buy new stuff?

□ Hire a third-party IR company?

НЕ
ПРИКАСАТЬСЯ
ОПАСНО
ДЛЯ ЖИЗНИ!

FOR
SALE
ADMIN

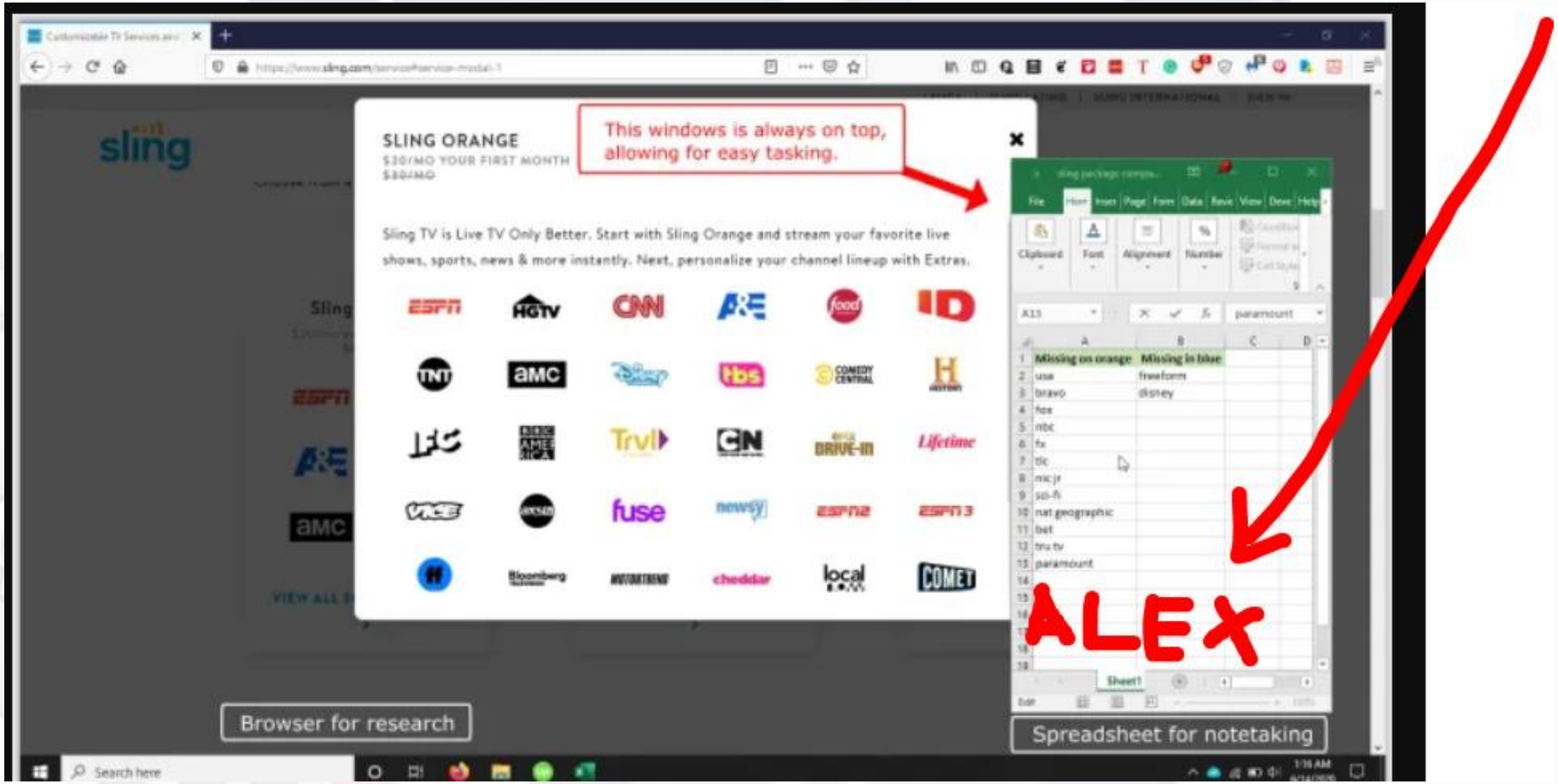
Tabletop Exercise: Admin Access

- Albany FBI receives a tip from a historically credible source that network access, administrator-level credentials for your organization are for sale to the highest-bidder on a Russian-language hacker Dark Web forum.
- FBI reaches out to a state / local DFIR resource who contacts you and suggests an immediate Webex to share available information.
- It is Friday at approximately 6:00 PM.

Notes:

- This is loosely-based on an actual network intrusion from 2021. It is still an open, active federal investigation.
- I’m going to pick on Alex and Champlain Valley
- I wasn’t sure how many teams would be able to attend and participate.

IT Director’s laptop: Confirmed



SLING ORANGE
$20/MO YOUR FIRST MONTH
~~$30/MO~~

Sling TV is Live TV Only Better. Start with Sling Orange and stream your favorite live shows, sports, news & more instantly. Next, personalize your channel lineup with Extras.

This windows is always on top, allowing for easy tasking.

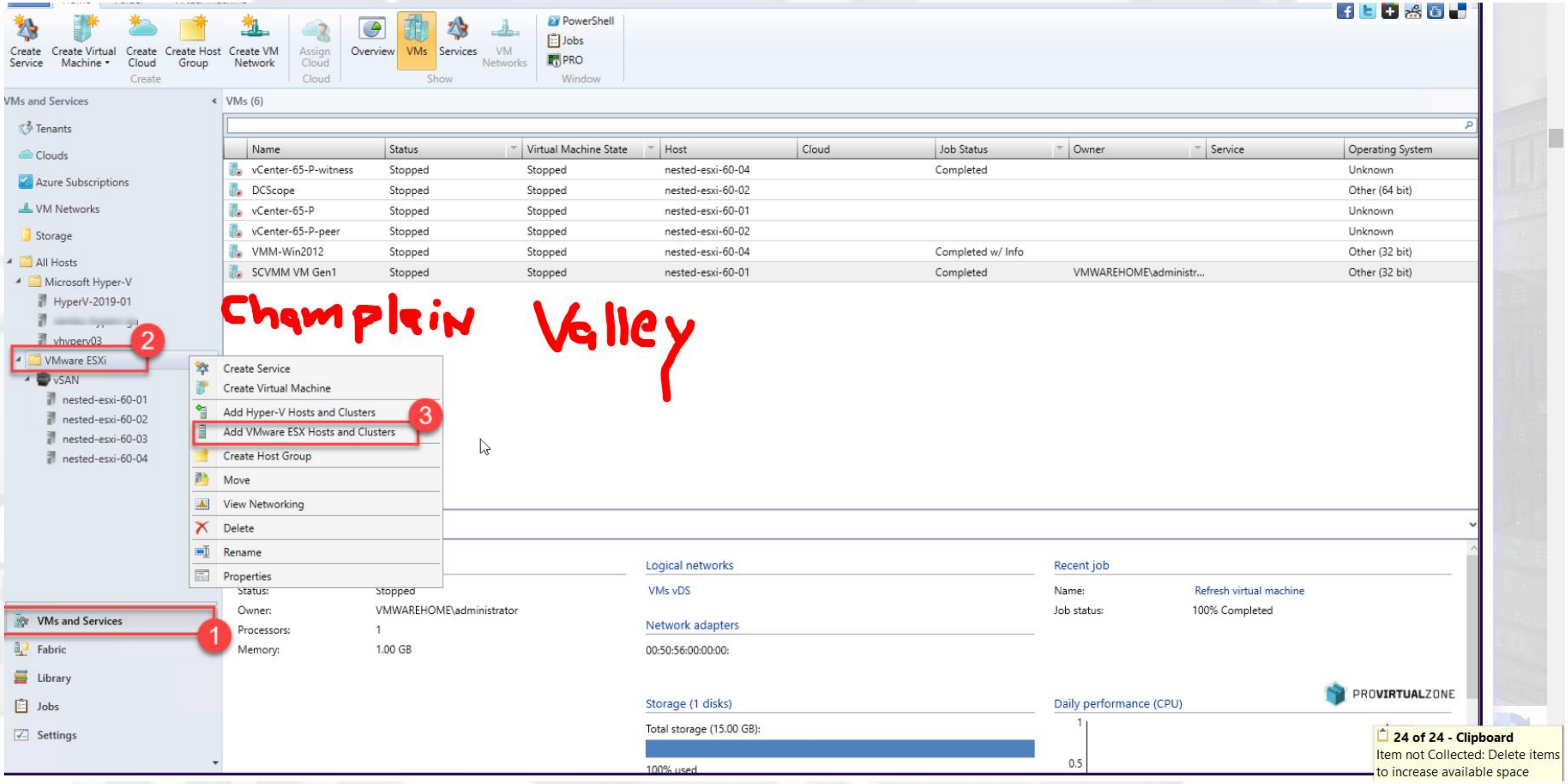
	A	B
1	Missing on orange	Missing in blue
2	usa	freeform
3	bravo	disney
4	fox	
5	nbc	
6	fx	
7	tlc	
8	nic jr	
9	sci-fi	
10	nat geographic	
11	bet	
12	tru tv	
13	paramount	

ALEX

Browser for research

Spreadsheet for notetaking

Admin-level Access: Confirmed



VMs (6)

Name	Status	Virtual Machine State	Host	Cloud	Job Status	Owner	Service	Operating System
vCenter-65-P-witness	Stopped	Stopped	nested-esxi-60-04		Completed			Unknown
DCScope	Stopped	Stopped	nested-esxi-60-02					Other (64 bit)
vCenter-65-P	Stopped	Stopped	nested-esxi-60-01					Unknown
vCenter-65-P-peer	Stopped	Stopped	nested-esxi-60-02					Unknown
VMM-Win2012	Stopped	Stopped	nested-esxi-60-04		Completed w/ Info			Other (32 bit)
SCVMM VM Gen1	Stopped	Stopped	nested-esxi-60-01		Completed	VMWAREHOME\administr...		Other (32 bit)

Champlein Valley

Status: Stopped
Owner: VMWAREHOME\administrator
Processors: 1
Memory: 1.00 GB

Logical networks
VMs vDS

Network adapters
00:50:56:00:00:00:

Storage (1 disks)
Total storage (15.00 GB):
100% used

Recent job
Name: Refresh virtual machine
Job status: 100% Completed

Daily performance (CPU)
1
0.5

24 of 24 - Clipboard
Item not Collected: Delete items to increase available space

Decision Points

- □ IR contact recommends immediately meeting at your office / data center.
- □ IR contact suggests taking your laptop (depicted in hacker forum) back to forensic lab for analysis.

Response

- How do we stop the theft of our information?
- How long have they been there and how do we find out?
- Who needs to be notified?
- What has been stolen so far?
- Is IT team authorized to take containment steps that will have an operational impact, such as disabling accounts or taking key systems offline.

Executive Flow

- What is the decision flow for taking organizations entire network offline?
- Does organization have a written Incident Response Plan?
- How will you communicate if the attacker can read your emails?
- Who should be notified?
- What is the role of IT at this time?
- Is this a data breach? Who decides?

IT Flow

- Is there a tool available to sweep the enterprise for file hashes, file names?
- Is there a tool available to enumerate scheduled tasks and installed services throughout the enterprise?
- What perimeter logging is in place? Firewall, NetFlow?
- Analysis discovers remote tunneling application on IT director laptop
- Event logs show attacker remotely accessing domain controllers
- Recommendation to rebuild domain controllers from scratch.

What if?

- Despite the timely and efficient response efforts, an employee with an infected laptop comes into the office Monday and plugs it into the network.
- It has remote tunneling application left by attacker.
- Attacker leverages connection to restore access to enterprise network
- So..

Tabletop Exercise: Ransomware

- With the rise in ransomware, it's crucial that your team reacts quickly and efficiently to stop the spread, preserve data, evaluate back-ups, evaluate ransom payments and much more.
- Ransomware can be financially disastrous. Being prepared and closing any process and security gaps can minimize the damage.

Scenario:

- Ransom messages appear on computer screens. The IT team members rush to the office and find that the files on the server and workstation are all encrypted.
- Attackers installed ransomware on shared server files **and it’s still spreading**.

Questions for Discussion:

- How do you contain and stop the spread?
- Do you have viable backups and system images?
- Would you ever consider paying the ransom, and who makes that decision?
- Is this covered by cyber insurance? (Do you have cyber insurance?)

Inject

- CEO receives a voicemail in which a digitally altered voice claims that they have stolen all the organization's files and will release them publicly if a ransom is not paid.

Questions for Discussion:

- How can your organization be certain that your data has been stolen?
- What is your organization’s policy regarding ransom payments?
- Who should be notified?
- What is the role of IT at this time?
- Is this a data breach? Who decides?

Inject

□ An internationally known cybersecurity journalist calls for a quote after hearing rumors on the dark web about the theft of your data. Do you comment? Who decides? Who issues the statement?

Further Discussion

- 7 Questions Frequently Arise From Table Tops Scenarios

Who authorizes decisions?

- Often, the IT team was not sure if they were authorized to take containment steps that would have an operational impact, such as disabling accounts or taking key systems offline.
- Further, they did not know who on the IR team could authorize such actions. Any confusion over decision-making authority can create delays and increase the potential spread and overall impact of a security incident, since speed is essential for effective containment.

When do we escalate?

- Incident response testing can reveal communication gaps that need to be addressed. For example, the IT team at a small company insisted on investigating suspicious activity quite thoroughly before escalating this issue and letting the management team know something was going on. To their credit, the team wanted to be sure they could provide as much information as possible when informing management. However, the management team was insistent they wanted to be made aware of a potential incident right away, even if details were limited. When the IT Lead asked the CEO: “But what if it turns out to be nothing?” The CEO stood up and replied enthusiastically, “Well that will be wonderful!”

To pay or not to pay?

- Ransomware scenarios often lead to interesting discussions. Our consultants often see disagreement among management teams on whether or not to pay the ransom, often due to ethical objections to paying criminals. While debate is healthy and essential, an actual ransomware incident usually has a quick timeline for making decisions. It is not the time for extended discussion of ethical concerns and options. It is much better to have that conversation during a tabletop exercise, when your organization’s data operations are not actually at risk.

We have backups, right?

□ During one incident response testing exercise, we found one organization had an unusually short back-up retention period – less than a week! We were not the only one who was surprised; the management team was under the impression that their retention periods were longer and followed best practices. Discussion during the exercise identified limited storage capacity as the problem and led to budgeting to support additional capacity.

Don’t we have that technology?

- Talking through incident detection and response can help management teams understand their organization’s technical capabilities and limitations. Here are a few examples we uncovered during incident response testing that have surprised management teams:

- **Limited detection capability** – We have heard about detection tools that have not been fully implemented or properly tuned to provide needed visibility, such as an IDS/IPS purchased and plugged in, but not yet put inline to actually monitor traffic. Other gaps include lack of alerting, no one assigned to review alerts, and IDS/IPS operating only as IDS, while management thought it was blocking suspicious traffic, not just detecting it.

- **Audit logs** – Some systems are not capturing audit logs, the logs are not retained long, or they are not included in monitoring via the SIEM.

- **Skills gaps** – Organizations may have one person on the team with needed knowledge on their security tools and how to use them. This can be related to reviewing firewall or IDS/IPS activity, retrieving audit logs, or creating and preserving forensic images. A tabletop exercise can help bring these gaps to light so that cross-training can be planned.

We have known cybersecurity gaps and vulnerabilities?

- Incident response testing exercises can also help identify a variety of security control gaps. In many cases, the gaps are known to the IT team, but management was not aware and therefore remediation was not planned and prioritized. Some examples:Unauthorized use of cloud storage
- Sensitive information stored locally, against policy
- Lack of technical enforcement of strong password requirements
- Local administrator rights on some endpoints
- Delayed patching or obsolete operating systems

What does our cybersecurity insurance cover?

- Cybersecurity insurance is a frequent topic during an incident response testing exercise, and we often see challenges in this area. A common scenario is where an organization has cybersecurity insurance, but no one on the response team has good knowledge of what it covers, when it should be activated, or how to activate it. In some cases, the organization does not have clear guidance on who can make decisions around when to activate insurance coverage or who is authorized to submit a claim. These gaps can cause delays or even cause an organization to miss out on response services their insurance can help with, such as forensic investigation services or media response support.

Resources -

Helpful Internet Sources

- https://www.lmgsecurity.com/surprising-lessons-from-incident-response-testing/
- https://www.lmgsecurity.com/incident-response-tabletop-exercise-scenarios/

CYBER SECURITY/INCIDENT RESPONSE RESOURCES

MS-ISAC: CIS Benchmarks (cisecurity.org) https://www.cisecurity.org/cis-benchmarks

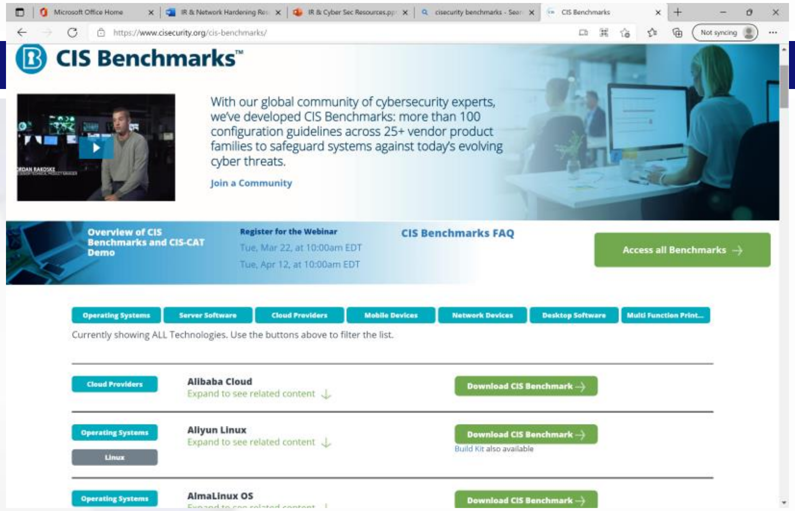
NIST: Cybersecurity Framework | NIST https://www.nist.gov/cyberframework

*How to Apply The NIST Cybersecurity Framework in K-12: https://securityboulevard.com/2020/02/how-to-apply-the-nist-cybersecurity-framework-in-k-12-school-districts/

SANS Institute: Cyber Security Resources | SANS Institute https://www.sans.org/security-resources

MS-ISAC K-12: https://cisecurity.org/ms-isac/k-12

Mandiant Article on Greater Visibility Through PowerShell Logging: https://www.mandiant.com/resources/greater-visibilityt



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

CIS Benchmarks™

With our global community of cybersecurity experts, we've developed CIS Benchmarks: more than 100 configuration guidelines across 25+ vendor product families to safeguard systems against today's evolving cyber threats.

Join a Community

Overview of CIS Benchmarks and CIS-CAT Demo

Register for the Webinar

Tue, Mar 22, at 10:00am EDT

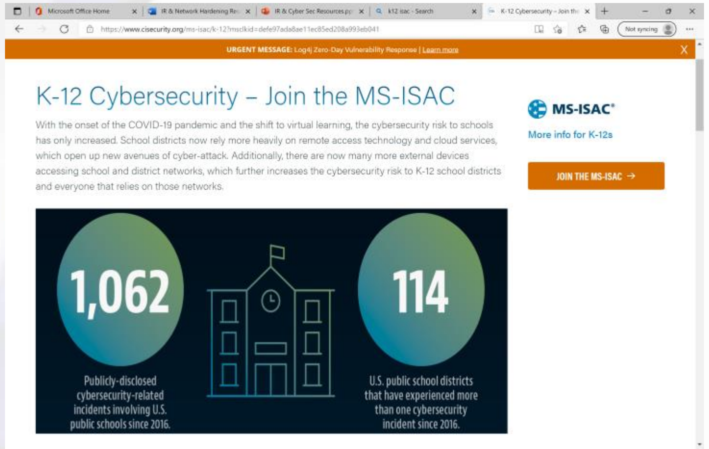
Tue, Apr 12, at 10:00am EDT

CIS Benchmarks FAQ

Access all Benchmarks →

Currently showing ALL Technologies. Use the buttons above to filter the list.

Cloud Providers	Alibaba Cloud Expand to see related content ↓	Download CIS Benchmark →
Operating Systems Linux	Aliyun Linux Expand to see related content ↓	Download CIS Benchmark → Build Kit also available
Operating Systems	AlmaLinux OS	Download CIS Benchmark →


Microsoft Office Home
IR & Network Hardening Re
IR & Cyber Sec Resources.pp
k12 isac - Search
K-12 Cybersecurity – Join the
Not syncing
MS-ISAC®

https://www.cisecurity.org/ms-isac/k-12?msclkid=defe97ada8ae11ec85ed208a993eb041

URGENT MESSAGE: Log4j Zero-Day Vulnerability Response | Learn more

K-12 Cybersecurity – Join the MS-ISAC

With the onset of the COVID-19 pandemic and the shift to virtual learning, the cybersecurity risk to schools has only increased. School districts now rely more heavily on remote access technology and cloud services, which open up new avenues of cyber-attack. Additionally, there are now many more external devices accessing school and district networks, which further increases the cybersecurity risk to K-12 school districts and everyone that relies on those networks.

More info for K-12s

JOIN THE MS-ISAC →

1,062 Publicly-disclosed cybersecurity-related incidents involving U.S. public schools since 2016.

114 U.S. public school districts that have experienced more than one cybersecurity incident since 2016.

CYBER SECURITY/INCIDENT RESPONSE RESOURCES

US-CERT: www.us-cert.gov

Carnegie Mellon University Software Engineering Institute:
www.cert.org

Information Security Policy Templates | SANS Institute
Community Preparedness Toolkit | Ready.gov
Cyber Incident Response | CISA
Federal Government Cybersecurity Incident and Vulnerability Response Playbooks (cisa.gov)

Vulnerability Assessment Resources

DHS CISA Cyber Hygiene Resources: Cyber Hygiene Services | CISA https://www.cisa.gov/cyber-hygiene-services

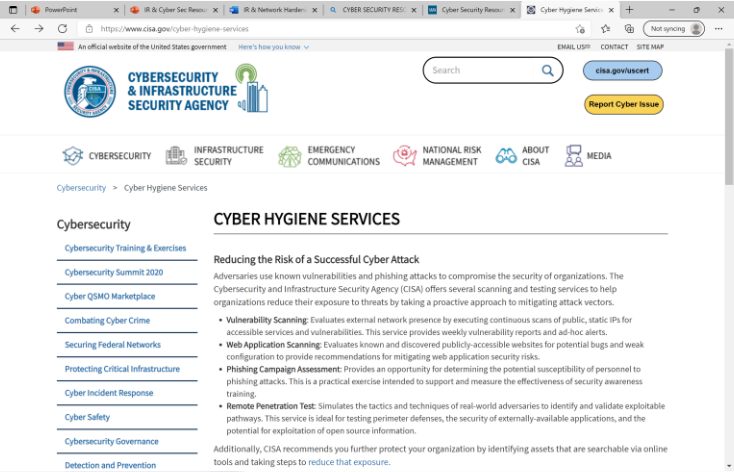
Nmap.org

OpenVAS.org

Nessus: https://www.tenable.com/products/nessus

Shodan.io to search your IP range to see what systems are internet facing (may find rogue or unsecured device)

*Before you have a company do a Pentest or vulnerability assessment, do your own to find everything you can so they have to do a deeper dive to find vulnerabilities.



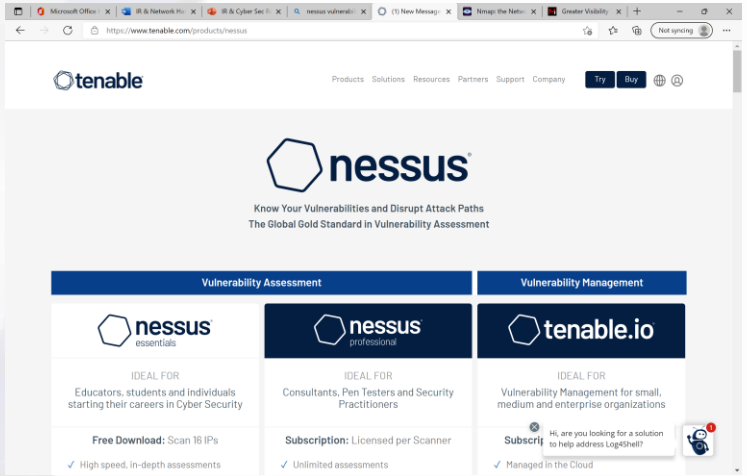
CYBER HYGIENE SERVICES

Reducing the Risk of a Successful Cyber Attack

Adversaries use known vulnerabilities and phishing attacks to compromise the security of organizations. The Cybersecurity and Infrastructure Security Agency (CISA) offers several scanning and testing services to help organizations reduce their exposure to threats by taking a proactive approach to mitigating attack vectors.

- **Vulnerability Scanning**: Evaluates external network presence by executing continuous scans of public, static IPs for accessible services and vulnerabilities. This service provides weekly vulnerability reports and ad-hoc alerts.
- **Web Application Scanning**: Evaluates known and discovered publicly-accessible websites for potential bugs and weak configuration to provide recommendations for mitigating web application security risks.
- **Phishing Campaign Assessment**: Provides an opportunity for determining the potential susceptibility of personnel to phishing attacks. This is a practical exercise intended to support and measure the effectiveness of security awareness training.
- **Remote Penetration Test**: Simulates the tactics and techniques of real-world adversaries to identify and validate exploitable pathways. This service is ideal for testing perimeter defenses, the security of externally-available applications, and the potential for exploitation of open source information.

Additionally, CISA recommends you further protect your organization by identifying assets that are searchable via online tools and taking steps to reduce that exposure.



Know Your Vulnerabilities and Disrupt Attack Paths
The Global Gold Standard in Vulnerability Assessment

IDEAL FOR
Educators, students and individuals starting their careers in Cyber Security
Free Download: Scan 16 IPs
✓ High speed, in-depth assessments

IDEAL FOR
Consultants, Pen Testers and Security Practitioners
Subscription: Licensed per Scanner
✓ Unlimited assessments

IDEAL FOR
Vulnerability Management for small, medium and enterprise organizations
Subscrip
✓ Managed in the Cloud

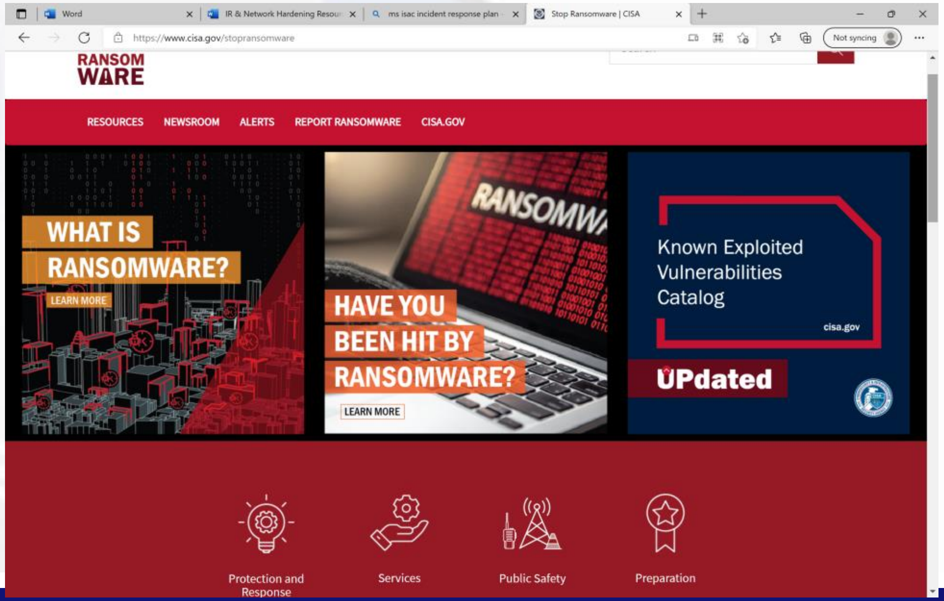
Hi, are you looking for a solution to help address Log4Shell?

RANSOMWARE RESOURCES

MS-ISAC: CISA MS-ISAC Ransomware Guide

CISA Stop Ransomware: Stop Ransomware | CISA https://www.cisa.gov/stopransomware

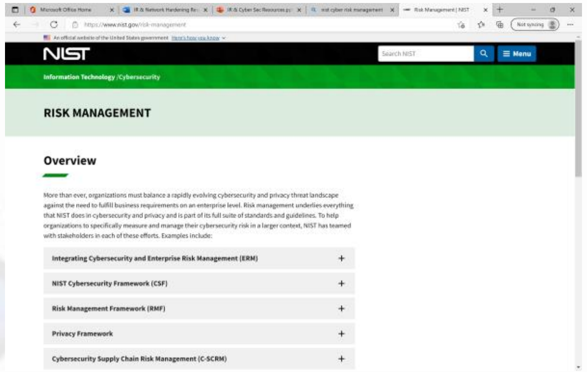
DHS-CISA Sheilds-Up Resources
CISA MS-ISAC Ransomware Guide https://cisa.gov



Risk Management Resources

NIST Risk Mangagement: https://www.nist.gov/risk-management

NIST: NIST Risk Management Framework | CSRC https://crsc.nist.gov/Projects/risk-management



https://www.nist.gov/risk-management

An official website of the United States government Here's how you know

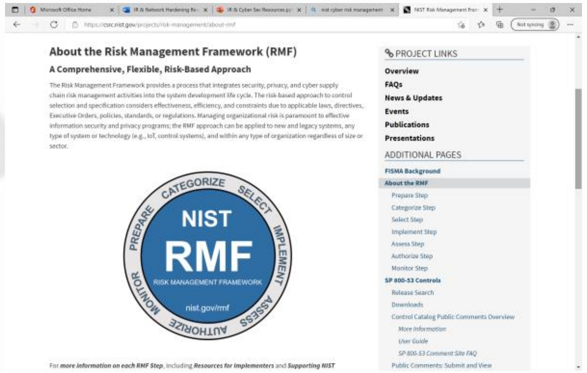
RISK MANAGEMENT

Overview

More than ever, organizations must balance a rapidly evolving cybersecurity and privacy threat landscape against the need to fulfill business requirements on an enterprise level. Risk management underlies everything that NIST does in cybersecurity and privacy and is part of its full suite of standards and guidelines. To help organizations to specifically measure and manage their cybersecurity risk in a larger context, NIST has teamed with stakeholders in each of these efforts. Examples include:

- Integrating Cybersecurity and Enterprise Risk Management (ERM) +
- NIST Cybersecurity Framework (CSF) +
- Risk Management Framework (RMF) +
- Privacy Framework +
- Cybersecurity Supply Chain Risk Management (C-SCRM) +

MITRE ATT&CK Framework: https://attack.mitre.org



https://csrc.nist.gov/projects/risk-management/about-rmf

About the Risk Management Framework (RMF)

A Comprehensive, Flexible, Risk-Based Approach

The Risk Management Framework provides a process that integrates security, privacy, and cyber supply chain risk management activities into the system development life cycle. The risk-based approach to control selection and specification considers effectiveness, efficiency, and constraints due to applicable laws, directives, Executive Orders, policies, standards, or regulations. Managing organizational risk is paramount to effective information security and privacy programs; the RMF approach can be applied to new and legacy systems, any type of system or technology (e.g., IoT, control systems), and within any type of organization regardless of size or sector.

For more information on each RMF Step, including Resources for Implementers and Supporting NIST

PROJECT LINKS

- Overview
- FAQs
- News & Updates
- Events
- Publications
- Presentations

ADDITIONAL PAGES

- FISMA Background
- About the RMF
  - Prepare Step
  - Categorize Step
  - Select Step
  - Implement Step
  - Assess Step
  - Authorize Step
  - Monitor Step
- SP 800-53 Controls
  - Release Search
  - Downloads
  - Control Catalog Public Comments Overview
    - More Information
    - User Guide
    - SP 800-53 Comment Site FAQ
  - Public Comments: Submit and View

Important Sites

- InfraGard Portal : www.infragard.org
- Join the Patriots Circle:
  - https://www.infragardnational.org/infragard-patriots-circle/
- Social Media presence:
  - Website: https://www.infragardalbany.org/
  - Facebook: https://www.facebook.com/InfraGardAlbany/
  - Twitter: https://twitter.com/InfraGardAlbany

QUESTIONS?
THOUGHTS?
DESIRED FUTURE
EVENTS/TRAINING?