



MIDWEST
RELIABILITY
ORGANIZATION

Welcome to the 2023 Hybrid Security Conference

**Cris Zimmerman Manager, Outreach &
Stakeholder Engagement**

MRO Logistics, Safety & E-Plan

- **Safety – First Aid, CPR and AED**
- **Food and beverages**
- **Restrooms**
- **Emergency plan – severe weather/evacuation**
- **Monitoring the Chat for questions**
- **Wi-Fi – Connect to: Sheraton-MeetingRoom**





HERO

HIGHLY EFFECTIVE RELIABILITY ORGANIZATION

FIVE BASIC PRINCIPLES:

1. **Preoccupation with failure**

Attention on close calls and near misses (“being lucky vs. being good”); focus more on failures rather than successes.

2. **Reluctance to simplify interpretations**

Solid “root cause” analysis practices.

3. **Sensitivity to operations**

Situational awareness and carefully designed change management processes.

4. **Commitment to Resilience**

Resources are continually devoted to corrective action plans and training.

5. **Deference to Expertise**

Listen to your experts on the front lines (ex. authority follows expertise).

Annual HERO Award

**Nominate Someone
Today!**



MIDWEST
RELIABILITY
ORGANIZATION

www.mro.net/about/hero/



HERO

HIGHLY EFFECTIVE RELIABILITY ORGANIZATION



Upcoming MRO Event Dates

- **Oct 10th – 12th MRO Co-Hosting with SERC, Physical Security Workshop @ MG&E offices in Madison, WI**
- **Oct 26th 8:30 am – 12:00 pm MRO 2023 Cold Weather Preparedness Virtual Workshop**
- **Dec 12th 10:00 am – 11:00 am 2023 Regional Winter Assessment**



2023 Security Conference Survey



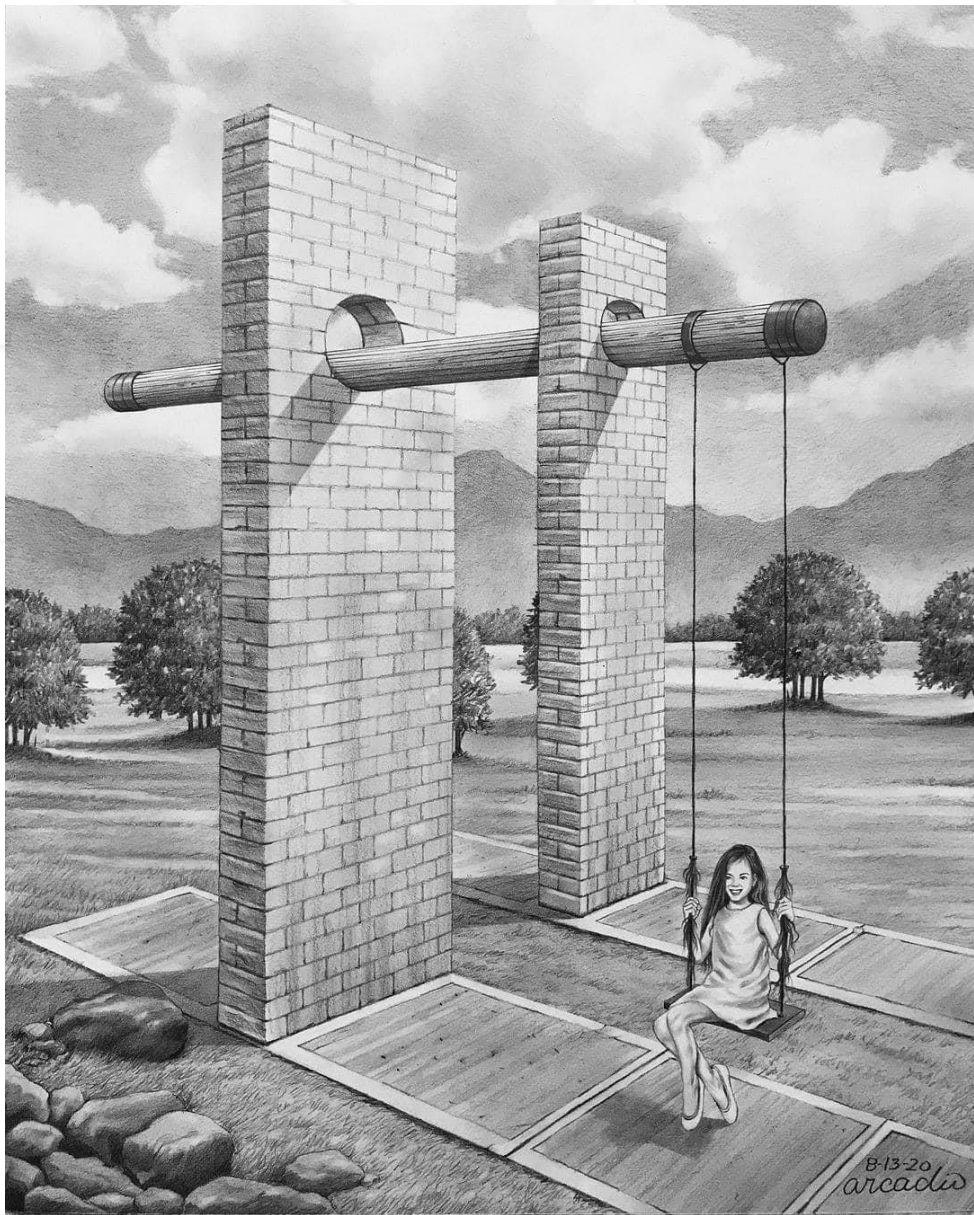
<https://www.surveymonkey.com/r/GTGH759>



Disclaimer for organizational group hosted events or materials:

Midwest Reliability Organization (MRO) is committed to providing outreach, training, and non-binding guidance to industry stakeholders on important industry topics. Subject Matter Experts (SMEs) from MRO's organizational groups and the industry may develop materials, including presentations, provided as a part of the event. The views expressed in the materials are those of the SMEs and do not necessarily express the opinions and views of MRO. Vendors presenting at, or attending, MRO events are not affiliated, associated, endorsed by MRO.





Steen Fjalstad
Director of Security, MRO

Ian Anderson
SAC Chair



CLARITY

ASSURANCE

RESULTS



MIDWEST
RELIABILITY
ORGANIZATION

Security in 3D

Richard Burt

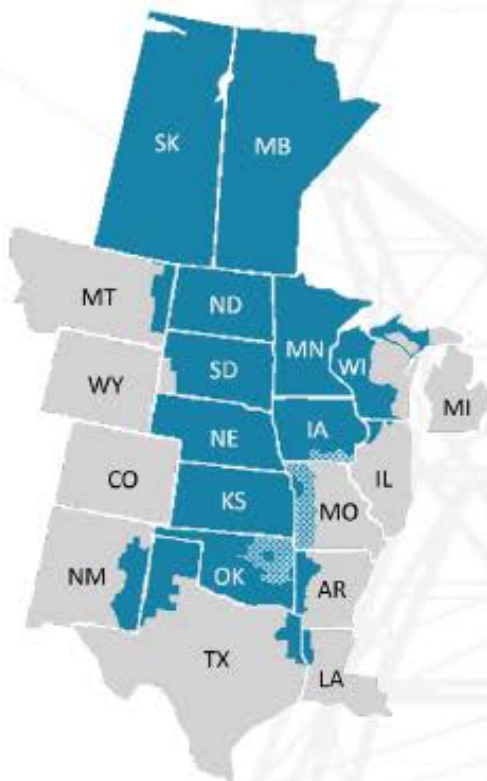
Senior Vice President & Chief Operating Officer



MRO 2023 Regional Risk Assessment

Top risks to the reliable and secure operation of the North American bulk power system in MRO's regional footprint.

Territory



About Us

As part of the [ERO Enterprise](#), MRO is committed to a shared mission to identify, prioritize and assure effective and efficient mitigation of risks to the reliability and security of the North American bulk power system in its regional footprint.

[Read more at www.MRO.net](http://www.MRO.net)

MRO Reliability Risk Matrix: Risk Rankings

Consequence / Impact (C)		Likelihood (L)				
		L1	L2	L3	L4	L5
		Very Unlikely	Unlikely	Possible	Likely	Almost Certain
C5	Severe					
C4	Major				4,5,6,16	
C3	Moderate		2	9,12,13	1	
C2	Minor			3,7,8,10,14,17	15	
C1	Negligible			11		



Assessment Overview

- Extreme weather, consumer demand, and changes in technology and generation resources continue to present a rapidly increasing number of challenges to grid planners and operators. Physical and cyber security risks also continue to evolve at an unprecedented pace.
- MRO's annual *Regional Risk Assessment* considers continent-wide risks to reliability and security of the North American bulk power system and determines which are more likely to occur and would have a higher impact in MRO's region.
- This report is focused on risk identification, prioritization and mitigation and highlights for industry the priorities needed to collaboratively address these challenges. It also serves to inform key decision makers of challenges the industry faces and the policies and regulations that will help define a variety of proposed solutions.

READ MRO'S [2023 REGIONAL RISK ASSESSMENT](#)

Top risks are reflected in orange above and described below. A full list of risks assessed can be found in the final report.

Key Findings: Top Reliability and Security Risks in MRO's Territory

Model Assumptions



RISK 1. Assumptions used in bulk power models to plan and operate the grid have not accounted for the rapid increase in inverter-based and distributed energy resources, challenging industry's ability to accurately assess current and future system characteristics.

Planning Reserves



RISK 4. Traditional methods to calculate Planning Reserve Margin are inadequate to properly plan for the generation capacity needed to meet increasingly uncertain system operations, especially during extreme weather events.

Energy Reliability



RISK 5. Increased uncertainty from changing energy supply and customer demand challenge the grid's ability to meet load for all hours of the year. There is no comprehensive planning that assesses assurance of available energy and fuel sources over all time periods to maintain grid reliability.

Generation Unavailability



RISK 6. Generation availability assumed during cold weather, particularly in the southern U.S., has been shown to be unrealistically high due to a lack of generation winterization and natural gas curtailments.

Transmission Line Ratings



RISK 12. Use of constant overhead transmission line ratings year-round (non-seasonal) limits available transmission capacity and leads to inefficient real-time decisions when system conditions deviate from assumptions that drive rating calculations, such as cooler temperatures or during emergency operations.

Insider Threats



RISK 9. Employees or contractors using their knowledge and authorized access of critical systems to do harm to the bulk power system is a continued, substantial threat to organizations and the reliability of the grid.

Malware/Ransomware

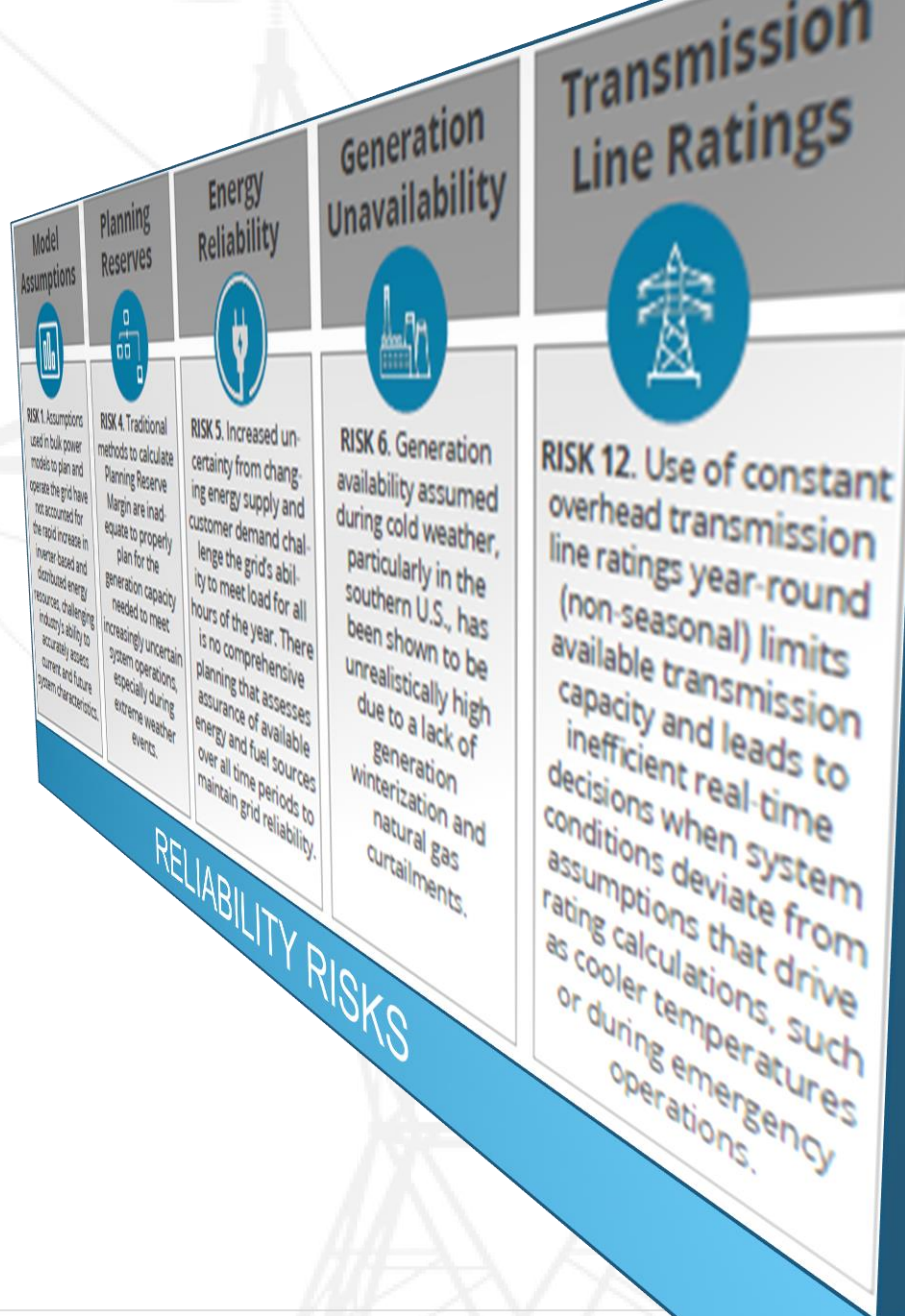


RISK 13. Phishing attacks can introduce malware or ransomware to corporate IT systems, which can impact critical systems necessary for reliable bulk power system operations through direct or in-direct connections those systems have to IT networks.

Supply Chain Compromise



RISK 16. A cyber security event carried out through the vendor supply chain can broadly impact bulk power system reliability, especially where the vendor is a market leader providing systems used for system operation.



Extensive Exchange of Models

New Critical 3rd Party Partners

Lost “Feel” for What’s Normal

Common Mode Configurations

Expansive Real-Time Data

Critical Remote Sensors

Cyber-Informed Transmission Planning

Roadmap for Integrating Cyber Security into
Transmission Planning Activities

May 2023



National Cyber-Informed Engineering Strategy

from the U.S. Department of Energy

JUNE 2022

December 2022

PES-TR105



Towards Integrating Cyber and Physical Security for a More Reliable, Resilient, and Secure Energy Sector

PREPARED BY THE
IEEE/NERC Joint Task Force on Security Integration into
BPS Engineering Practices



© IEEE (2022) The Institute of Electrical and Electronics Engineers, Inc.
No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher.

TR-105 – Integrating Cyber and Physical Security into Bulk Power System Engineering Practices

Consequence-driven Cyber-informed Engineering (CCE)

Mission Support Center Concept Paper



Prepared by:
Mission Support Center
National & Homeland Security Directorate
Idaho National Laboratory
October 18, 2016



INL/EXT-16-39212



Questions



Edward J. Gray
Special Agent in Charge



Rob M. Lee
CEO & Co-Founder,
Dragos

Security at an 8th Grade Level

Lessons Ranging from the Battlefield to Securing K-12

Patrick Tatro



Agenda

Introduction

Who am I, where I've been, & what I do

Ranger School

Lessons learned that contribute to success in my career

Operation Iraqi Freedom

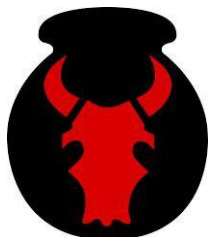
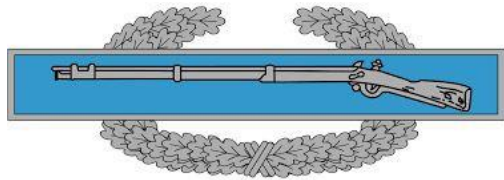
Experiences that influence my approach to cybersecurity

Securing K12

Fundamentals and playing to strengths



Introduction



Ranger School



Army Ranger School



The Five Principles of Patrolling



- Planning
- Reconnaissance
- Security
- Control
- Common Sense



Planning



“Quickly make a simple plan and effectively communicate it to the lowest level.

A great plan that takes forever to complete and is poorly disseminated isn't a great plan.

Plan and prepare to a realistic standard, and rehearse everything.”



Reconnaissance



“Your responsibility as a Ranger leader is to confirm what you think you know,

and to find out what you don't.”



Security



“Preserve your force as a whole, and your recon assets in particular.

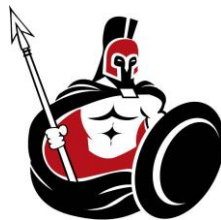
Every Ranger and rifle counts; anyone could be the difference between victory and defeat.”



Control



“Clear concept of the operation and commander’s intent, coupled with disciplined communications, to bring every man and weapon you have available to overwhelm your enemy at the decisive point.”



Common Sense



“Do what you’re supposed to do, without someone having to tell you, despite your own personal discomfort or fear.”



Doctrinally Sound not Doctrinally Bound

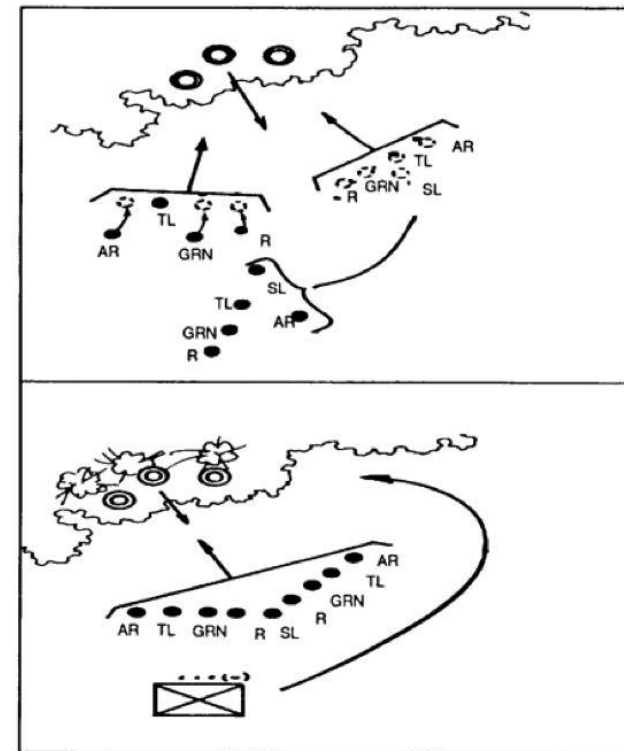


Figure 4-4. React to contact.



Securing the Hilltop

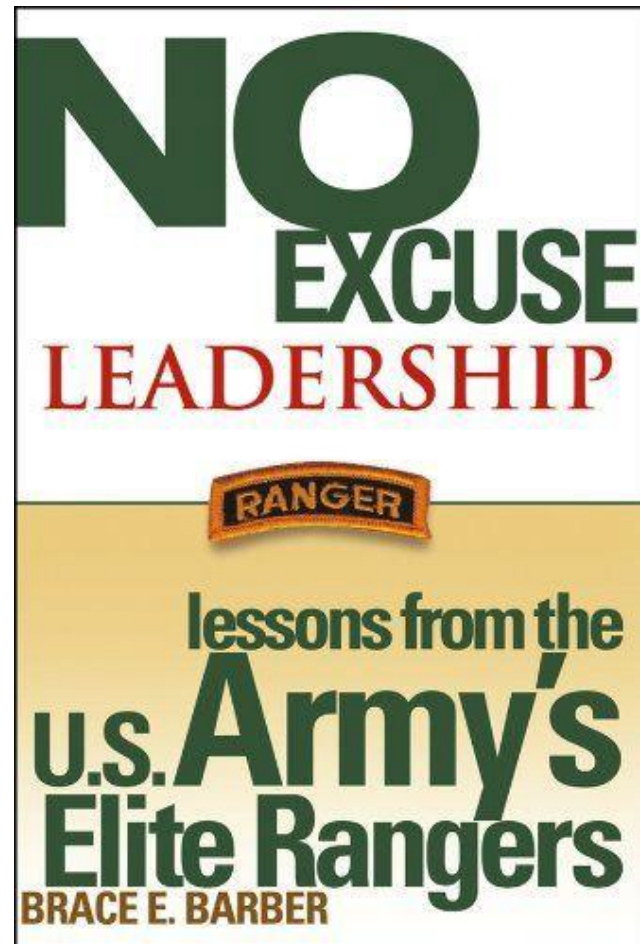
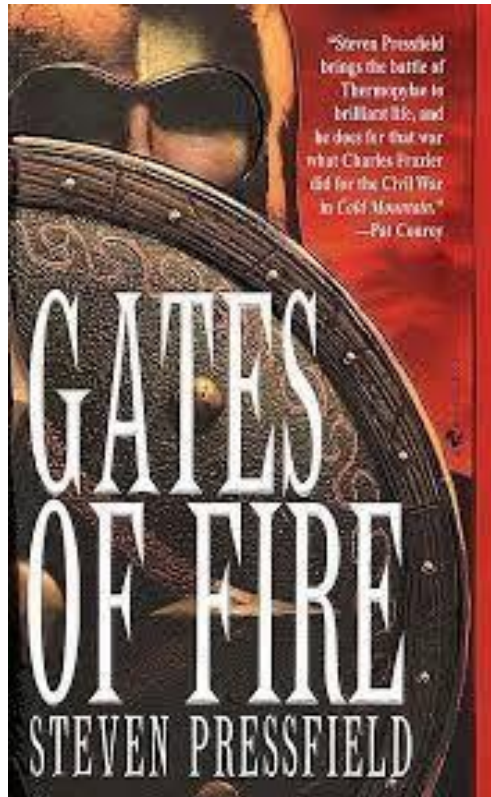


Applying the Principles of Patrolling

<u>Principles</u>	<u>Professional</u>	<u>Leader</u>
Planning	<ul style="list-style-type: none">• Manager's Priorities• Organized Tasks (Excel / JIRA)	<ul style="list-style-type: none">• Year Goals• Budget• Backlog Groomed
Reconnaissance	<ul style="list-style-type: none">• How are breaches happening?• Prep for meetings	
Security	<ul style="list-style-type: none">• My job for Identify, Prevent, Detect, Respond, Recover• Informing decision makers	<ul style="list-style-type: none">• Controls deployed & effective• Capabilities for Identify, Prevent, Detect, Respond, Recover• Informed decisions
Control	<ul style="list-style-type: none">• Maintain communications (email, collaboration app, text)• Bandwidth management• Controlling the situation vs situation controlling you	
Common Sense	<ul style="list-style-type: none">• Ask clarifying questions• KISS	<ul style="list-style-type: none">• Minimize exercises in futility• Avoid tickets to create tickets



Learning More



Surviving the Cut
Ranger School



Operation Iraqi Freedom



Iraq Deployment



First Day on the Job ~ Follow Me



Not all Intelligence is the Same



Nobody Pulls Security Like We Do



Different Threat Environments



Different Tactics



Days of Days

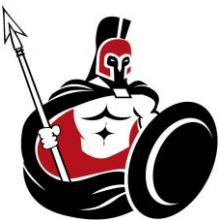


Understanding Capabilities and Controls



Why Were We Successful

- 5 Principles of Patrolling
- Every extra wrinkle is another place to fail
- Focused on intelligence gathering and briefings
- Threat assessments to drive tactics
- Designed communications and reporting to improve situational awareness
- Implemented controls effectively and appropriately
- Learned what to ignore and what to worry about



Lessons Learned that Continue to Apply

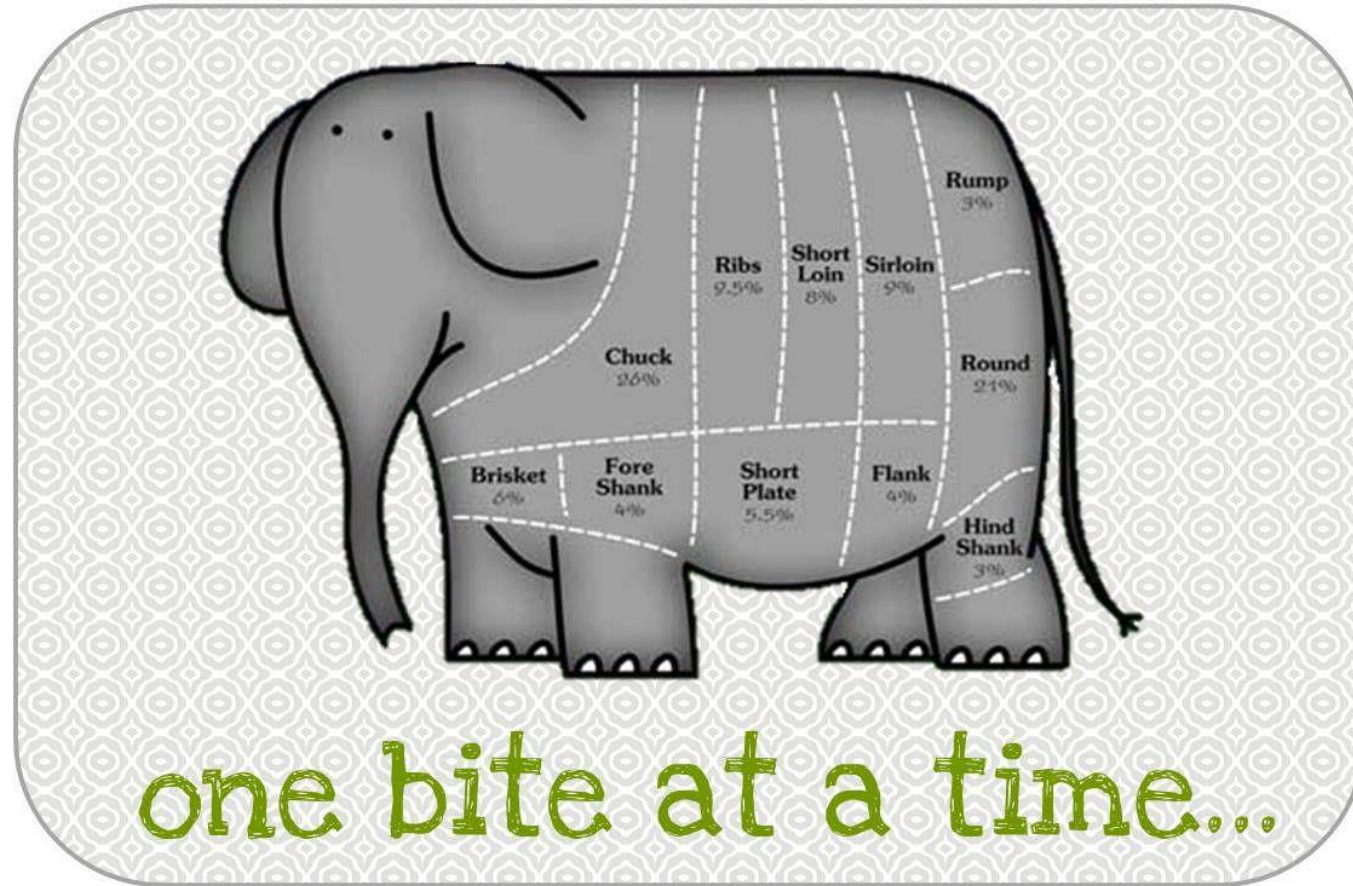
- Better than yesterday
- Security standards and expectations vary regardless of the domain
- Over reliance on hard controls
- Balance complacency and paranoia
- Give employees things to look for
- Emphasis into understanding how things work and how things break



Securing K12

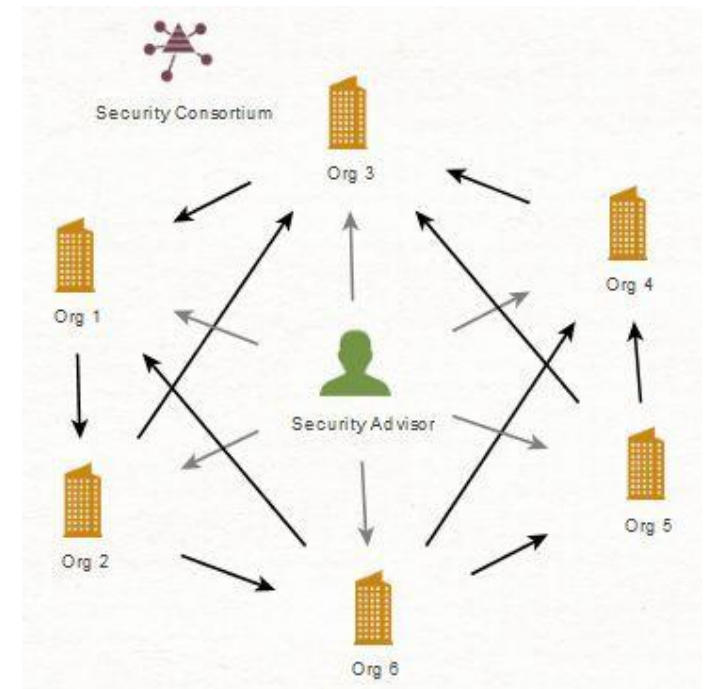


Eating the Elephant...



Stronger Together a Security Consortium Story

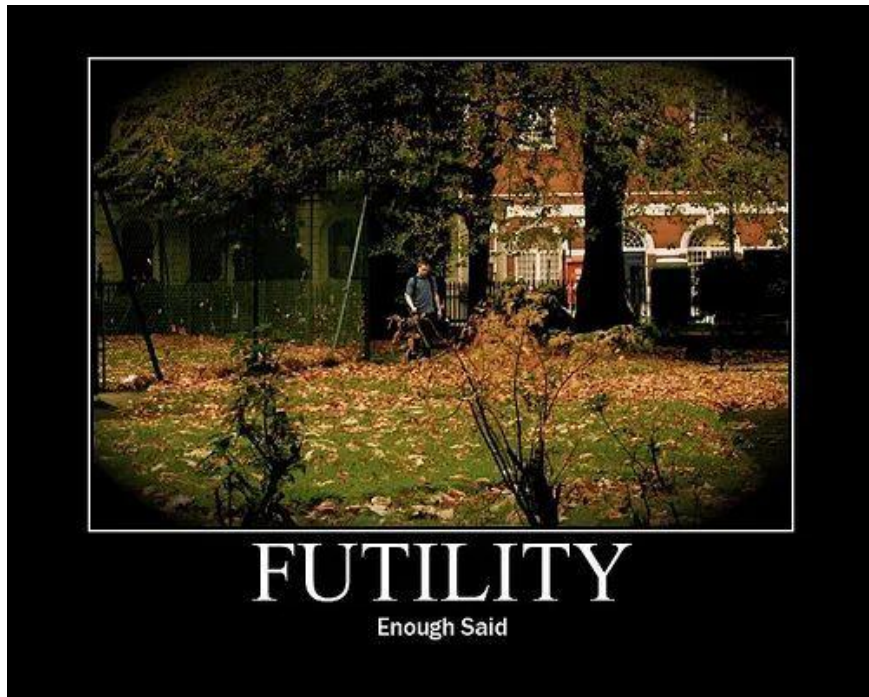
- Group of 6 districts fosters:
 - trust
 - sharing of information
 - accountability
 - competitiveness
 - discussion
- Individual and shared access to a trusted Cybersecurity Advisor
- Monthly group meeting & a one day Summer Workshop
- Shared resources such as procedures, guides, & training material
- Collectively improve and exchange:
 - Cybersecurity Program Progress
 - Risk management
 - Policies & Procedures
 - Configs
 - Playbooks
 - Contract templates



LEAD.UNDERSTAND.SECURE



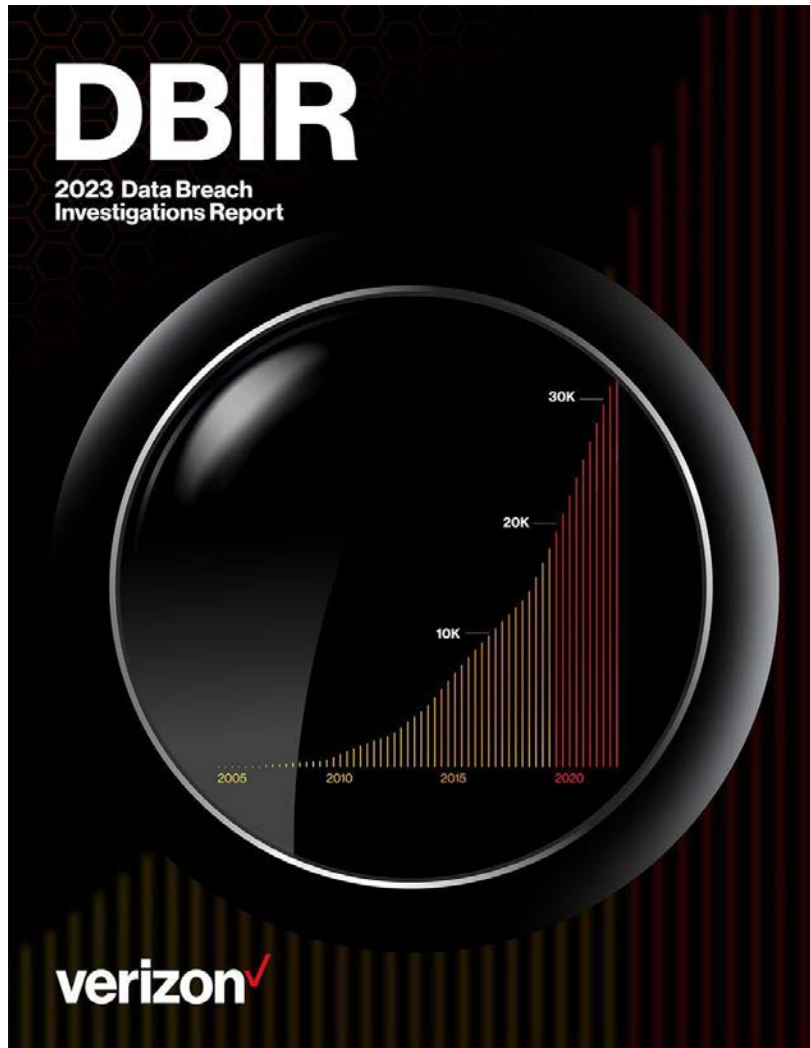
Challenges for Organizations of all Sizes



- Acknowledging and accounting for the gap between doctrine and reality
 - Doctrinal sound, not doctrinal bound
 - Detect, Respond, Recover exist for a reason
- Decision making
 - “Doers” aren’t always empowered to make fast enough operational decisions
 - “Thinkers” often don’t know what decisions are theirs
- How do I compare to my peers?
 - Usually asked to get a sense of comfort
 - Comfort isn’t the key to outrunning a bear
- Lack of ability to stick to a maturity plan
 - Start and stopping of security efforts
 - Budget fluctuations
 - Changing and conflicting priorities



Big Organizations



- Strengths:
 - Large budgets
 - Dedicated security staff
 - Compliance drivers
 - Plenty of security tools and blinky lights
- Challenges:
 - “Buying” your way to secure
 - Large security staffs become bureaucratic
 - Compliance dictates priorities
 - Silos of org charts and controls
 - Security tools rarely fully optimized

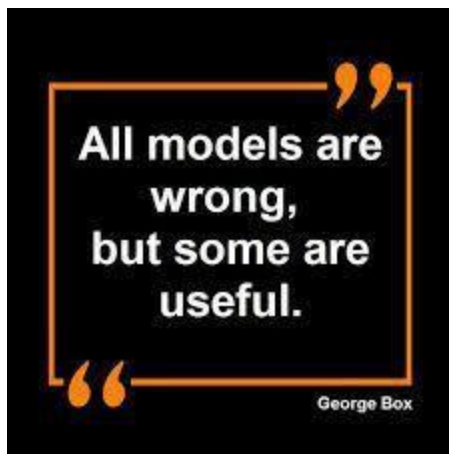


Security is a Leadership and People Problem

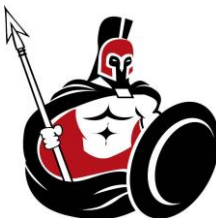
- Lead:
 - Strong and confident leadership is needed as security is a series of decision making
 - Planning that is complete and sustainable
- Understand:
 - Know the threat and the true impact
 - Fundamentals of technology and applying defense in depth
 - Slow is smooth, smooth is fast
 - There is always a human involved
- Secure:
 - Strategic decisions to address risk, compliance, and alignment with district mission
 - Operational decisions to prevent, detect, and respond
 - Situational awareness between complacency and paranoia



K-12 Organizations (Good IT = Good Security)



- Challenges:
 - Lack of resources
 - Insecure vendors due to lack of pressure
 - Demand for high availability and “unhindered” learning
 - Misconception there isn’t valuable data
- Strengths:
 - Mature policy, procedures, SOPs
 - Service Desk and Field Services are customer centric
 - Pride in managing & getting the most technology
 - Culture of learning and education
 - Shared mission and vision that provides purpose



Security Posture Progression

Exposure Without Maturity

■ Opportunistic ■ Targeted



Exposure With Maturity

■ Opportunistic ■ Targeted



Summer Workshops with Peers



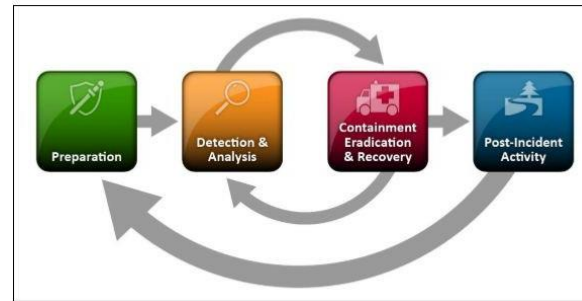
- Security Program & NIST CS
- Data Breaches & Incident Re
- Making Cybersecurity Routine
PCI
- Risk Register, Ransomware,
Audits
- Tabletop Exercises
- Learning Continuity Plans &
Attacks



Security Journey



NIST Cybersecurity Framework



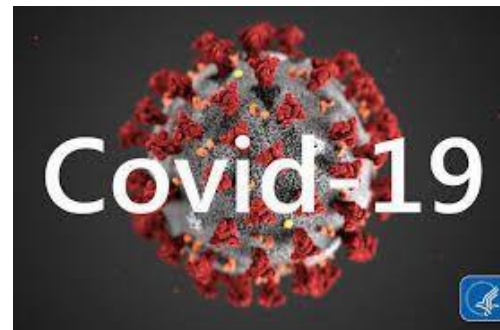
Breach and Incident Response



Training and Awareness



Vulnerability Scanning and Management



Remote Learning & Work Securely



Vendor Breaches and Vulnerabilities



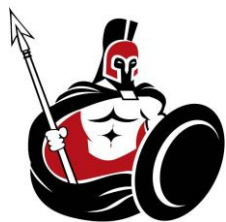
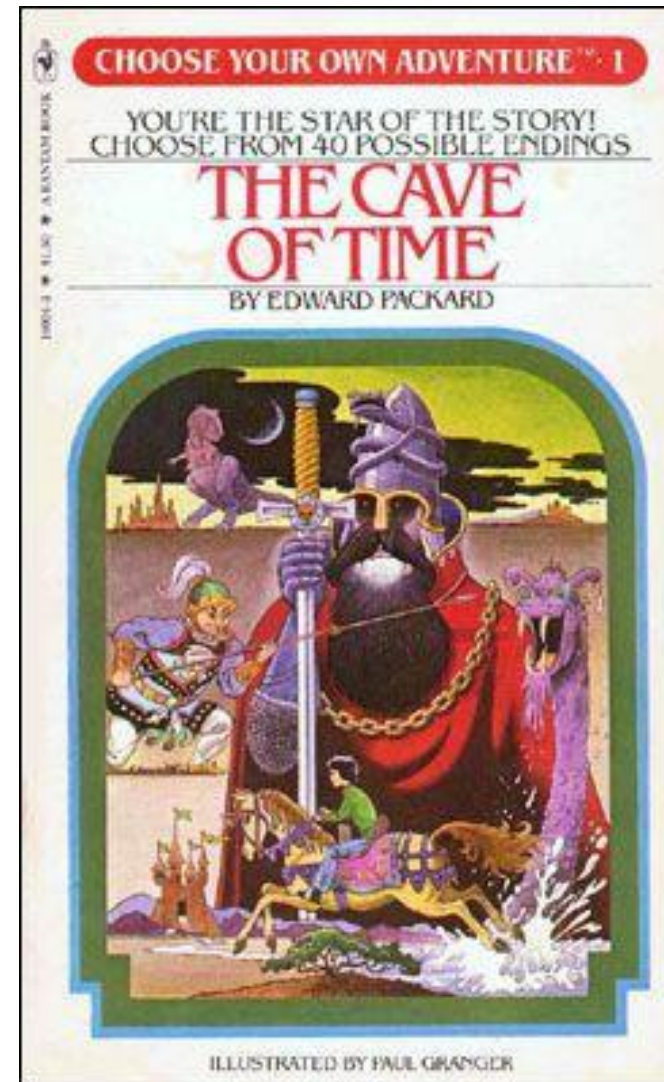
Security as a Routine Practice

	<u>Time</u>	<u>Knowledge</u>	<u>Possible Solutions</u>
Scenario 1	Don't Have Time	Don't Know What to do	Adjust priorities Security knowledge and/or direction More people
Scenario 2	Have Time	Don't Know What to do	Security knowledge and/or direction
Scenario 3	Don't Have Time	Know What to do	Adjust priorities More people
Scenario 4	Have Time	Know What to do	Evaluate work and project management Review leadership direction and guidance



Navigating the Covid Pandemic

- Going Fully Remote in Lockdowns:
 - Maintain a small perimeter surface and multi-factor authentication
 - VPNs and cloud services
 - Remote device management
 - Checklist for cloud services
- Start of School Fall 2020:
 - Continued remote workers
 - Hybrid learning with distance learning
 - Virtual Desktop Environments
 - Always on VPN
 - Microsoft Intune?
 - Azure AD?



Mitigating the Risk and Prioritizing Bites

Drive By Ransomware

- Spam and exploit kits distribute the ransomware.
- Tax, invoice, package delivery themes with attachments or links to documents.

Risk Breakdown

Probability: High **Impact:** Low (Smaller surface area)

Network Compromise Ransomware

- Exfiltrating data to a FTP server to release should ransom not be paid.
- Deploying ransomware to multiple servers in the network using admin accounts.

Risk Breakdown

Probability: Low **Impact:** High

Controls

Spam Filter ~~X~~

IDS/IPS ~~X~~

Removal of Local Admin ~~X~~

Windows Server and AD Logging ~~X~~

EDR ~~X~~

Web Filter ~~X~~

Phishing Playbook ~~X~~

Firewall ACLs ~~X~~

SIEM Alerts and Dashboards ~~X~~

Threat Hunting ~~X~~

Managed SOC ~~X~~

Training & Awareness ~~X~~

Vuln Scanning ~~X~~

Anti-Virus ~~X~~

Malware Playbook ~~X~~

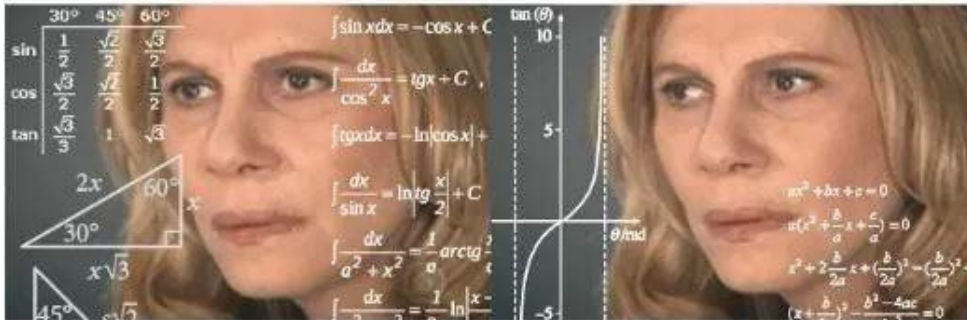
Backups ~~X~~

Cyber Insurance ~~X~~



A Good Plan Executed Now...

HOW MY FRIENDS PLAY STRATEGY GAMES



HOW I PLAY STRATEGY GAMES



MEDUSA BLOG

TWITTER TELEGRAM

DAYS

HOURS

MINUTES

SECONDS

00

00

00

05

MINNEAPOLIS PUBLIC SCHOOLS

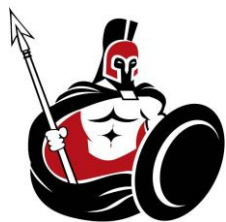
Minneapolis Public Schools

Minneapolis Public Schools (MPS) or Special School District Number 1 is a public school district serving students in pre-kindergarten through twelfth grade from Minneapolis, Minnesota. Minneapolis Public Schools enrolls 36,370 students in public primary and secondary



Bringing K12 Security to the Day Job

- Take advantage of good IT
- Less talk more patching
- Be better than we were yesterday
- Keep intelligence simple
- Continue to learn how things work
- Defense in depth is still a thing
- “Next Gen” isn’t a need to have
- Stay grounded



Thank you!



Questions, Contact Info, & What I'm up to

Patrick Tatro

patrick.tatro@darkknightsolutions.com



splunk[®]>





We Energize Life

Sean Trauschke

OG&E President and CEO



Emergent Threats and Soft Target Hardening



Dr. Jennifer L. Hesterman
Colonel, U.S. Air Force (retired)

Overview



Humans and Security

International and Domestic Threats

Understanding Soft Targets

What Are We Doing Wrong?

Takeaways



*Security is always seen as too much
until the day it's not enough.*

~ William Webster, Former FBI and CIA Director

The Security Landscape



Humans and Security



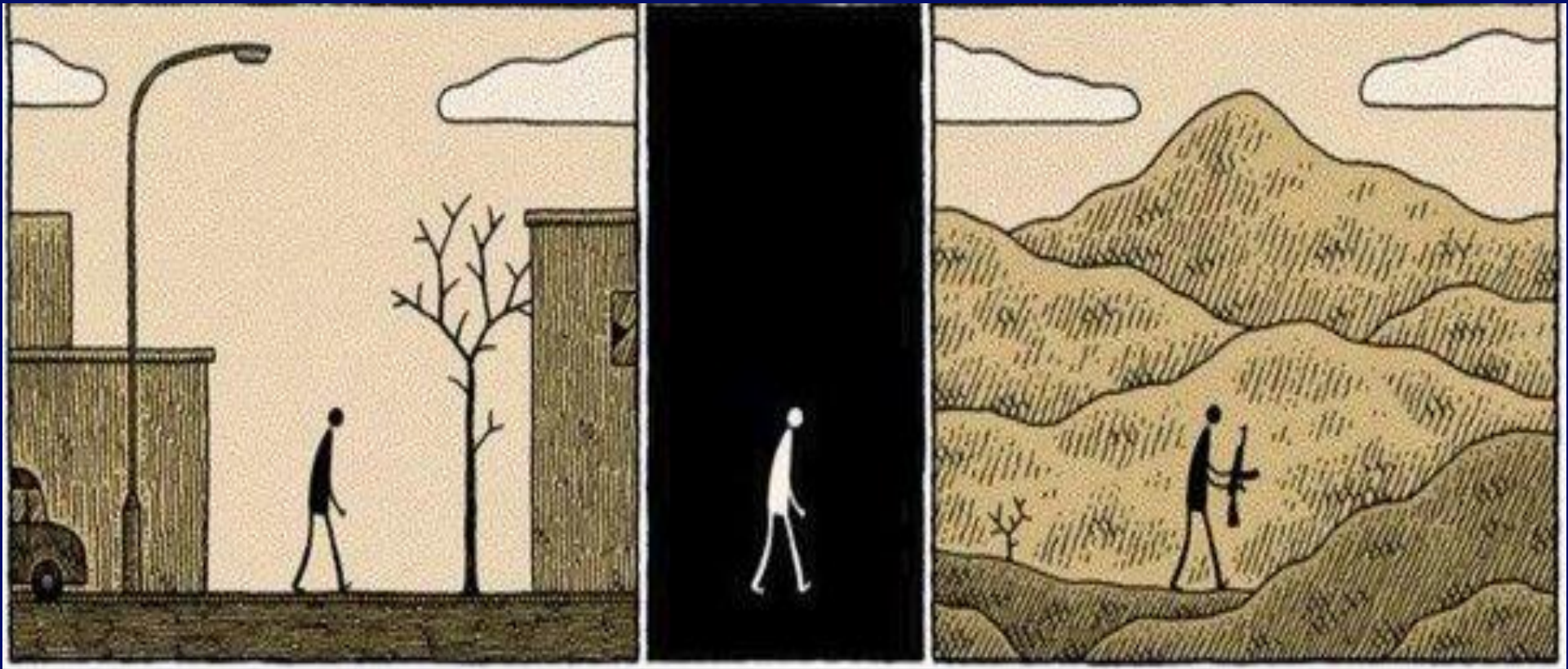
Emotional traps

- Resignation or acceptance - “new normal”
- Hopelessness - There’s nothing we can do; defeatism
- Infallibility - It will never happen here
- Invulnerability - It can’t happen to me/us
- Inescapability - If it’s unavoidable, why try to mitigate
- Denial - Lack of preparedness = delayed/ineffective response

Humans and Security



- Hope events are “one off” or bad actors are “unique”
- Move on quickly, no lessons learned
- Distracted....juggling multiple crises
- Safety fatigue, compassion fatigue from the pandemic
- Security fatigue?



Credit: Tom Gauld for the New York Times

Ideology: A Powerful Force

“They do not know it, but they are doing it.” Karl Marx

“Something absolutely vast and powerful...
beyond all perception and objective intelligibility”

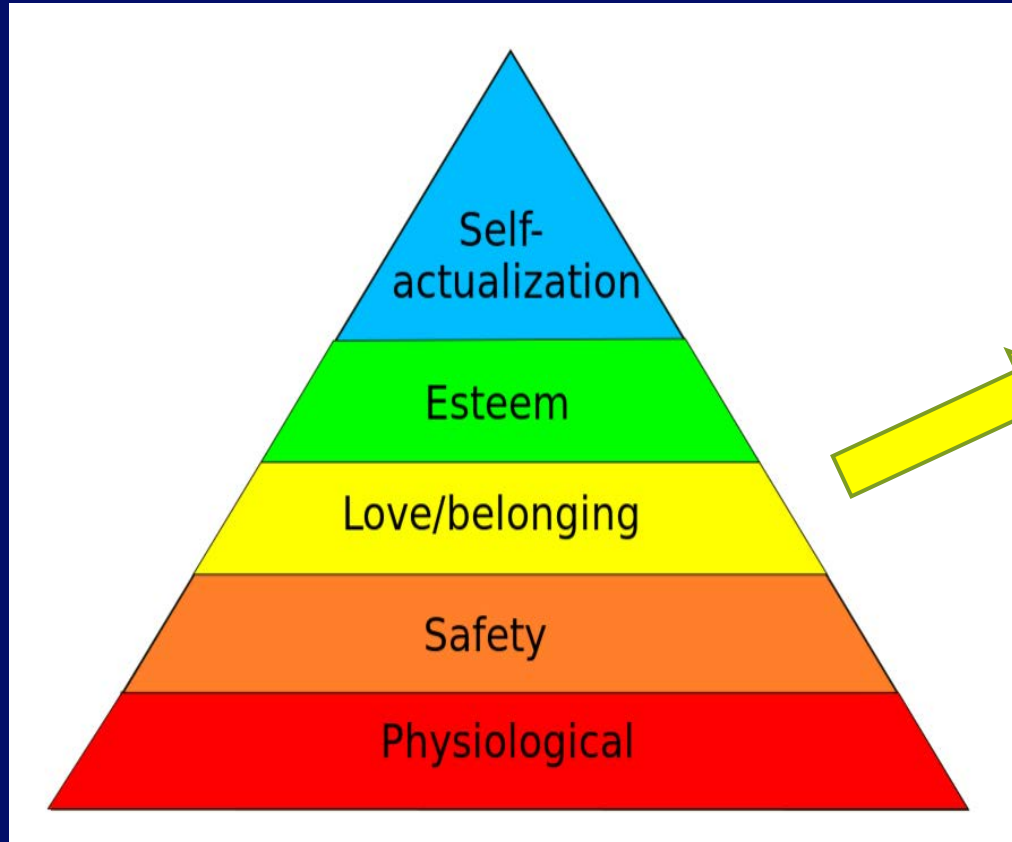
“In you more than yourself”

Read: Slavoj Žižek, The Sublime Object of Ideology (1989)



Credit: Rabea for alRiyadh.com, 2009

Need for Affiliation

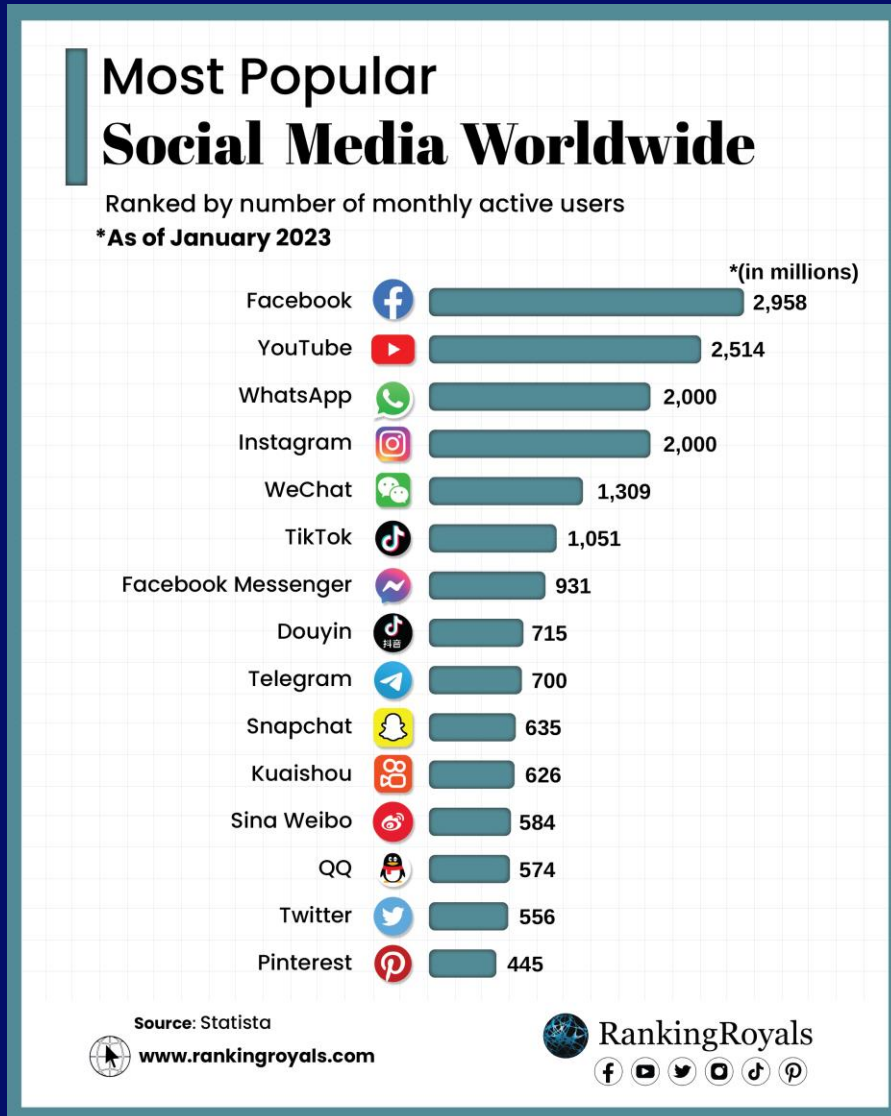


A person's need to feel a sense of involvement and "belonging" within a social group

Anxiety and stress feeds need for affiliation

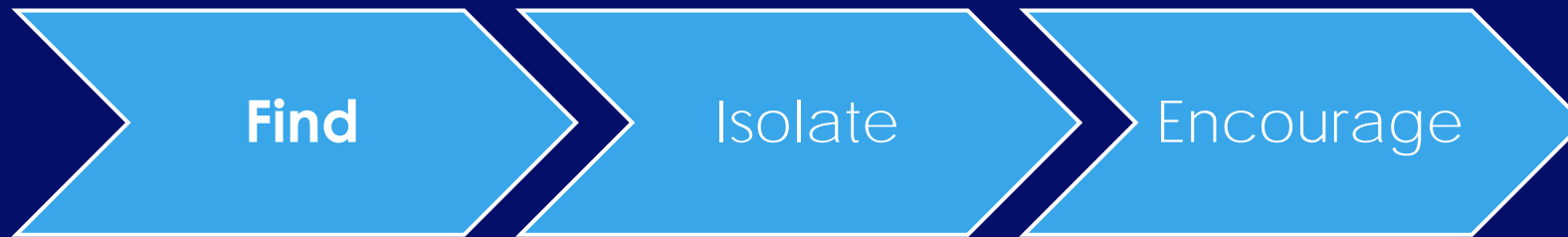
The pandemic "fed the beast"

How Do People Radicalize?



The Internet accelerates the speed of radicalization, provides instant interface between recruiters and recruits and 24/7 access to tactical information.

Online Recruitment Strategy




“Inspired Terror” at Ohio State in 2016
Abdul Razak Ali Artan



Mis- Dis- and Mal-information (MDM)

The United States remains in a heightened threat environment fueled by several factors, including an online environment filled with false or misleading narratives and conspiracy theories, and other forms of mis- dis- and mal-information (MDM) introduced and/or amplified by foreign and domestic threat actors."

<https://www.dhs.gov/ntas/advisory/national-terrorism-advisory-system-bulletin-february-07-2022>



National Terrorism Advisory System
Bulletin
DHS.gov/advisories

February 7, 2022 2:00 PM ET

*This Bulletin will expire on
June 7, 2022 at 2:00 PM ET*

****The NTAS Bulletin issued on November 10, 2021 and
set to expire on February 8, 2022 is hereby canceled.****

SUMMARY OF THE TERRORISM THREAT TO THE UNITED STATES

The United States remains in a heightened threat environment fueled by several factors, including an online environment filled with false or misleading narratives and conspiracy theories, and other forms of [mis-dis- and mal-information](#) (MDM) introduced and/or amplified by foreign and domestic threat actors. These threat actors seek to exacerbate societal friction to sow discord and undermine public trust in government institutions to encourage unrest, which could potentially inspire acts of violence. Mass casualty attacks and other acts of targeted violence conducted by lone offenders and small groups acting in furtherance of ideological beliefs and/or personal grievances pose an ongoing threat to the nation. While the conditions underlying the heightened threat landscape have not significantly changed over the last year, the convergence of the following factors has increased the volatility, unpredictability, and complexity of the threat environment: **(1)** the proliferation of false or misleading narratives, which sow discord or undermine public trust in U.S. government institutions; **(2)** continued calls for violence directed at U.S. critical infrastructure; soft targets and mass gatherings; faith-based institutions, such as churches, synagogues, and mosques; institutions of higher education; racial and religious minorities; government facilities and personnel, including law enforcement and the military; the media; and perceived ideological opponents; and **(3)** calls by foreign terrorist organizations for attacks on the United States based on recent events.

ADDITIONAL INFORMATION

The primary terrorism-related threat to the United States continues to stem from lone offenders or small cells of individuals who are motivated by a range of foreign and/or domestic grievances often cultivated through the consumption of certain online content. The convergence of violent extremist ideologies, false or misleading narratives, and conspiracy theories have and will continue to contribute to a heightened threat of violence in the United States.

RESOURCES TO STAY SAFE

Stay Informed and Prepared

- [Be prepared](#) for emergency situations and remain aware of circumstances that may place you at risk. Make note of your

Humans and Security



Humans: force multiplier or weakest link?

- The human element is the most difficult to address in the security realm - yet can make or break our efforts
- Cauldron of emotions and behaviors are extremely detrimental to security efforts – and also a dangerous and exploitable phenomena

Terrorism

The battlefield isn't a place, it's in the mind.

Ideology is the "glue."

The Internet is the vehicle.



What is Terrorism?

Terror: From the Latin word *terrorem*, “great fear”

A *terrorist* uses violence (or the threat of violence) to kill, cause fear,
intimidate, coerce

A *terrorist act* translates intentions to action

Challenge: Definition of a *terrorist* and a *terrorist act* still in debate in the U.S.

FTOs of Greatest Threat

Corporate structure, vast resources, adaptable, impermeable, persistent ideology, staying power. Undefeatable.

- ISIS/splinters: Regrouping, more sophisticated
- al Qaeda/splinters: 27-year war
- Hezbollah and HAMAS: 30+ years and going strong
- Religious ideology is the most dangerous = apocalyptic
- Military tactic of decimation not effective

Escalation in U.S. Plots and Attacks

During the pandemic...

- Ft Myers, FL. Alison Marie Sheppard, material support to ISIS
- Tampa, FL. Muhammed Momtaz Al-Azhari, ISIS inspired; Clearwater Beach, Honeymoon Island, Lafayette College
- Naval Air Station Corpus Christi, TX. Radam Salim Alsahli, AQ inspired; one injured, attacker killed
- Dr. Muhammad Masood, Mayo Clinic, ISIS, lone actor attacks
- Searching for Libyan Haji Mohamed, Alexandria, VA, al Shabaab
- Plot to blow up White House and Trump Tower, ISIS inspired
- Seattle man tried to join ISIS, planned attack on Seattle Pride parade

The FBI has 2,000 active cases tied to FTOs; 50% increase!

Case Study: Colleyville Synagogue Standoff

- January 15, 2022 - British citizen Malik Faisal Akram took four people, including a rabbi, hostage at a synagogue in the small town of Colleyville, TX
- On the MI5 watchlist as a "subject of interest" in 2020, investigated and moved to the "former subject of interest" list, no longer considered a threat
- Gained access to the synagogue during the service by claiming to be homeless
- Demanded the release of Aafia Siddiqui, a Pakistani, US-educated neuroscientist radicalized by AQ, serving an 86-year prison sentence in Fort Worth
- Rabbi fought back and hostages escaped; Akram was killed after a 10-hour siege
- During the standoff, ISIS, AQ and White Supremacist group thought leaders were chatting live about the situation
- Wake-up call about the ongoing threat of foreign terror + he was a "traveler"
- Attacker had a confluence of issues and ideology – mental health issues, radicalized, personal grievances (anti-vax, anti-government)

AQ and ISIS: Similar Strategies

- Soft targets primary choice
- Actively recruiting Americans
- Using the Internet to recruit, inspire, plan, direct, fundraise, boost morale, communicate, share and perfect tactics
- Focused on overwhelming, exhausting us
- Infiltrating economy, seeking to influence political process
- Leverage the pandemic, Ukraine, etc. - pile misery on misery
- Infiltrating/destabilizing/exploiting failed states
- Using drones, much chatter about WMD

New Tactics Quickly Spread: Prepare!

Evolution of the truck-into-crowd attack:

- AQ and ISIS propaganda online (late 2015)
- Bastille Day Parade (July 14, 2016)
- German Christmas Market (December 19, 2016)
- London bridges (March 22, 2017 & June 3, 2017)
- Barcelona Square (August 17, 2017)
- NYC truck onto the bike path (October 31, 2017)



Attack Plot Trends



- Asymmetric, creative (2018 Cleveland 4th of July plot)
- Preoperational surveillance
- Multiple attacks - but not simultaneous; spread across city, sequential to cause chaos, delay response, cause panic
- Targeting people fleeing from exits
- Attacking at the end of the event
- Targeting first responders

Domestic Terror in the U.S.

- Right Wing: neo-Nazism, neo-fascism, white nationalism, religious nationalism, anti-government patriots, militias, sovereign citizens
- Left Wing: Revolutionary socialism, antifascism, anarchism
- Religious: Most dangerous, apocalyptic, martyr
- Single Interest: Animals, environment, climate
- Wildcards: Male supremacism (Incel), Boogaloo Bois, Proud Boys

Challenge: No U.S. domestic terror list



DOMESTIC EXTREMIST ATTACK AND PLOT TRENDS 2021-2022



This assessment identifies trends and patterns of 13 domestic extremist attacks and plots by 15 individuals, associated with racially motivated and anti-government extremist ideologies from January 1, 2021, to August 31, 2022. Incidents were collected, reviewed, and analyzed from publicly available sources to create a comparable data set. Chosen parameters included whether a subject had an identifiable extremist ideology, conducted an attack or plot in furtherance of their ideology, and acquired materials, firearms, or improvised explosive devices with the intent to cause harm. Domestic extremists who did not meet these criteria for the allotted time frame were excluded from this assessment.

THREAT SUMMARY

An NJOHSP review of the data set revealed notable statistics and trends among domestic extremists, including arrests and fatalities, methodology, social media engagement, and group affiliation. The largest percentage of perpetrators identified with either white racially motivated or anti-government extremist ideology. They would rarely write manifestos or equip themselves with body armor or improvised explosive devices. Perpetrators were more likely to be arrested after an attack than killed during one. Most perpetrators used various social media platforms to discuss their ideology and plan attacks. Smaller percentages utilized these applications to either consume propaganda or procure weapons or other attack materials.

KEY FINDINGS (13 INCIDENTS INVOLVING 15 PERPETRATORS)



*Chart depicts number of victims in attacks. 10 of the 13 killed were from one attack.

WROTE MANIFESTOS



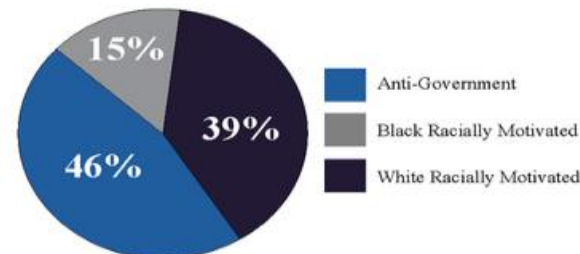
USE OF BODY ARMOR



UTILIZED IMPROVISED EXPLOSIVE DEVICES



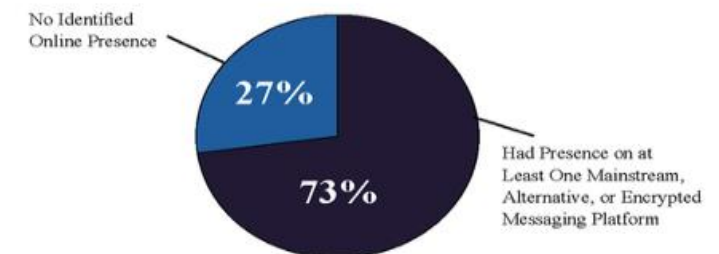
IDEOLOGICAL AFFILIATION



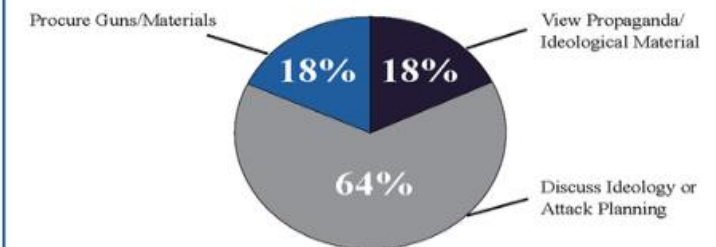
NEW JERSEY CASE STUDY

In April 2022, a lone offender conducted several violent attacks on members of the Orthodox Jewish community in and around Lakewood (Ocean County). Authorities charged the perpetrator with willfully causing bodily injury to four victims and of those, attempting to kill and cause injuries with dangerous weapons to three. While the incident in Lakewood is still an ongoing investigation, the attacker allegedly targeted these individuals solely on the basis of their culture and religion.

SOCIAL MEDIA PRESENCE



USE OF SOCIAL MEDIA



Boogaloo Bois: From Meme to Movement to Murder



UK bans fifth neo-Nazi group under terror laws

By Daniel De Simone
BBC News

12 July 2021



Members of "The Base" tried to groom teenagers in the UK and elsewhere as recruits

News | The Far Right

Canada declares far-right Proud Boys a 'terrorist' organisation

Canada lists 13 groups as 'terrorist entities', saying ideological extremism poses 'most significant' security threat.



New Zealand designates Proud Boys, The Base as 'terrorist' groups

Two US far-right groups join 18 other organisations that have been given an official 'terrorist' designation by New Zealand.



NEWS

Australia Adds U.S.-Based Neo-Nazi Group to List of Banned Terrorist Organizations

BY KATIE WERMUS ON 11/24/21 AT 6:10 PM EST

Domestic Violent Extremism (DVE)

Domestic violent extremists are US-based actors who conduct or threaten activities that are dangerous to human life in violation of the criminal laws of the United States or any state; appearing to be intended to intimidate or coerce a civilian population; and influence the policy of a government by intimidation or coercion, affect the conduct of a government by mass destruction, assassination, or kidnapping, as per the definition of domestic terrorism in 18 U.S. Code 2331 (5).

Mere advocacy of political or social positions, political activism, use of strong rhetoric, or generalized philosophic embrace of violent tactics may not constitute violent extremism and may be constitutionally protected.

Source: FBI

Leader Insights

John Cohen, Coordinator for Counterterrorism and Assistant Secretary for Counterterrorism and Threat Prevention, DHS says the FBI has 2,500 open domestic terrorism cases.

“Most significant terrorist threat to the US are lone actors or small groups based on an ideological group they connect with online – combination of beliefs and personal grievances” and “Threat comes from people who have a superficial understanding of the ideology. They’re angry, disconnected, treated unfairly, and participating in these groups provides a sense of self-worth.”

Christy Abizaid, NCTC director: *“My primary concern is the domestic extremist threat – racially and ethnically motivated – especially those with nexus to foreign groups.”*



National Terrorism Advisory System

Bulletin

DHS.gov/advisories

May 24, 2023, 2:00 PM ET

*This Bulletin will expire on
November 24, 2023 at 2:00 PM*

SUMMARY OF TERRORISM-RELATED THREAT TO THE UNITED STATES

The United States remains in a heightened threat environment. Lone offenders and small groups motivated by a range of ideological beliefs and personal grievances continue to pose a persistent and lethal threat to the Homeland. Both domestic violent extremists (DVEs) and those associated with foreign terrorist organizations continue to attempt to motivate supporters to conduct attacks in the Homeland, including through violent extremist messaging and online calls for violence. In the coming months, factors that could mobilize individuals to commit violence include their perceptions of the 2024 general election cycle and legislative or judicial decisions pertaining to sociopolitical issues. Likely targets of potential violence include US critical infrastructure, faith-based institutions, individuals or events associated with the LGBTQIA+ community, schools, racial and ethnic minorities, and government facilities and personnel, including law enforcement.

ADDITIONAL INFORMATION

- In May 2023, a now-deceased individual killed eight and injured seven others at an outlet mall in Allen, Texas. Law enforcement continues to investigate the motive behind the attack, but initial reporting suggests the attacker fixated on mass shootings and held views consistent with racially or ethnically motivated violent extremist (RMVE) and involuntary celibate violent extremist ideologies.
- In March 2023, a now-deceased individual shot and killed six people at a Christian elementary school in Nashville, Tennessee. Law enforcement continues to investigate the motive behind the attack and has indicated the individual studied other mass murderers.
- Also in March 2023, a RMVE driven by a belief in the superiority of the white race was arrested and charged with allegedly attempting to use an improvised incendiary device to burn down a church in Ohio that was planning to host a drag-themed event.
- In February 2023, two RMVEs driven by a belief in the superiority of the white race were arrested and are now awaiting trial for plotting an attack against

RESOURCES TO STAY SAFE

Stay Informed and Prepared

- [Be prepared](#) for emergency situations and remain aware of circumstances that may place you at risk. Make note of your surroundings and the nearest security personnel.
- Keep yourself [safe online](#) and maintain [digital and media literacy](#) to recognize and build resilience to false or misleading narratives.
- Review Department of Homeland Security (DHS) resources for how to better protect [businesses](#), [houses of worship](#), and [schools](#), and ensure the [safety of public gatherings](#).
- Prepare for potential [active shooter](#) incidents, [build counter-improvised explosive device capabilities](#), and [enhance awareness of terrorist threats, to include bomb threats](#).

NATIONAL STRATEGY FOR COUNTERING DOMESTIC TERRORISM

JUNE 2021

NATIONAL SECURITY COUNCIL



THIS IS A
PROJECT
THAT SHOULD
**UNITE ALL
AMERICANS**



TOGETHER
WE MUST
AFFIRM THAT
**DOMESTIC
TERRORISM
HAS NO
PLACE IN
OUR SOCIETY**

- DHS needs communities to engage – identify high risk individuals, off road and take care of them to reduce risk of violence
- DVE now a top priority - 7.5% of DHS funds; focus is on improving comm between agencies and helping communities with tools and programs

U.S. Crime is Escalating

- 2019: Worst year for school, church, retail, health care crime; 417 mass shootings; 31 mass killings; 3 majors (VA Beach, Walmart, Ned Peppers bar)
- 2020: 611 mass shootings (up 50%); 17 mass killings; 1 major (Molson Coors)
- 2021: 693 mass shootings, 28 mass killings, 5 majors (San Jose VTA, FEDEX Indianapolis, King Soopers in Boulder, Massage Parlors in Atlanta, iHop shooting spree, Evanston IL)
- 2022: 648 mass shootings, 39 mass killings, 11 majors (Chesapeake Walmart, Colorado Springs LGBTQ nightclub, Sacramento entertainment area, Indiana mall, Buffalo grocery store, Uvalde school, Tulsa medical center, Highland Park 4th parade)
- 2023: 498 mass shootings, 30 mass killings, 8 majors (Star Ballroom, Tennessee school, mushroom farm, Alabama birthday party, Texas Outlet Mall, Philly, domestics)

Mass shooting: 4 or more shot in one incident, excluding shooter

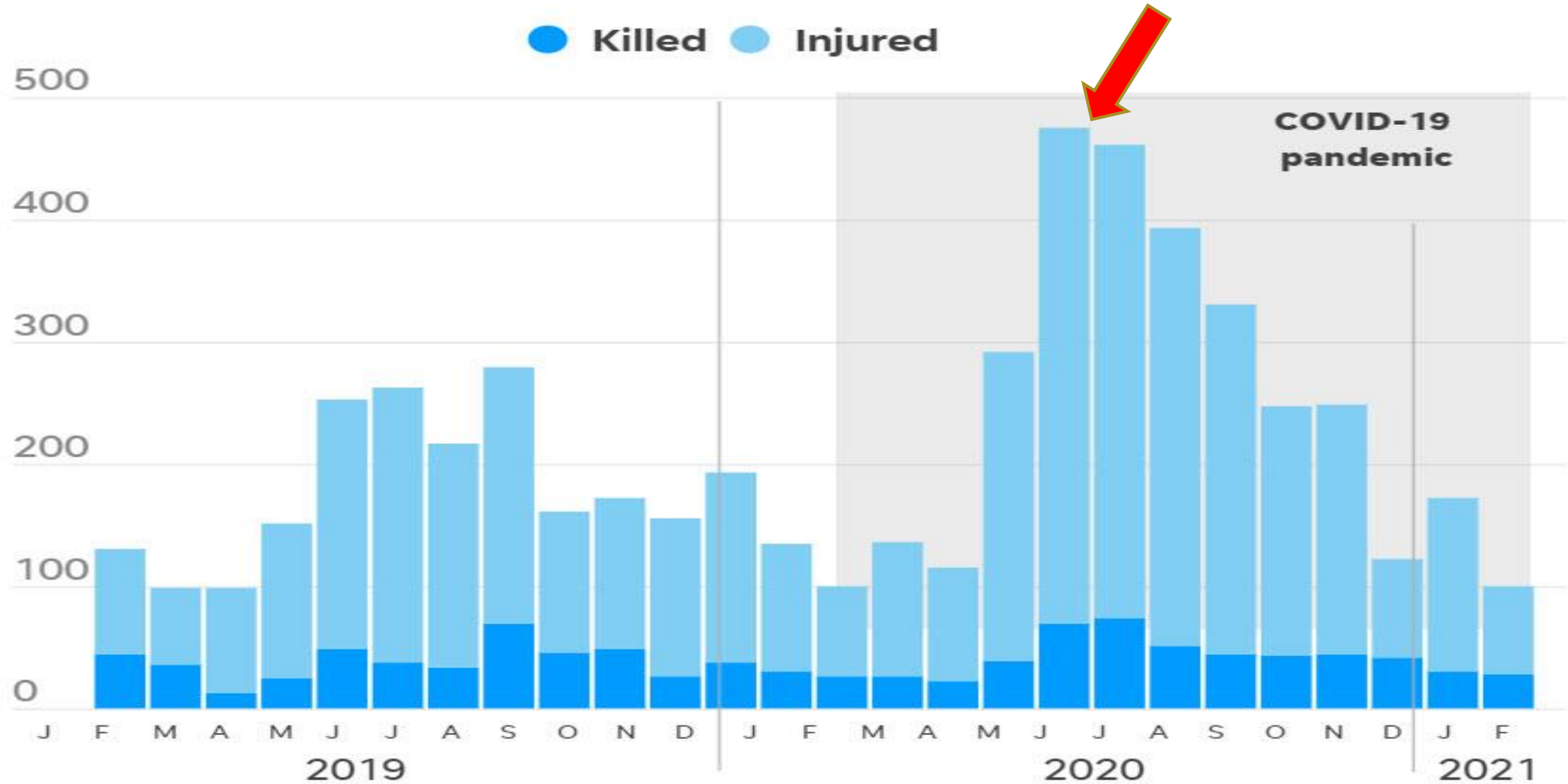
Mass killing: 4 or more killed in one event

Major mass shooting: 6 or more killed in one event

<https://www.gunviolencearchive.org/>

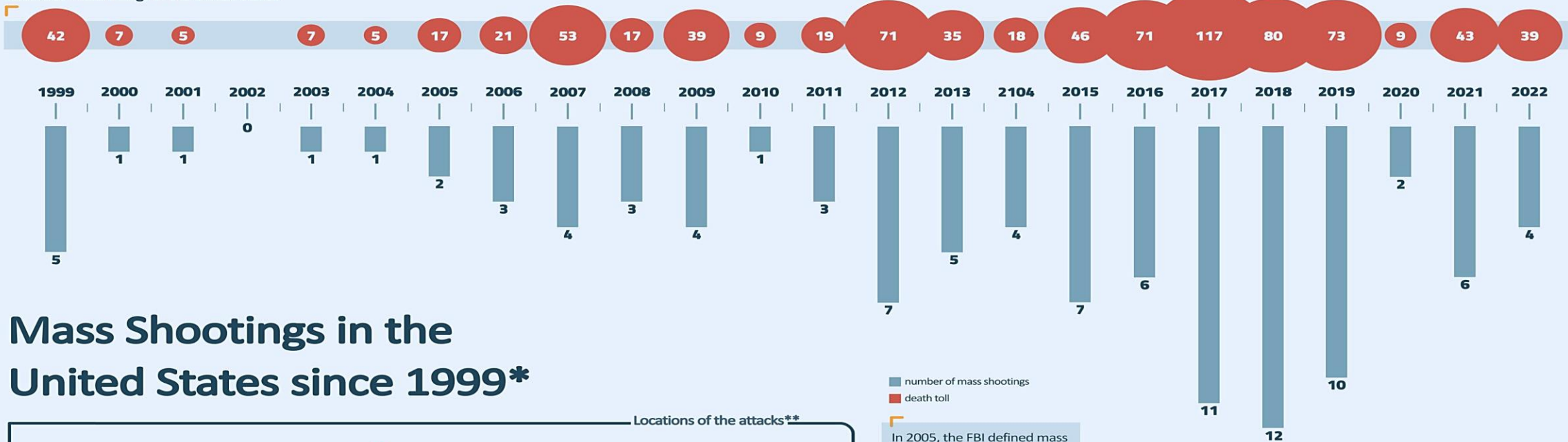
Mass shooting victims

Events that injure or kill four or more people excluding the perpetrator.

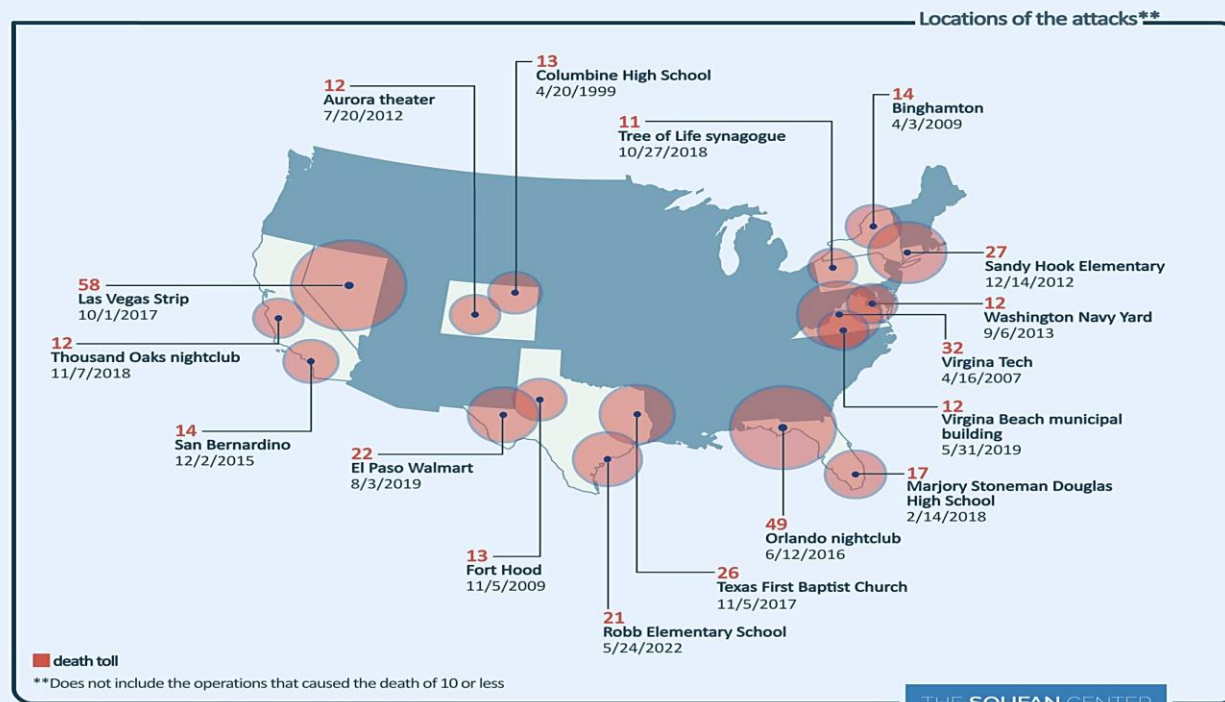


SOURCE: Gun Violence Archive

Recorded mass killings in the United States

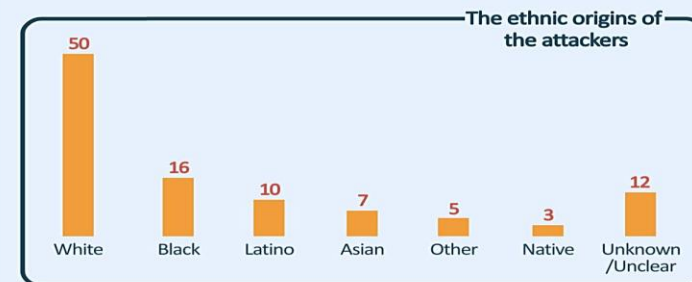


Mass Shootings in the United States since 1999*



■ number of mass shootings
■ death toll

In 2005, the FBI defined mass murders as those carried out in a public place with a single attack, killing at least 4 victims. In January 2013, President Barack Obama authorized reducing the number to three fatalities. We have chosen *Mother Jones* database, as it strictly abides by this definition. Some other sources have less restrictive definitions, and numbers could go higher.

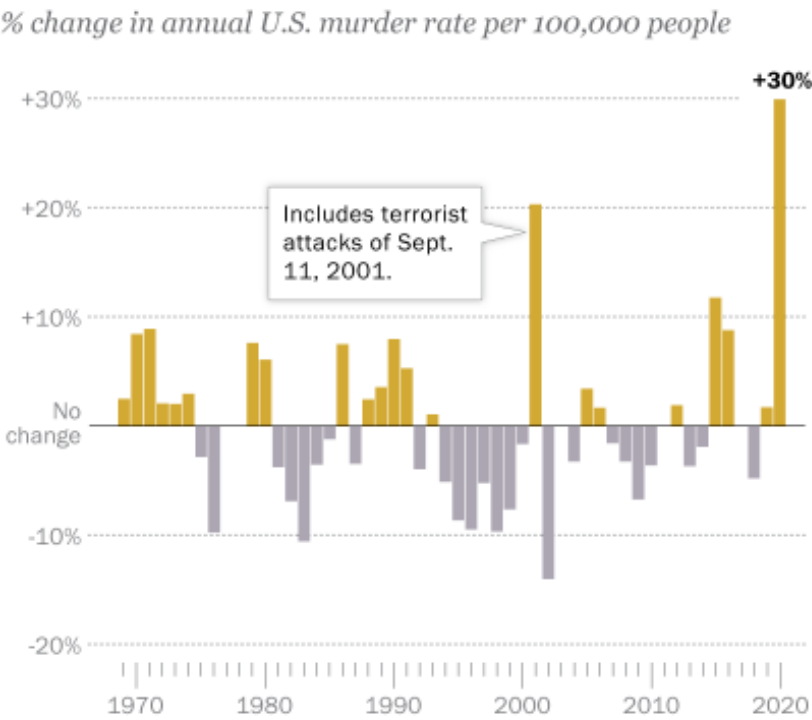


Distribution by sex of perpetrators of attacks



Homicide Trends

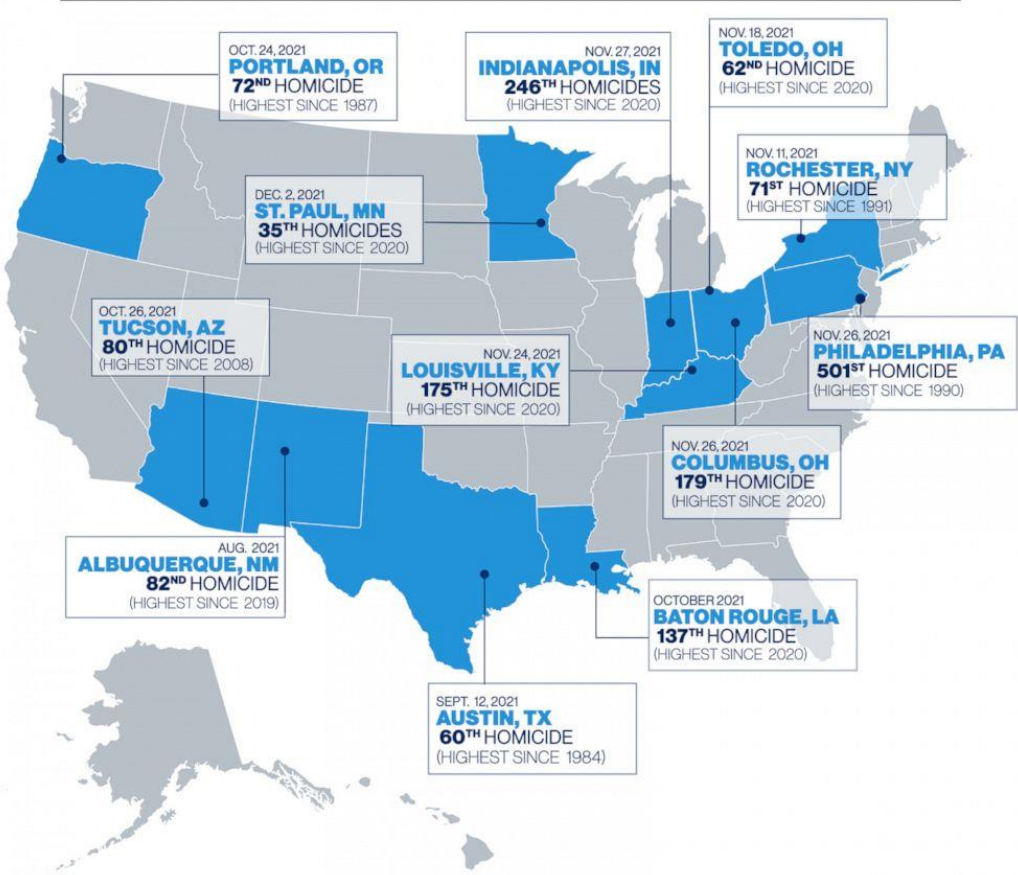
U.S. murder rate rose by nearly a third in 2020, marking one of the biggest annual increases on record



Note: 2020 data is provisional. While the U.S. murder rate rose 30% in 2020, it remained below the levels of earlier decades.
Source: Centers for Disease Control and Prevention.

PEW RESEARCH CENTER

12 U.S. Cities That Have Broken Annual Homicide Records



SOURCE: ACCORDING TO EACH STATE'S POLICE DEPARTMENT

abc NEWS

Active Shooter Trends

An active shooter is "an individual actively engaged in killing or attempting to kill people in a confined and populated area; in most cases, there is no pattern or method to their selection of victims."

DHS - Mass shooting events average 580 seconds in length

Active shooter incidents increased more than 50 percent last year, FBI data shows

103 people were killed and 140 were wounded in 61 active shooter incidents across 30 states last year, the FBI reported.

Incident Statistics

Active Shooter Incidents 2017–2021

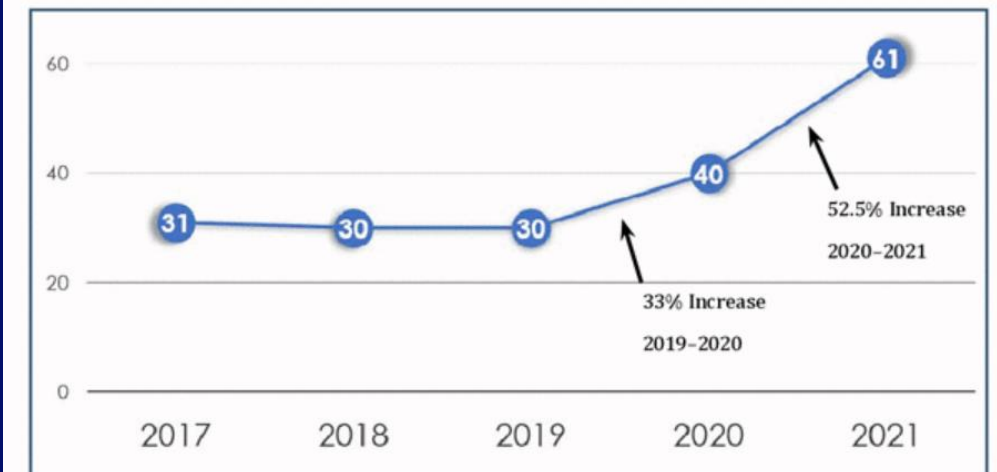
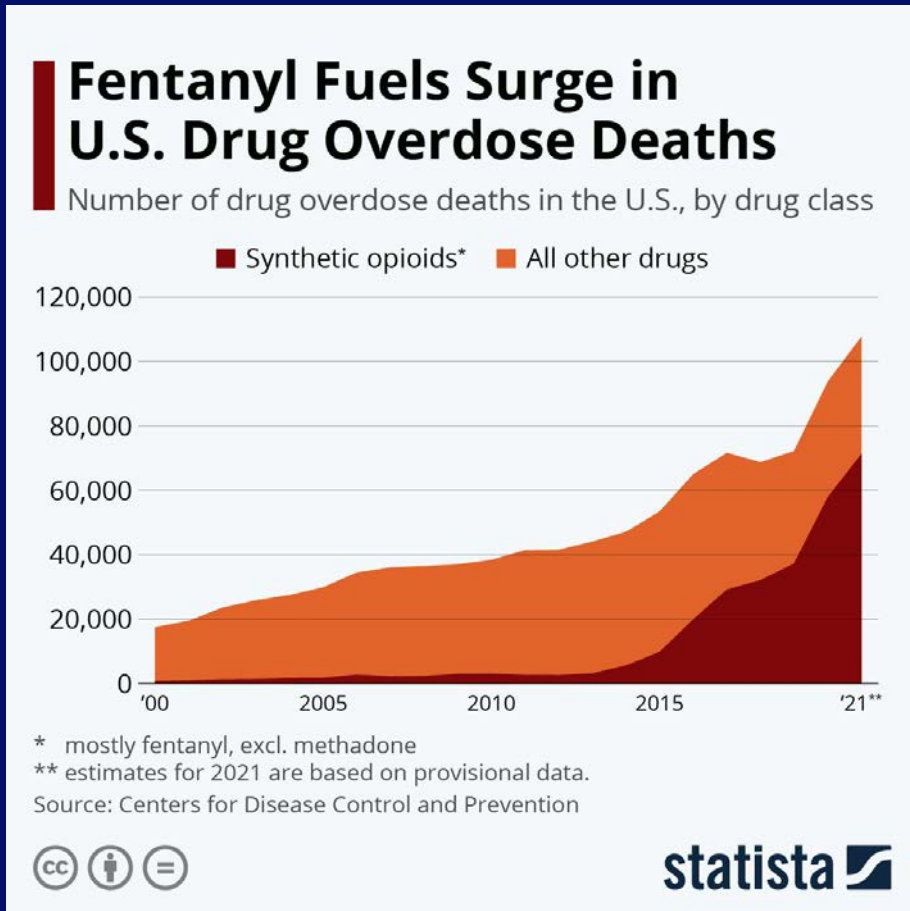


Figure 1

Don't Forget Stabbings!

- Knife attacks are on the rise in schools, malls, hospitals, et al crowded spaces
- Gun attacks more feared, but knife attacks are also silent, fast, unexpected and cause devastating injuries
- Knives are easier to obtain and conceal
- Few pain sensors inside the body; a large blade penetrating a critical organ results in death so quickly that most people pass out and die without pain
- People are more willing to engage and try to subdue an attacker with a knife, while choosing to run or hide from a shooter
- Physically confronting an enraged assailant wielding a knife is difficult

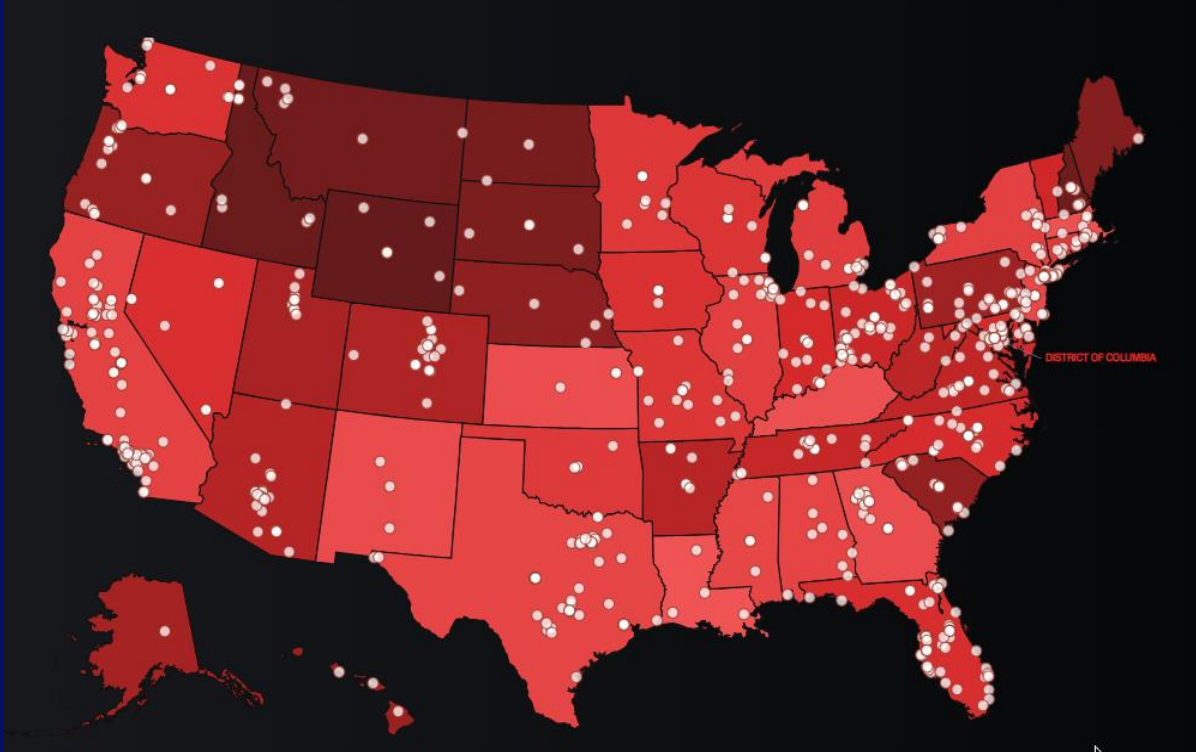
Drugs, Gangs, Transnational Crime



Gang violence accounts for 48% of all violent crime in America.
An estimated 1.4 million people make up over 33,000 gangs across the US (FBI)

Hate Groups

IN 2022, WE TRACKED 1,225 HATE AND ANTIGOVERNMENT GROUPS ACROSS THE U.S.



A hate group is an organization or collection of individuals that – based on its official statements or principles, the statements of its leaders, or its activities – has beliefs or practices that attack or malign an entire class of people, typically for their immutable characteristics.

A hate crime is a “criminal offense against a person or property motivated in whole or in part by an offender’s bias against a race, religion, disability, sexual orientation, ethnicity, gender, or gender identity.” (FBI)

Lone Actor Terror (LAT)

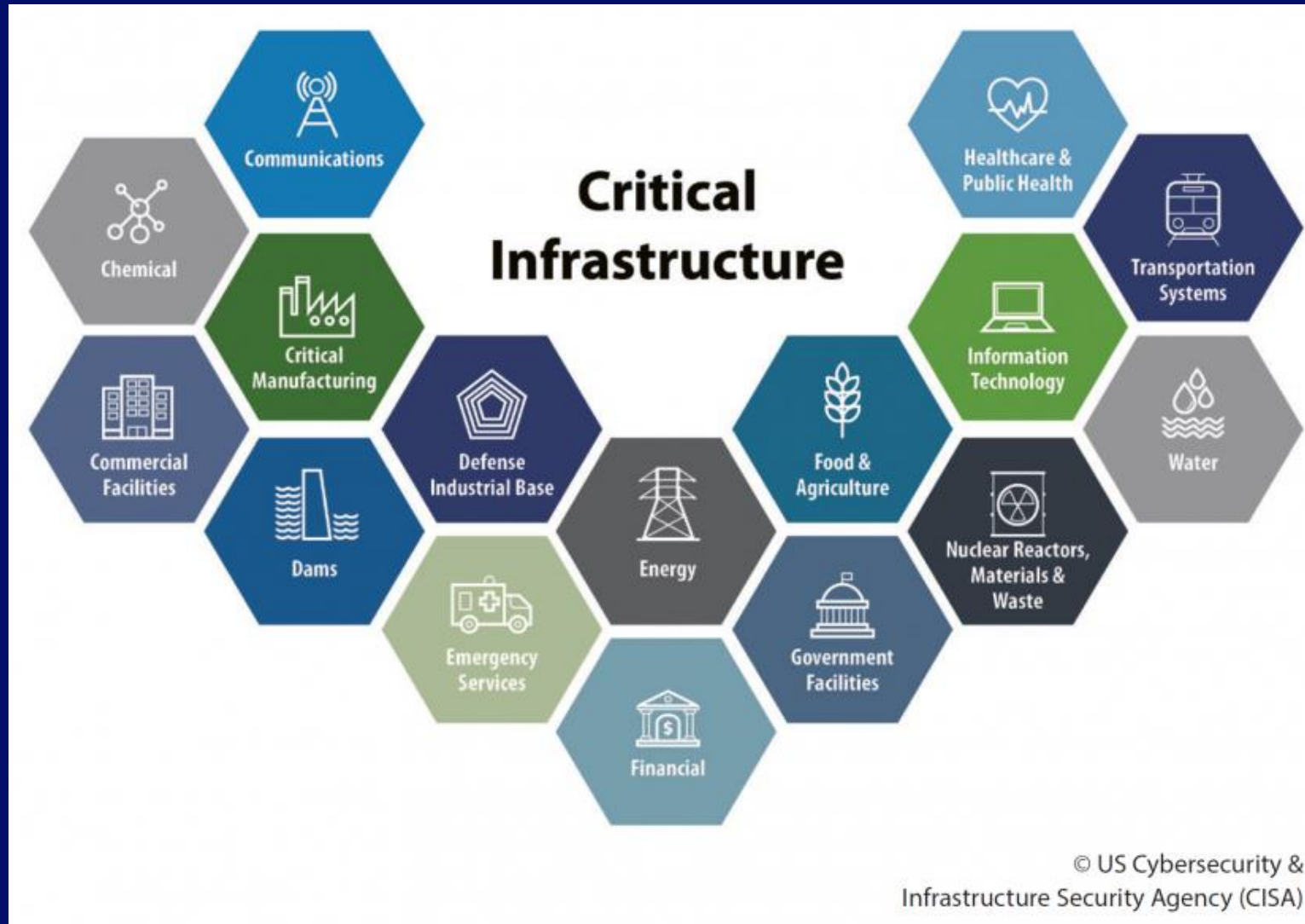


Nashville Bombing
Christmas Morning, 2020

- Lone ~~Wolf~~ Actor Terror: “Terror undertaken by individuals who prepare for and execute violence without external assistance” FBI
- Two types of Lone Actors:
 - Well adapted to society, mentally fit; makes a tactical choice to engage in lone actor ops; leaves society
 - Not well adapted, suffering mental health issues or in psychological distress; society leaves them
- LAT doubled in last decade

Visit: ICCT project: Countering Lone Actor Terrorism
<https://icct.nl/topic/countering-violent-extremism/>

Target List = Everything



FOR IMMEDIATE RELEASE

Wednesday, February 23, 2022

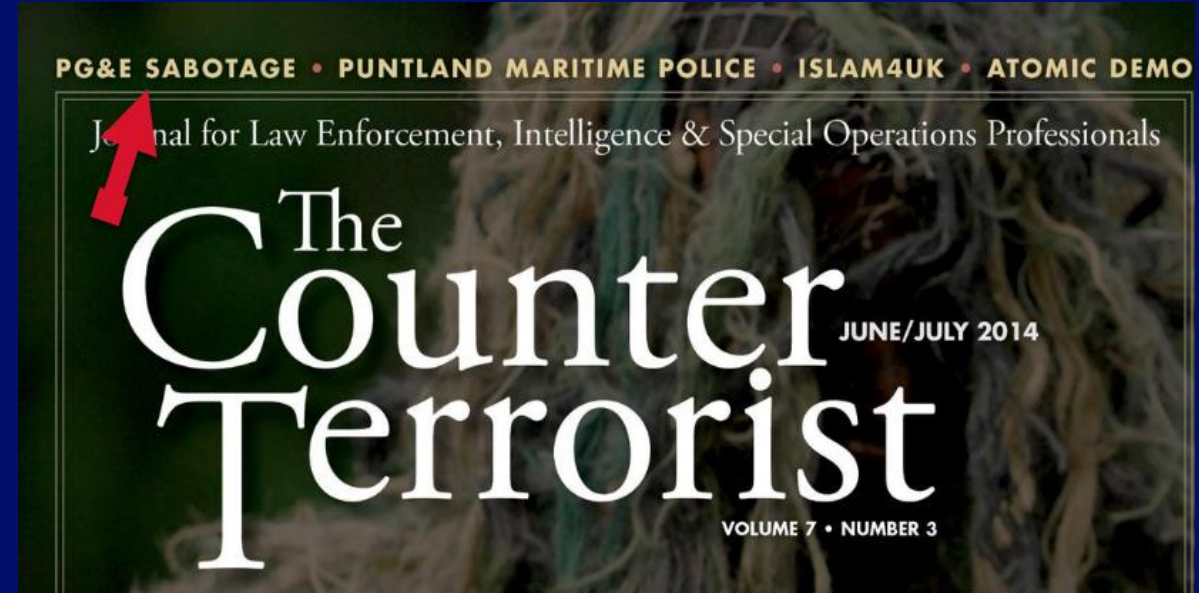
Three Men Plead Guilty to Conspiring to Provide Material Support to a Plot to Attack Power Grids in the United States

Domestic Terrorism Plot was in Furtherance of White Supremacist Ideology

Three men pleaded guilty today to crimes related to a scheme to attack power grids in the United States in furtherance of white supremacist ideology.

According to court documents, Christopher Brenner Cook, 20, of Columbus, Ohio; Jonathan Allen Frost, 24, of West Lafayette, Indiana, and of Katy, Texas; and Jackson Matthew Sawall, 22, of Oshkosh, Wisconsin, each pleaded guilty to one count of conspiring to provide material support to terrorists. The charge and plea agreements indicate that the defendants knew and intended that the material support they conspired to provide would be used to prepare for and carry out the federal offense of destroying energy facilities.

“These three defendants admitted to engaging in a disturbing plot, in furtherance of white supremacist ideology, to attack energy facilities in order to damage the economy and stoke division in our country,” said Assistant Attorney General for National Security Matthew G. Olsen. “The Justice Department is committed to investigating and disrupting such terrorist plots and holding perpetrators accountable for their crimes.”

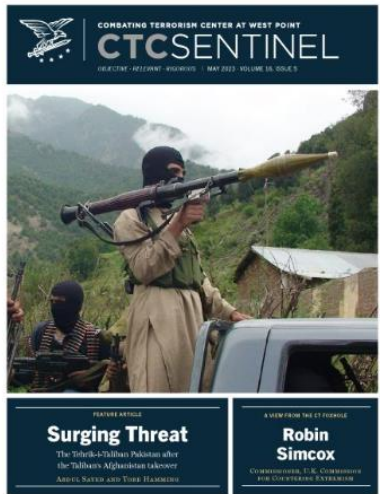


CRIME >

2 suspects arrested for conspiring to attack Baltimore power grid, officials say

BY EMILY MAE CZACHOR, NICOLE SGANGA

UPDATED ON: FEBRUARY 6, 2023 / 7:06 PM / CBS NEWS



The Targeting of Infrastructure by America's Violent Far-Right

MAY 2023, VOLUME 16, ISSUE 5

Authors:

COLIN CLARKE, MOLLIE SALTSKOG, MICHAELA MILLENDER, NAUREEN C. FINK

<https://ctc.westpoint.edu/the-targeting-of-infrastructure-by-americas-violent-far-right/>



Mayhem, Murder, and Misdirection: Violent Extremist Attack Plots Against Critical Infrastructure in the United States, 2016-2022

Ilana Krill & Bennett Clifford
September 2022

Program on Extremism
THE GEORGE WASHINGTON UNIVERSITY

 **NCITE** NATIONAL COUNTERTERRORISM,
INNOVATION, TECHNOLOGY,
AND EDUCATION CENTER
A U.S. DEPARTMENT OF HOMELAND SECURITY CENTER OF EXCELLENCE

What is a Soft Target?

A civilian-centric place

Crowded

Not typically “fortified”

Vulnerable, unprotected, undefended

Security not a primary mission

Privately owned

Possibly resource constrained

Soft Target Psychology

- 90% of casualties in conflicts now civilians
- We protect these targets, don't purposely strike them
- Bound by international law, Geneva Conventions, religious doctrine or rules of engagement in a coalition battle
- Threat met with disbelief, but we must ask:

What do we most fear?

How should we respond?



Soft Target Security Truths

- ✓ Actions generate results.
- ✓ Inaction is a choice, and also generates results.
- ✓ “Not seen” does not mean “not there.”
- ✓ The “fog of war” means we don’t know everything about the threat, there are inescapable unknowables.
- ✓ Security actions no longer canned, must be tailored.
- ✓ Security plans must be fluid; constantly assess/adjust based on changes in the environment.
- ✓ Copycat attacks **will** happen.
- ✓ Goal of hardening: remove the enemy from the fight before it starts.

Soft Targeting Motivations

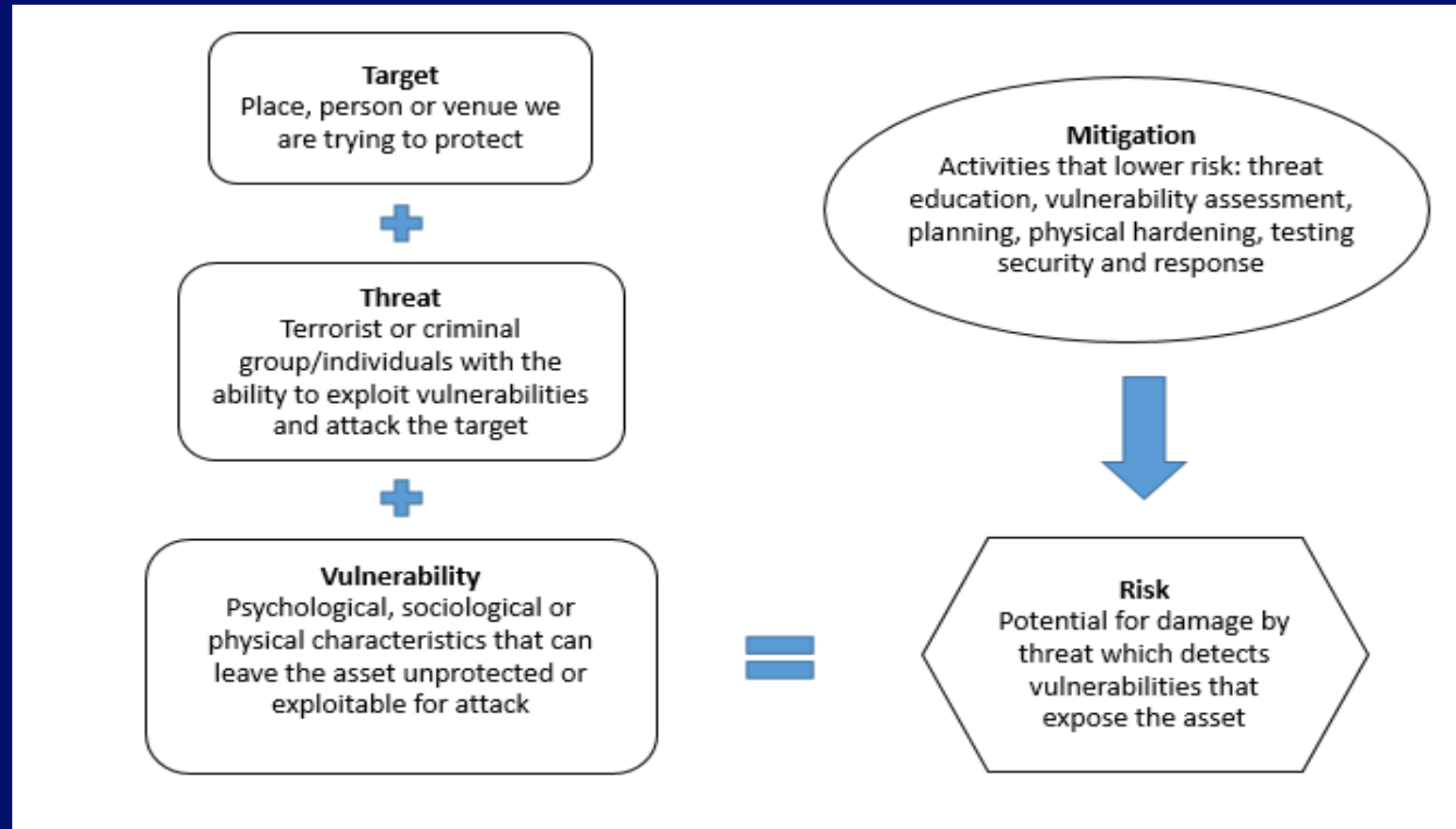
- ✓ Target rich environment
- ✓ Easy, cheap, short planning cycle
- ✓ Increased likelihood of success
- ✓ Success = Credibility
- ✓ Recruiting value
- ✓ Proof of viability, group's last gasp
- ✓ Test a new strategy, tactic, weapon
- ✓ Quickly damage a market
- ✓ Plant seeds of fear
- ✓ Delegitimize a government – can't protect its people
- ✓ Get the government to the negotiation table
- ✓ Cause political instability during an election
- ✓ Attain global media coverage

What Are We Doing Wrong?



1. No Methodology

- ✓ Identify the target(s)
- ✓ Understand the threat
- ✓ Assess vulnerabilities
- ✓ Calculate risk
- ✓ Harden/mitigate using an informed planning process





Most organizations accomplish a risk assessment

Some accomplish a vulnerability assessment

Few do a threat assessment – but this is where they need to start!

Threat Analysis

- ✓ Answer why you might be targeted and who are the actors?
- ✓ Identify and assess the capabilities of these actors
- ✓ Identify threat tactics, and methodologies through case studies plus data from law enforcement and intelligence agencies – most is open source!
- ✓ This informs your vulnerability and risk assessments, also security planning and budgeting efforts

Understand Vulnerability

Definition: Psychological, sociological, or physical characteristics that can leave the asset unprotected, or exploitable for attack.

Identify “how” and “where” the bad actor might strike for maximum effect.

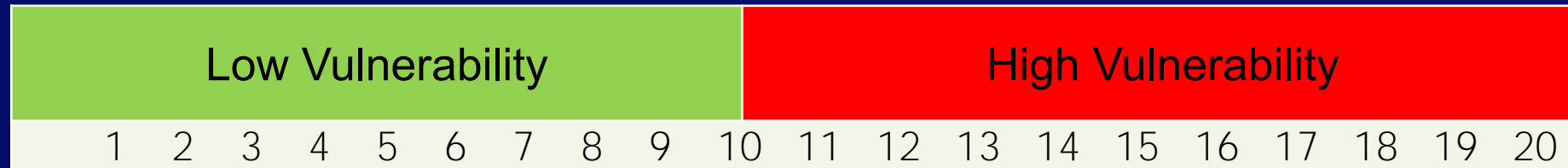
Identify Your Achilles Heel.

The Ability To Deter Attack Is Amplified By Understanding Vulnerability!

Target Analysis and Vulnerabilities

	Criticality	Accessibility	Recuperability	Vulnerability	Effect	Recognizability
Value	C	A	R	V	E	R
5	Loss would be mission stopper	Easily accessible. No effective security	Extremely difficult to replace. Long down time	A dedicated adversary has the capability and expertise to attack	Very high sociological, economical, political impact; considerable loss of lives and/or injured	Easily recognized by all with no confusion
4	Loss would reduce mission performance considerably	Accessible	Difficult to replace with long down time	A dedicated adversary most likely has the capability and expertise to attack	High impact; some loss of lives or injuries	Easily recognized by most
3	Loss would reduce mission performance	Somewhat accessible	Can be replaced in a relatively short time	A dedicated adversary may have the capability and expertise to attack	Moderate impact; some adverse impact on persons	Recognized with some training
2	Loss may reduce mission performance	Difficult to gain access	Easily replaced in a short time	A dedicated adversary most likely does not have the capability and expertise to attack	Little impact; no adverse impact on persons	Hard to recognize. Confusion probable
1	Loss would not affect mission performance	Very difficult to gain access	Immediate replacement. Spare parts are readily available or asset redundancy	A dedicated adversary does not have the capability and expertise to attack	No unfavorable impact	Extremely difficult to recognize without assistance

Vulnerability Assessment



7. Security Environments and Overall Vulnerability to an Attack

Does your organization have effective internal security procedures?

What is the law enforcement presence in your area?

What is the hardness, level of blast protection, etc. of your facilities?

How accessible (security presence, access control, id badges, metal detection buffer zones, fences, etc.) is your facility?

Are your assets and/or its potential recognized as a symbol?

What level of public access is necessary for you to function?

Can you control high-speed vehicle approaches to your facility?

Source: FBI (now my) Terrorism Vulnerability Self-Assessment Checklist

Calculate Risk and Impact

		Consequences				
		Insignificant (1) No injuries / minimal financial loss	Minor (2) First aid treatment / medium financial loss	Moderate (3) Medical treatment / high financial loss	Major (4) Hospitable / large financial loss	Catastrophic (5) Death / massive financial loss
Likelihood	Almost Certain (5) Often occurs / once a week	Moderate (5)	High (10)	High (15)	Catastrophic (20)	Catastrophic (25)
	Likely (4) Could easily happen / once a month	Moderate (4)	Moderate (8)	High (12)	Catastrophic (16)	Catastrophic (20)
	Possible (3) Could happen or known it to happen / once a year	Low (3)	Moderate (6)	Moderate (9)	High (12)	High (15)
	Unlikely (2) Hasn't happened yet but could / once every 10 years	Low (2)	Moderate (4)	Moderate (6)	Moderate (8)	High (10)
	Rare (1) Conceivable but only on extreme circumstances / once in 100 years	Low (1)	Low (2)	Low (3)	Moderate (4)	Moderate (5)

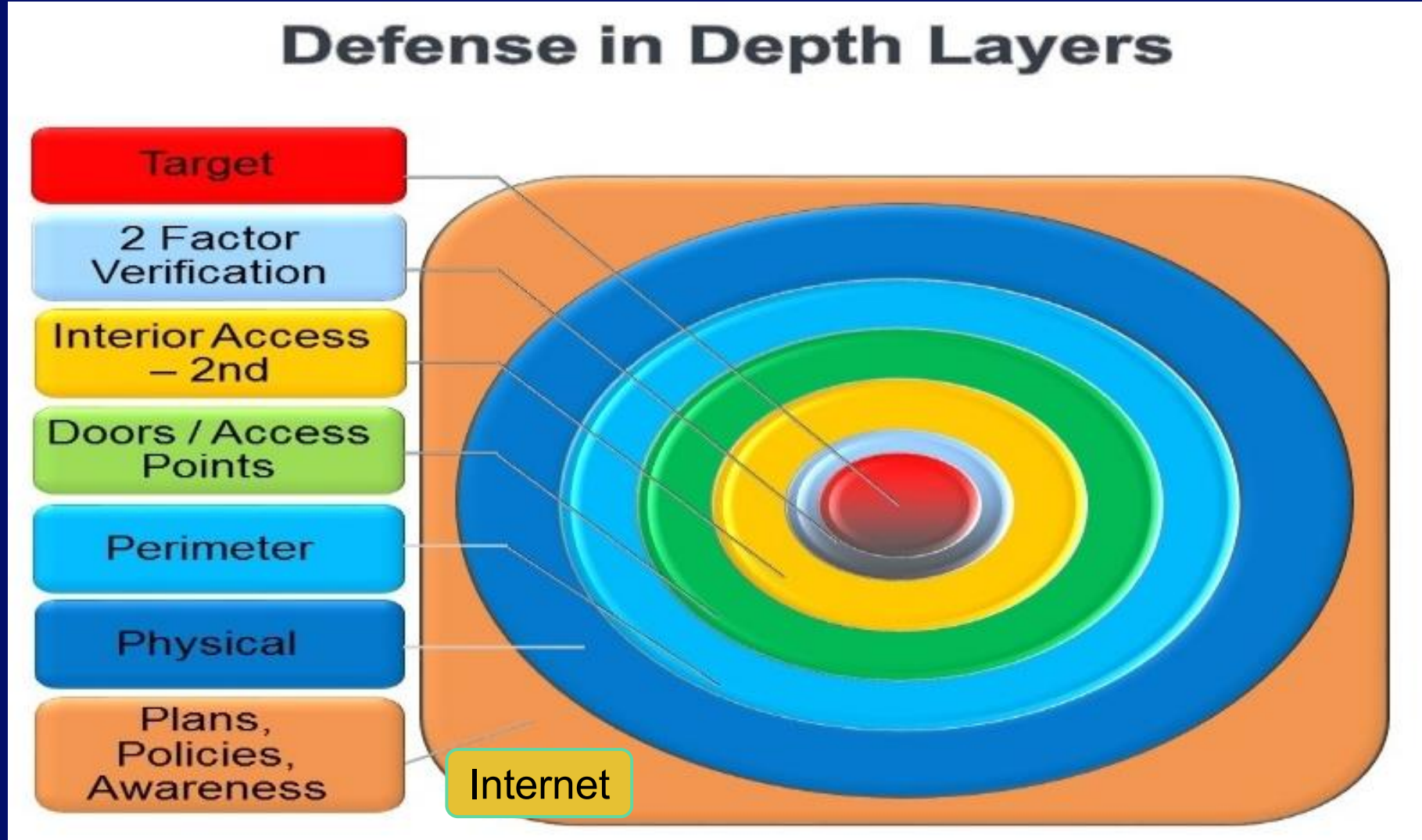
Risk Management Framework (RMF)

Targeted Mitigation

- Effects Based Hardening: System cross applied from the military model of Effects Based Operations
- Visualize violent scenarios unemotionally, through a data-driven lens
- Harmonize/synchronize/prioritize security activities

Prioritized Scenario	Desired Effect	Means	Capabilities and Cost	Implement/ Partially Implement/ Table
1. Highly visible location on busy highway draws opportunists	Lower "heat"	Remove external signage facing road	In house, volunteers, free	Implement
2. Too many people with keys to the main door	Restrict building access	Install electronic key lock on main door and obtain keying equipment and cards	Contracted; \$3,000	Partially implement; rekey current lock, reissue keys; budget electronic key system for summer 2015
3. Holding meetings after hours for outside groups, attendees wandering in building	Restrict access to the rest of the building	Install locking door between basement and upstairs offices	Contracted; \$1,500 with labor	Implement

2. Think Security Starts at the Front Door



3. Not “Baking” in Security



4. Think Security is Ugly



Vehicle-into-building trend



3 days ago
CBS 17
Car crashes into NC apartment building...



4 days ago
Fox News
huffing, crashed car into building ...



2 days ago
Colorado Springs Gazette
Car crashes into building in sout...



4 days ago
FOX8 WGHP
Car crashes into building in Greensboro ...



6 days ago
WHAM
crashing into building in Brighton ...



6 days ago
FOX8 WGHP
Asheboro Verizon store ...



5 days ago
Canarsie Courier
Kings Plaza - Car Rams Into Building...



5 days ago
PIX11
Car crashes into building in the Bronx ...



5 days ago
ABC7 Chicago
Car Into Building - ABC7 Chicago



5 days ago
ABC7 New York
Car Into Building - ABC7 New York



6 days ago
FOX8 WGHP
Asheboro Verizon store deemed...



4 days ago
FOX 5 Atlanta
SUV crashes into Atlanta apartment building



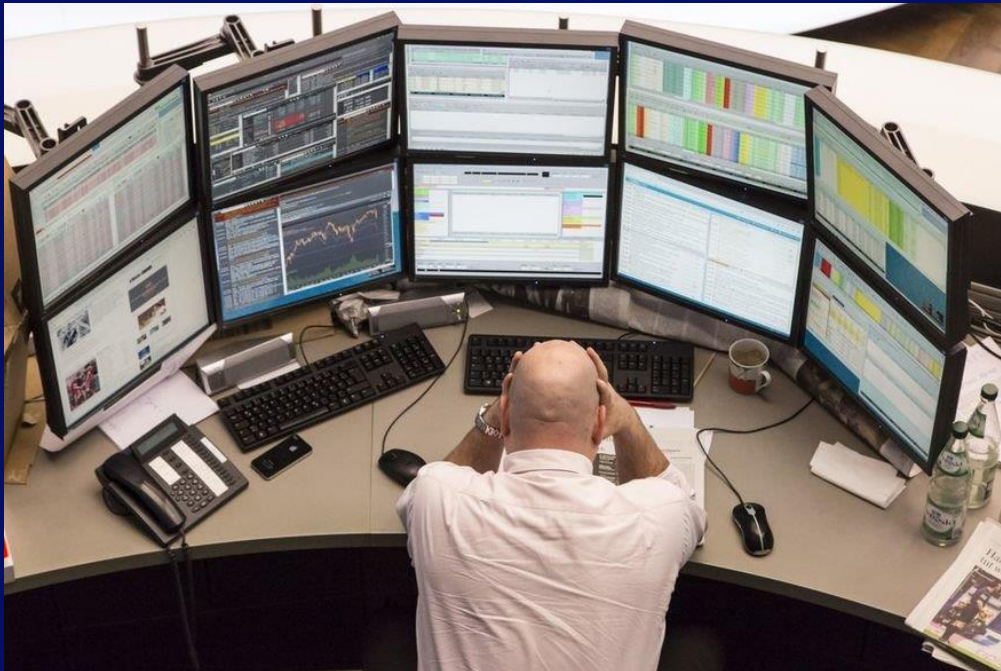
0:45 5 days ago
YouTube
Man hospitalized after crashing car ...

5. Expending Resources “Right of Bang”



Technology

Delicate balance:
The perils and promise of security technology



Security Robot Given The Gift Of Intelligence Chooses To Drown Itself



6. Not Using Informed Response

For example, Bomb Threats.

What we envision:



What we experience:



Bomb Threats

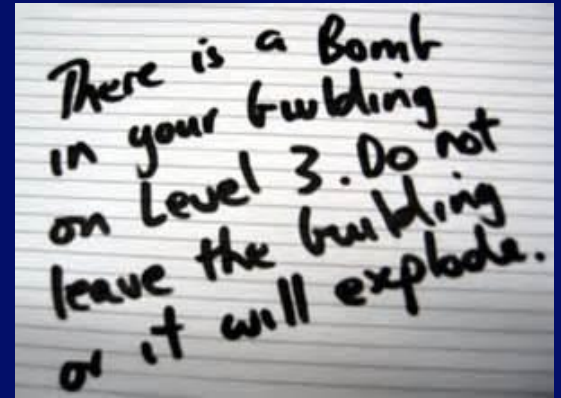
If you receive a bomb threat – one of these 4 things is happening:

- There is no bomb (most likely scenario)
- There is a bomb placed outside
- There is a bomb placed inside
- This is an ambush (gun/knife attack)

BOMB THREAT CHECKLIST	
DATE:	TIME:
TIME CALLER HUNG UP:	PHONE NUMBER WHERE CALL RECEIVED:
Ask Caller:	
• Where is the bomb located? (building, floor, room, etc.)	
• When will it go off?	
• What does it look like?	
• What kind of bomb is it?	
• What will make it explode?	
• Did you place the bomb? Yes No	
• Why?	
• What is your name?	

Bomb Threats

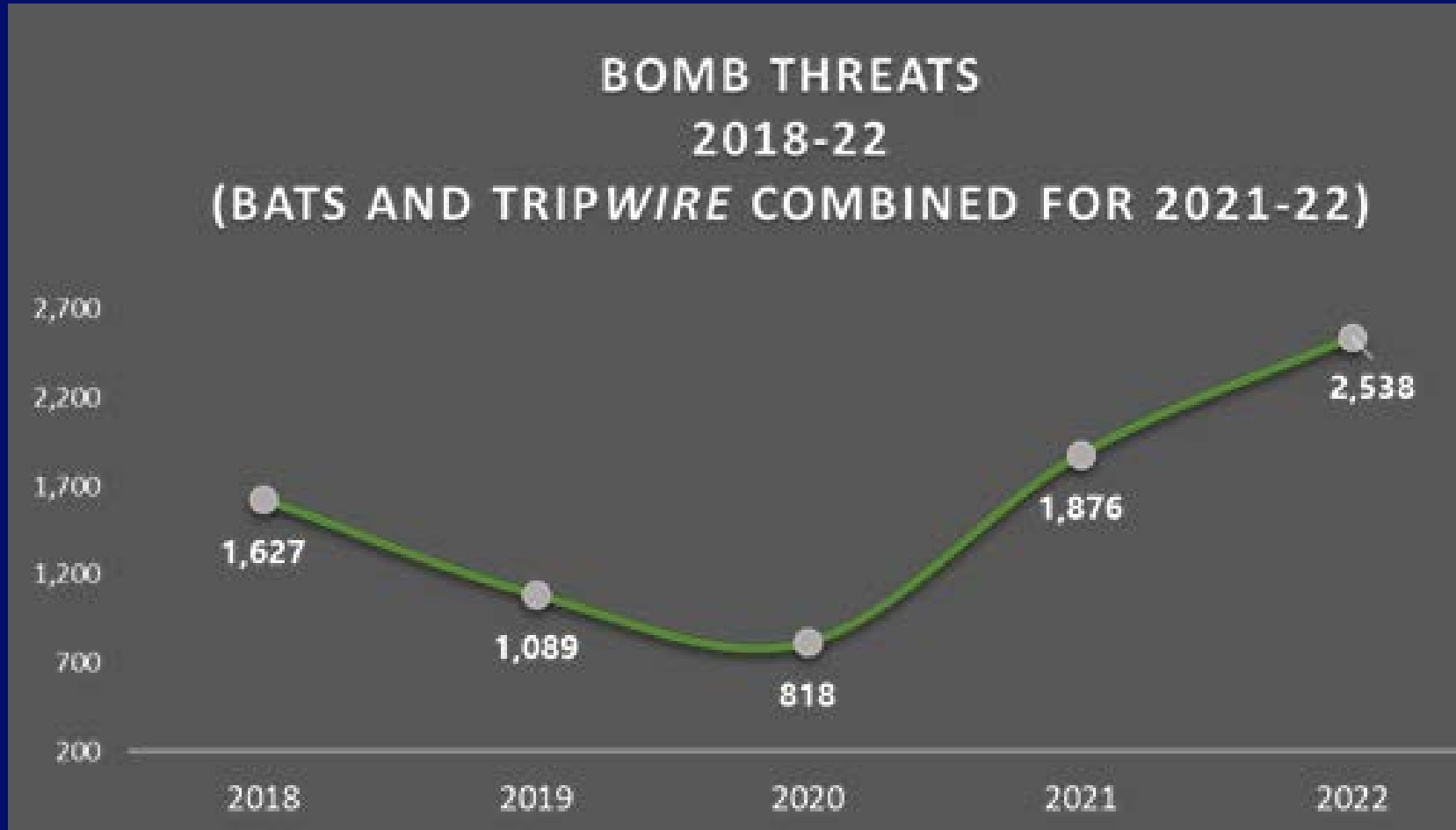
- Total bomb threats made in 2022: 2,538
Bombings after a threat: likely 0
- Total bombings in the U.S. in the last 5 years: 1,683
Bombings preceded by a threat: likely 1 (Nashville)
- Most actors who are a bombing threat will never make one
- Evacuating maybe not the best course of action
- Most "bombs" are crudely made devices like a pipe bomb
- Blast radius much smaller than a vehicle bomb
- Buildings provide best protection



Data from the United States Bomb Data Center, ATF

See my article: *Rethinking Bomb Threat Response*, *Journal of Business Continuity and Emergency Planning*, January 2019

Bomb Threats



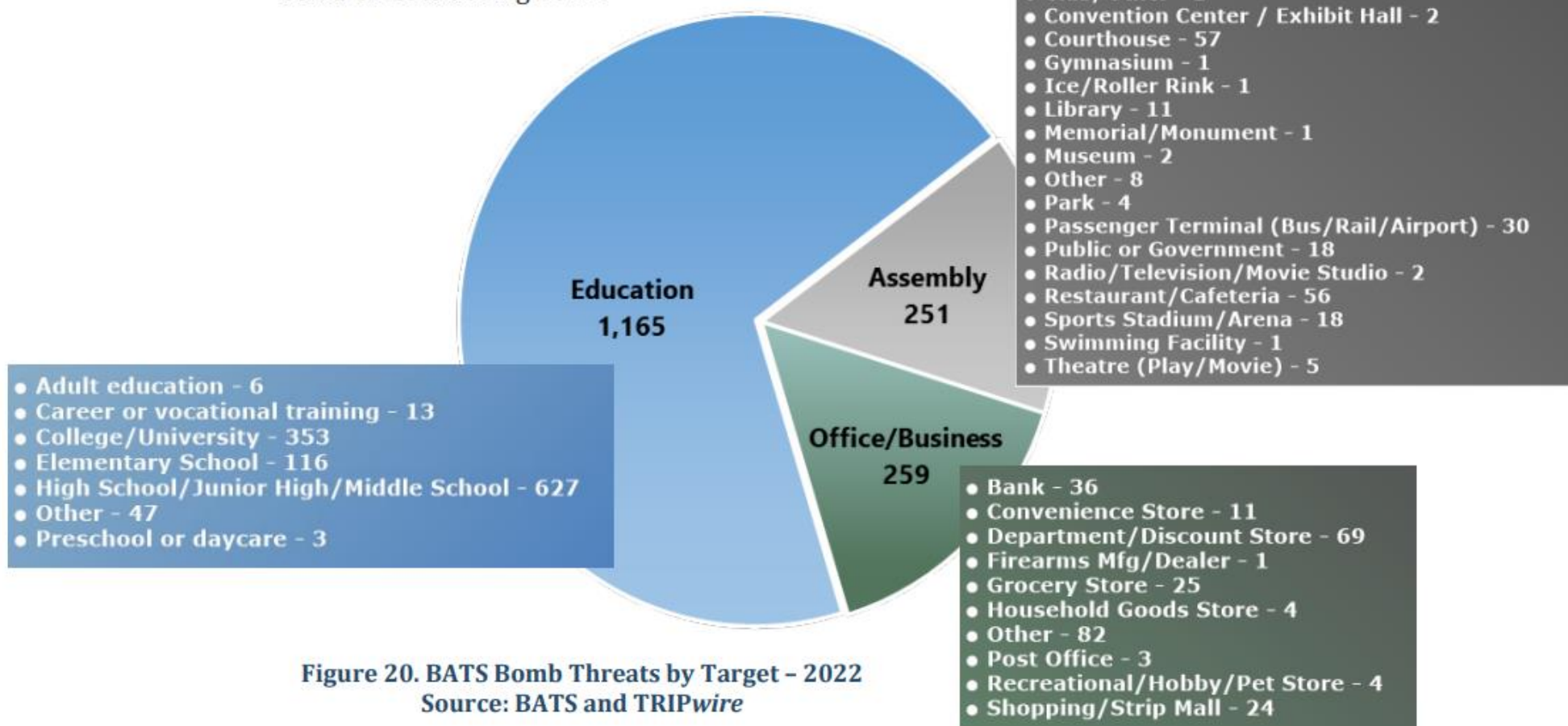
Source: ATF, United States Bomb Data Center

<https://www.atf.gov/resource-center/docs/report/2022-explosives-incident-report-eir/download>

Bombing Threat Targets

4.2 Bomb Threats by Target

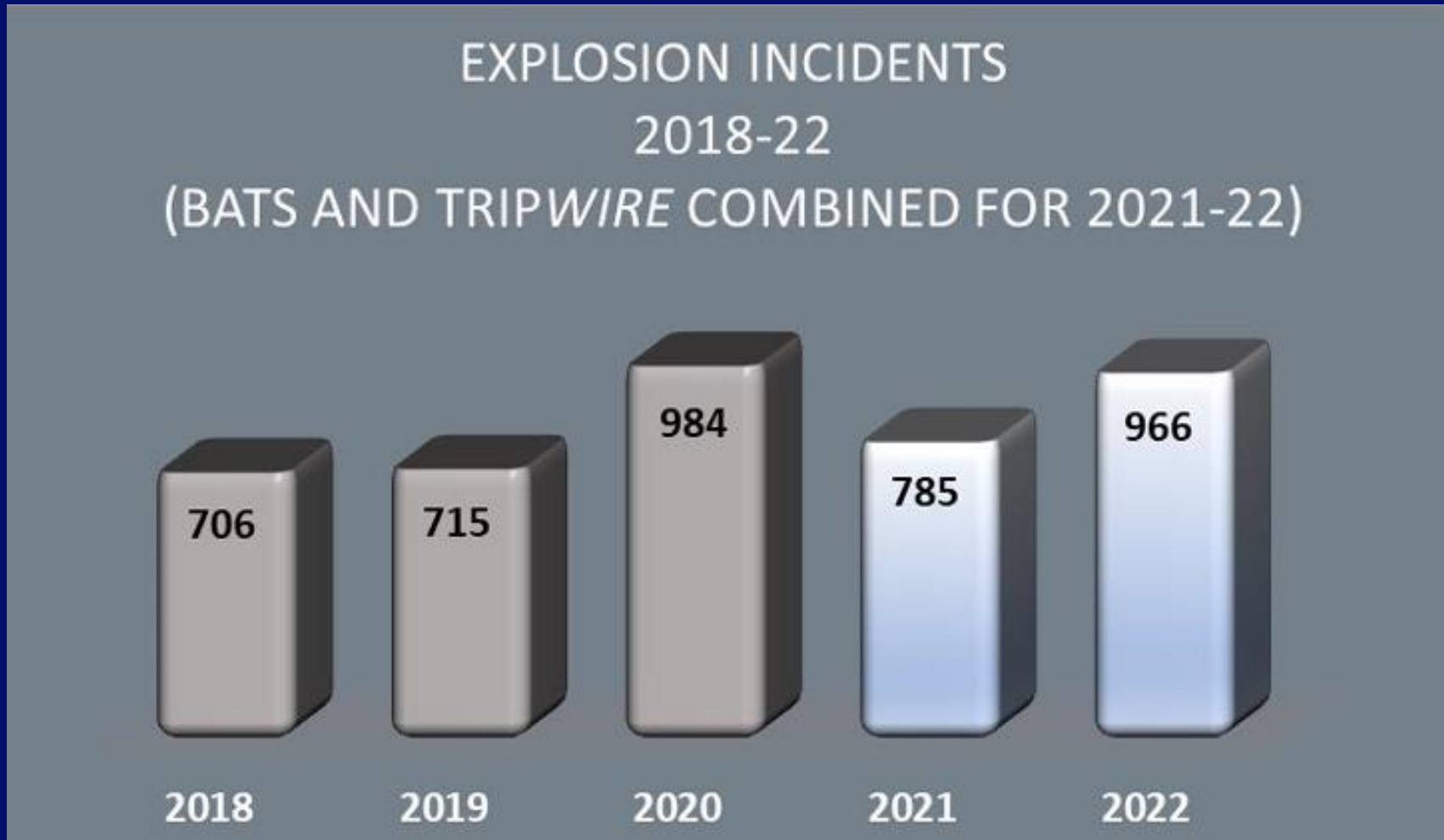
(U) Education facilities (1,165), Office/Business (259), and Assembly (251) locations were the **top three** targets of bomb threats during 2022.



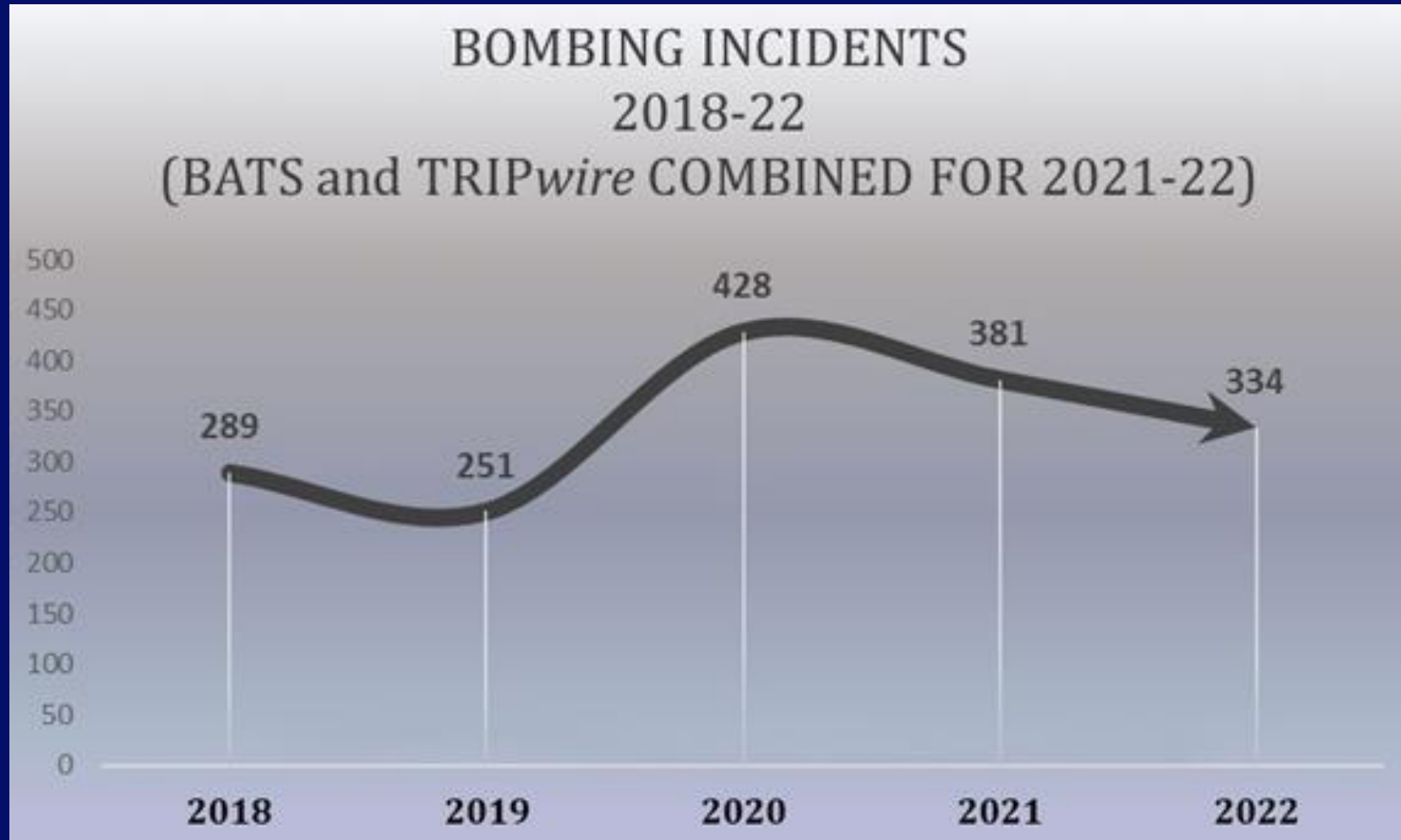
Bomb Threat Case



Explosion Incidents



Bombing Incidents



Research Informs Action

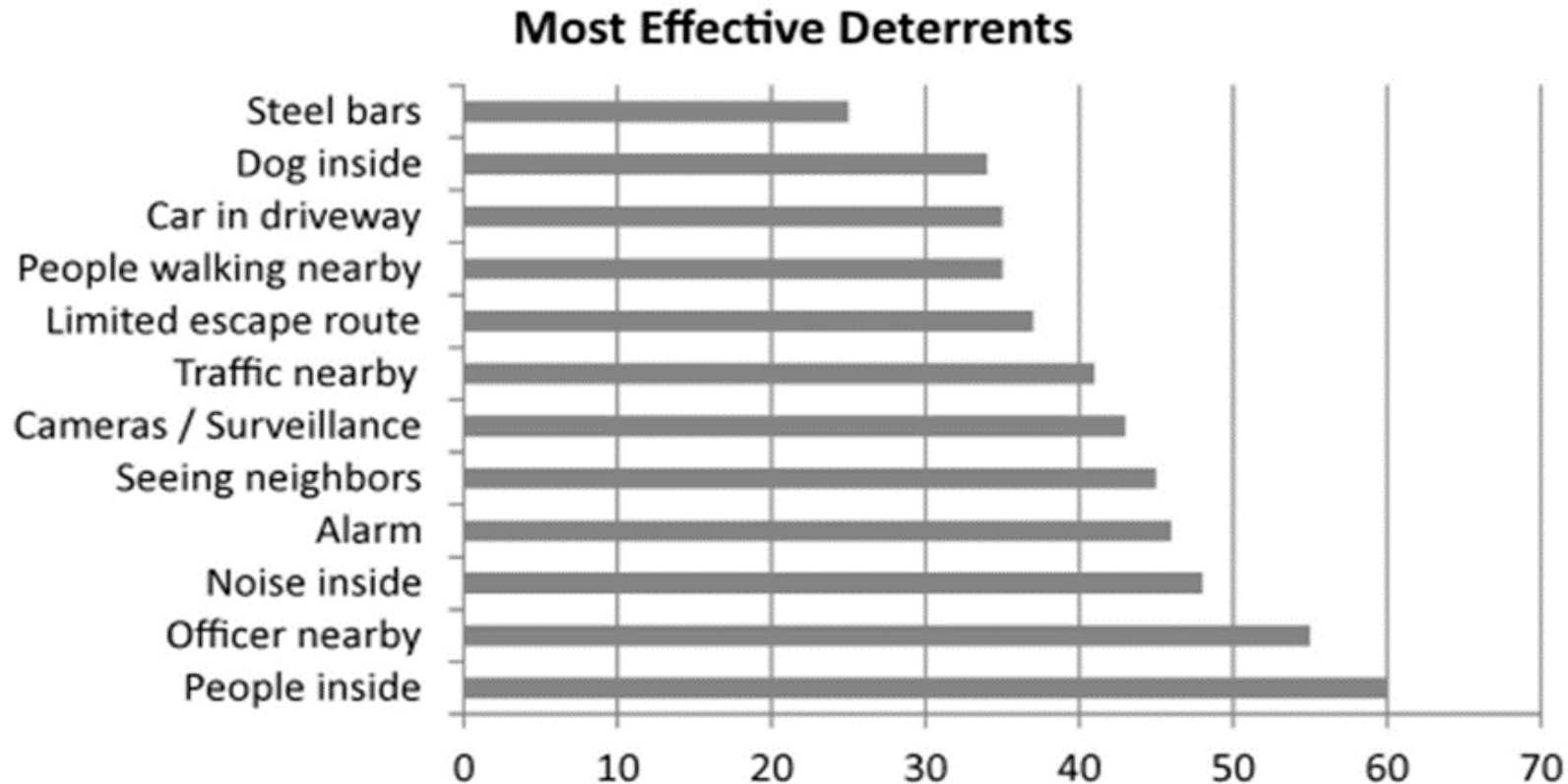
Dr. Martin Gill's research of murders on death row

- Why criminals choose their targets - because they are easy!
- CCTV does not affect the way violent actors commit their offenses, in fact, may escalate their actions
- More concerned about being stopped by people than any type of technology
- Favor large, bulky security guards since they can be outrun
- The decision to shoot and kill a lone security guard actually comes easy - eliminates the one key piece of evidence

Seeing the potential crime scene through the eyes of a criminal is invaluable!

Research Informs Action

Perception of Effectiveness of Burglary Deterrents According to Burglars:
% of sample identifying factors that would cause them to avoid a target
(N=360)

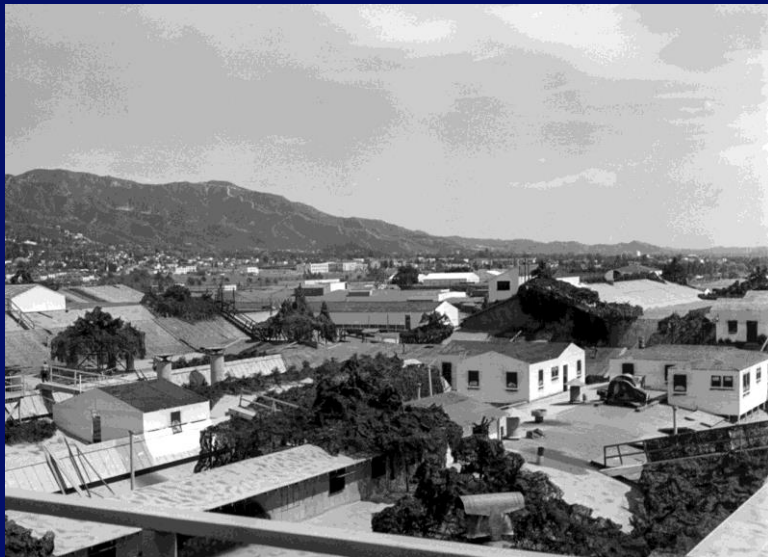


7. No Use of Imagination

Remember the goal of target hardening is to remove enemy from the fight before it starts!

- Divert/off-road: Concealment, cover, disguise
- Deter: Security language on the property, websites, event announcements
- Deceive: Physical deception tactics – look harder than you are!

The best defense is a good offense!





Crime Prevention Through Environmental Design (CPTED)



8. Poor Crisis Preparedness

- Identify “crisis leaders”
- Have a response and communications plan
- Pre-craft crisis messages, communicate often, control the message
- Train for the “golden hour” - invest in life-saving, life-preserving education like *Stop the Bleed*



What's the cost of NOT protecting facility, employees, visitors?

Planning and Training

- Security plans must be tailored and a living document
- Practice = resiliency
- Exercise to failure!
- Leverage the power of smart phones and apps



Hot Topic - Convergence



- Attacks impacting two or more security functions are “blended attacks”
- Convergence is formal collaboration between two disjointed security functions
- Security convergence is often referred to as “converged security”

Source: CISA’s Cybersecurity and Physical Security Convergence website
<https://www.cisa.gov/resources-tools/resources/cybersecurity-and-physical-security-convergence-action-guide>

Convergence

Together, cyber and physical assets represent a significant amount of risk to physical security and cybersecurity – each can be targeted, separately or simultaneously, to result in compromised systems and/or infrastructure. When physical security and cybersecurity divisions operate in silos, they lack a holistic view of security threats targeting their enterprise. As a result, successful attacks are more likely to occur and can lead to impacts such as compromise of sensitive or proprietary information, economic damage, disruption of National Critical Functions (NCFs), or loss of life.

Source: CISA's Cybersecurity and Physical Security Convergence website

Takeaways



- ✓ We all “do” security!
- ✓ Fight the emotional traps
- ✓ Strongly consider insider threat – fight NIMO!
- ✓ Study the threat, calculate vulnerability and risk
- ✓ Identify the “Achilles heel” – fix it!
- ✓ Think rings of security – layers of defense around the target
- ✓ Focus security resources “left of bang”
- ✓ Use data and case studies to inform your security plans
- ✓ Practice and training = resiliency
- ✓ Bake security into decision-making and all activities

We can strike a balance between normalcy and vigilance!

- ✓ Citizens now expect/demand security
- ✓ Making \$\$ decisions based on their assessment
- ✓ In this age, security won't scare them away, but pull them in!

Shape the environment and culture you want.
Take control, be proactive, get on the offensive!

Unapologetically.

Contact Information



*Dr. Jennifer L. Hesterman
Colonel, U.S. Air Force (retired)*

jennihesterman@gmail.com

571.289.7225 cell



Physical Security Threats & Vulnerability Mitigation

Norma Browne

2023 MRO Fall Security Conference



nbrowne@ameren.com

Ameren

We provides energy services to approximately 2.4 million electric customers and 900,000 natural gas customers across 64,000 square miles in Illinois and Missouri.

Our executive leadership is committed to the success of BES resiliency, physical security, and for the reliability of the BES.

- Adversaries have often successfully attacked electric infrastructure internationally. These attacks have included many components of the electric grid including generation, transmission towers, and substations including simultaneous attacks on multiple targets.



Nationwide Bulk Electric System

There is a great deal of emphasis placed on cyber assets, however these assets are useless if we lose our physical infrastructure of generation facilities, substations, transmission & distribution lines:

- 11,000+ power plants
- 79,000 substations
- 642,000 miles of high-voltage transmission lines
- 6.3 million miles of local distribution lines
- 300 million customers

[Transmission – NEMA Electrification Infographic](#)

Today, we will explore identification of risk, unacceptable consequences, “the cookbook”, and the importance of resiliency



Threats to the Bulk Electric System

Historical threats to the Bulk Electric System include

- Thefts of copper
- Natural disasters
- Property damage or vandalism

In addition to these threats, today we face environmentalists, accelerationist, decelerationists, EMP, supply chain, UAS, geopolitical threats, eco-extremists, every other of “flavor-of-the-day” extremist, and the media *e.g. FERC and WSJ March 12, 2014*

Threats to the Bulk Electric System Not Something New...





Imminent Danger: Black Cross Movement Hits Big Coal Giants and Global Forum in St. Louis and Midwest

You shall not press upon the brow of labor this crown of thorns. You shall not crucify us any longer upon a cross of coal...Toxic coal ash contaminates groundwater and soil supplies across the nation;

Manual is an anonymously written WSE manual (also referred to as *The White Patriot Survival Manual*) that provides instructions on various topics such as manufacturing explosives, OPSEC, selective assassinations, leaderless resistance, etc. One section of the manual provides information on sabotaging "electrical power generation and distribution". The manual suggests "attacking the power supply at the source which has the advantage of creating a total blackout of the supplied area with just one attack". The best methods of sabotage are listed as arson, explosives or a long range rifle to "disable substations, transformers and suspension pylons. A



[Download The White Patriot Survival Manual Firearms Explosives Sabotage And Guerrilla Warfare Pdf](#)

Start Download Now



The White Patriot Survival Manual Firearms Explosives Sabotage and Guerrilla Warfare pdf

[Download File](#) [Add to your account](#) [Embed](#)

Size: 0 MB
Pages: 380
Date: 2011-04-01

UNCLASSIFIED // FOR OFFICIAL USE ONLY

Brief No. 13-01-01 Authored by: E. Davis / A. Rice Phone: 407-850-1901



Extremist News Brief

29 January 2013

Militia Extremist Suggests Targeting Power Grids

(U//FOUO) The Central Florida Intelligence Exchange (CFIE) assesses with medium confidence based on extremist chatter, open source reporting and historical trends, that power grids, which represent a vital sector of U.S. infrastructure, continue to be an attractive target for extremist groups or lone offenders seeking to carry out attacks that would have a major impact on the economy, as well as furthering their ideological agenda and long-term strategic objectives.





Aug 2014 AR

Jason
Woodring



June 2014 AZ
A rudimentary
incendiary
device ...
50,000 gallon
diesel fuel tank

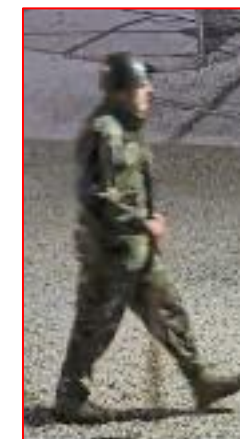


Midwest May 2017



One tower had
approximately 36
bolts and 2 splice
plates missing.
The second tower
had
approximately 60
bolts removed
and 4 splice
plates missing.

Midwest
Feb. 2023





Yemen June 2014 23 million people without power.



Mindanao Philippines January 2017 18 towers & 138 kV transmission lines.



Ukraine November 2015 attack by Ukrainian activists ... use of explosives to destroy four transmission towers ... 1.9 million people or fully without electricity.

December 2014 Dec. 4, two high-voltage transmission power lines from ... cluster of hydroelectric dams inexplicably went offline, power loss to 188,000 Montreal area customers.



Threats to the Bulk Electric System

PGE Metcalf Substation March 20, 2015

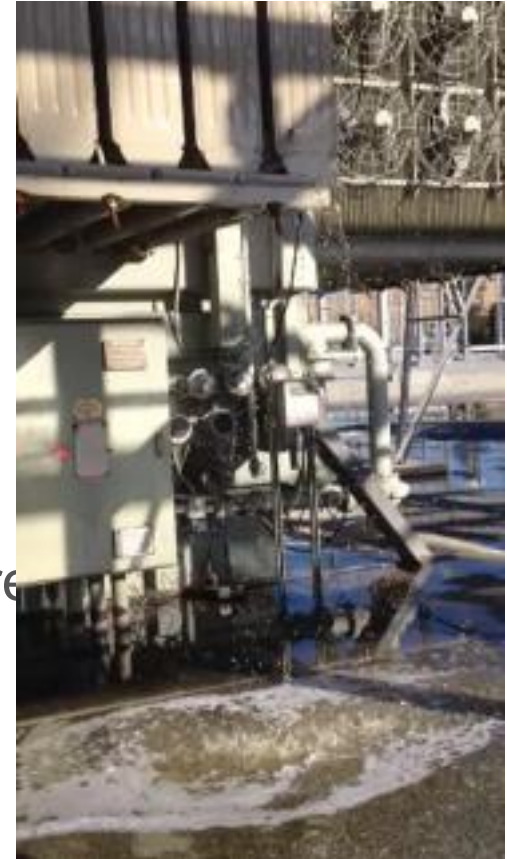


The sniper(s) utilized 7.62x39mm rounds to target the **oil-driven cooling systems** for 17 large transformers. The shell casings found had been wiped clean of fingerprints.



In excess of 120 (7.62) shell casings were located. 110 impact points were documented on PG&E equipment.

<https://www.youtube.com/watch?v=7N-4tynUMJo>



Threats to the Bulk Electric System

Electromagnetic Pulse – Grid Resilience

- An EMP is a blast of electromagnetic energy that can disrupt—if not destroy—electronic devices within a given area
- Within the range of EMPs, there are variations in terms of impacts and responses. Just as the consequences and likelihood of each of these threats vary, so, too, does the approach to protecting the electric grid against them
- While “devices” can produce an EMP to create a local impact, EMPs generated by a high-altitude nuclear explosion are the only ones that pose a widespread potential threat to the reliability of the electric power grid as a whole - or within a region.



Threats to the Bulk Electric System

Create Your Own EMP Generator

<http://www.wikihow.com/Build-an-EMP-Generator>

1. Obtain a disposable camera
2. Open the case
3. Slip on a pair of rubber gloves - if you touch the flash capacitor, it carries about 300 volts
4. Locate the capacitor
5. Discharge the capacitor
6. Remove the board and capacitor
7. Prepare your wire to connect the switch to the capacitor.
8. Solder the wire.
9. Attach to the switch.
10. Prepare your coil.
11. Remove the enameled coating on the wire
12. Solder the coil to the capacitor
13. Attach the coil to the switch.
14. Fire when ready

Threats to the Bulk Electric System

UAS

Ameren CIP-014 Workshop: Featured a segment titled “Drones: Threats, Benefits, and Laws”, presented by a FAA licensed pilots, A&P (full-sized airframe & power plant) aircraft mechanics, who are UAS owner-operators. Live demonstrations of nine UAS capabilities were presented at a University arena to validate the UAS threat potentials. Topics included surveillance threats, investigative, operational, and security use of UAS.

- As you encourage coworkers to be aware of their surroundings ensure they listen for UAS while they are in the field
- Train coworkers to immediately report a UAS to your Security Operations Center. Ensure your SOC procedure includes information vetting against company flights and internal information dissemination.
- If it is safe to do so, have the coworker note the location the UAS came from, went to, and if possible, observe who may be operating the UAS.



Interdependencies With Other Critical Infrastructure

Interdependencies with other critical infrastructure require special consideration

Banks, data centers, transportation, law enforcement, EMS - even our own natural gas operations are dependent on electric infrastructure

“Running a compressor station on electricity creates a coupled vulnerability between what were once two independent energy supply systems. A substation attack in the Northern Tier resulted in exactly this, a short-term outage to a compressor station

Similar coupling vulnerabilities can occur with oil delivery systems, communication systems, railways, and other critical infrastructure”

Q1-Q3 2023 DNGISAC had 131 incident reports EXCLUDING suspicious activity, vandalism and trespassing

Compliments to John Bryk DNGISAC





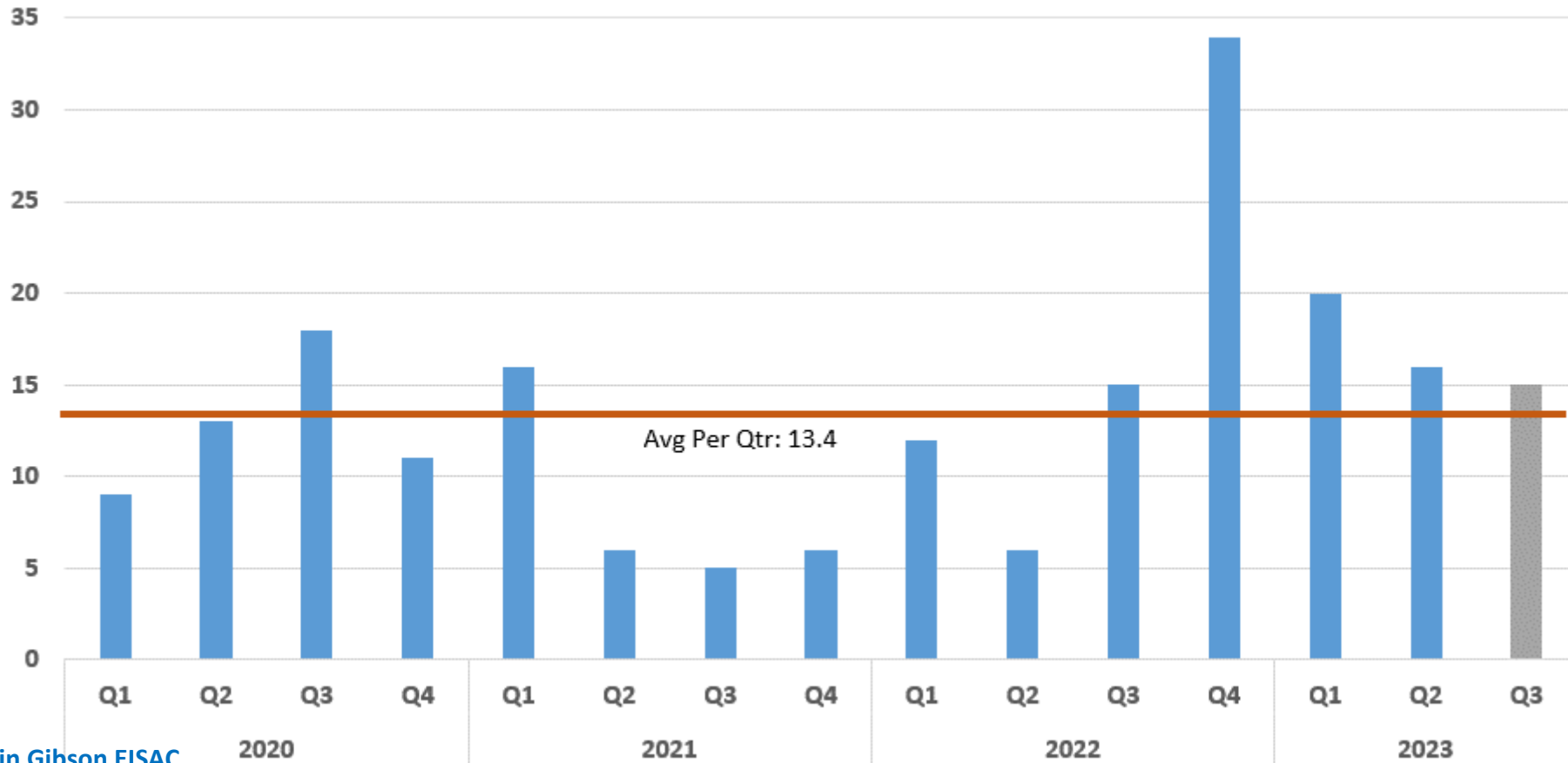
What Are the Threats?



Physical Security Trends: Grid Impacting Incidents By Quarter

The following chart shows the number of Level 2 and 3 incidents (combined) shared with the E-ISAC by quarter. Please note that Q3 2023 is in progress and is represented in gray.

- **Level 2:** incidents with some impact to the grid
- **Level 3:** incidents with significant impact to the grid

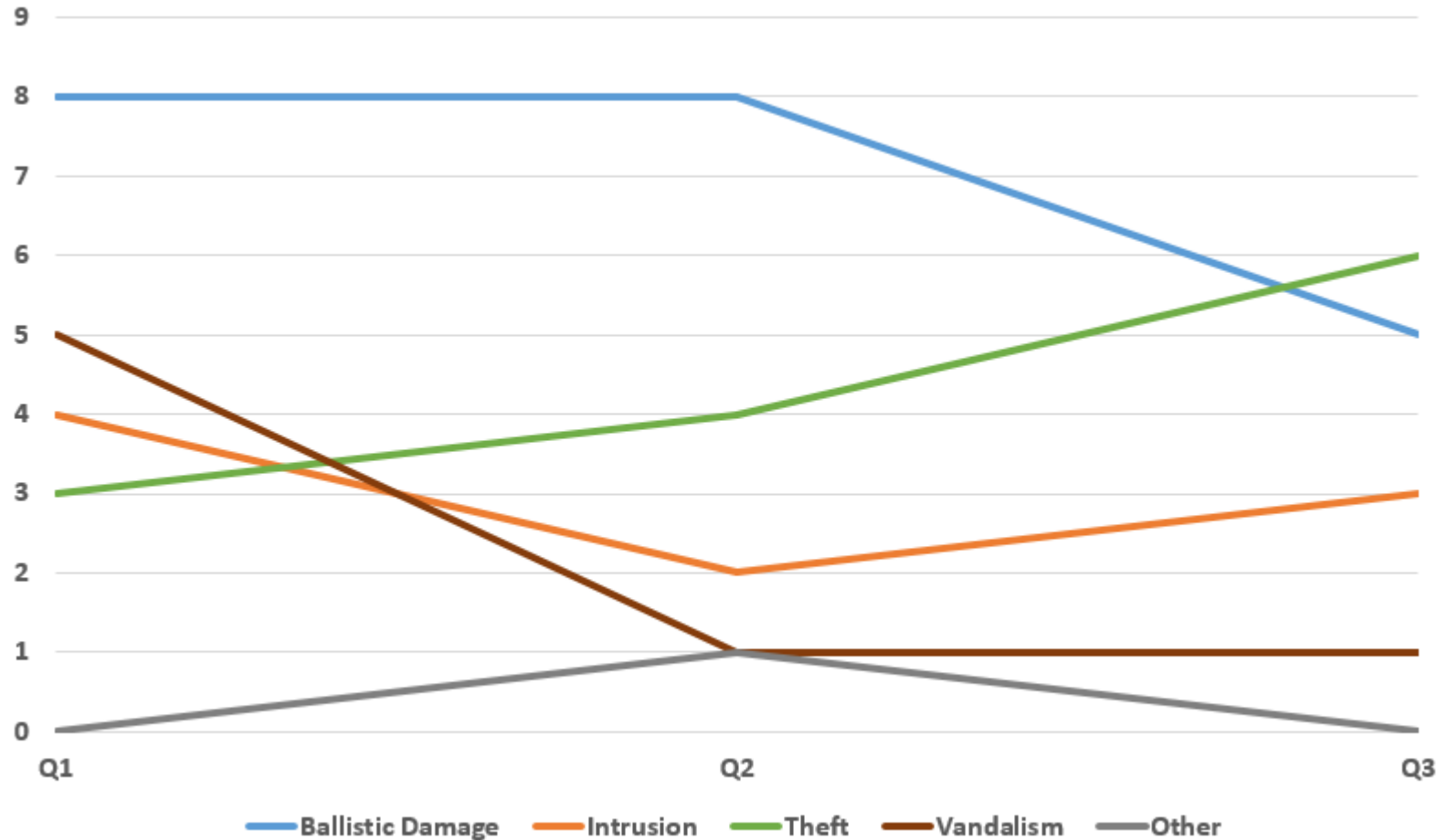


Compliments to Benjamin Gibson EISAC



Physical Security Trends: Grid Impacting Incidents By Type

The following chart shows the number of Level 2 and 3 incidents (combined) shared with the E-ISAC in 2023 by incident type. Please note the third quarter is still in progress.

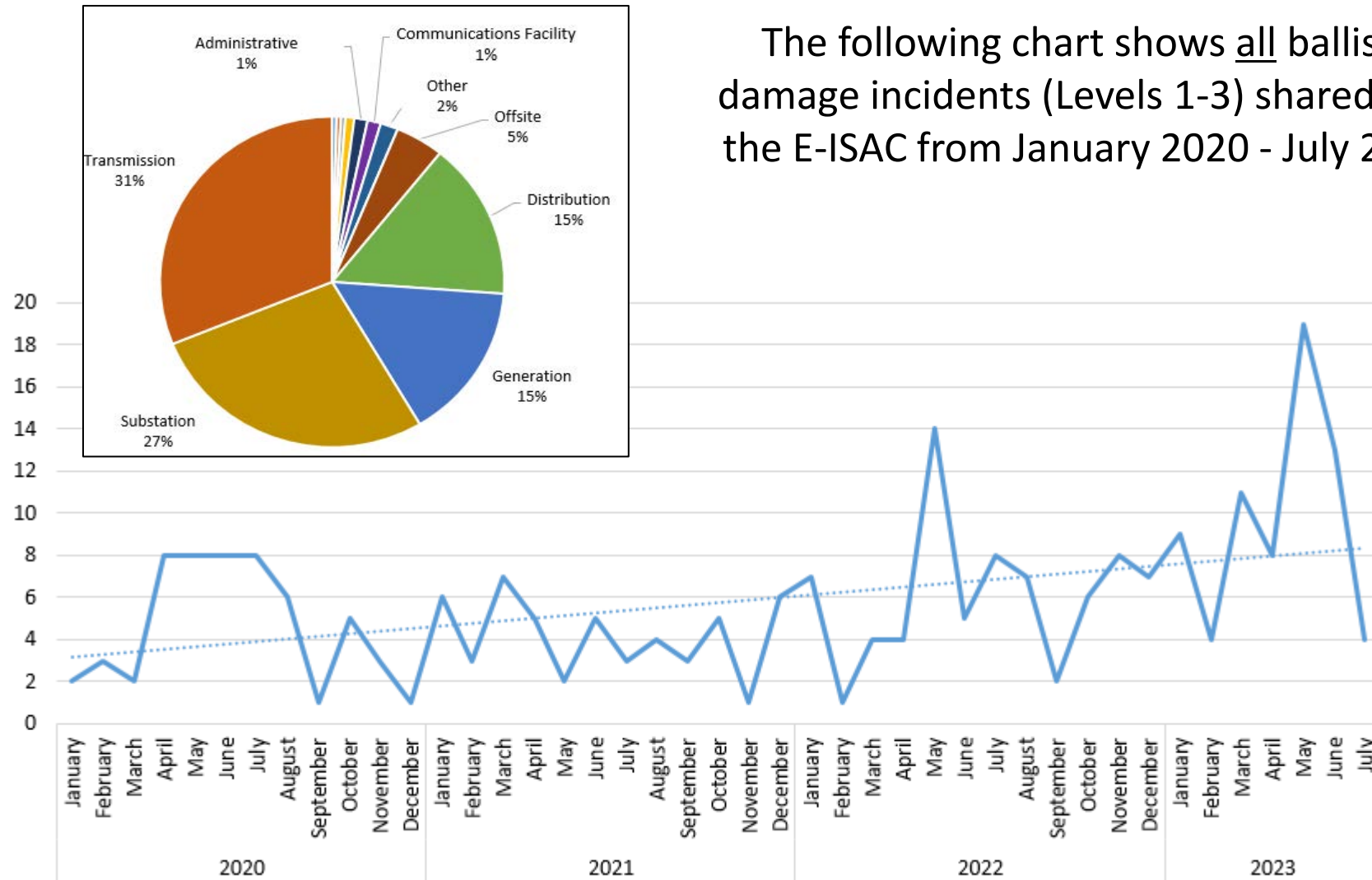


Compliments to Benjamin Gibson EISAC



Increase in Ballistic Damage

The following chart shows all ballistic damage incidents (Levels 1-3) shared with the E-ISAC from January 2020 - July 2023.



Compliments to Benjamin Gibson EISAC

Them: The Threat is Motivated, Agile, Knowledgeable, Determined...



Us: Our Industry is NOT a Sitting Duck...



Vulnerability Assessment Considerations



Vulnerability Assessment

Access or Attack Methods & Potential Aggressors

- Forced
- Duress
- Surreptitious
- Deceit
- Granted access
- Vehicle / ATV / Waterway
- Air
- Subterranean
- Gunfire / Weapons
- Arson
- UAS
- Criminal
- Domestic terrorist
- Rogue/lone wolf
- Insider
- International terrorist
- Any extremist

Vulnerability Assessment



Areas for assessment can be grouped into distinct risk areas:

- Outside the Perimeter
- Perimeter
- Equipment
- Buildings or Enclosures
- Areas within Buildings or Enclosures
- Communications



Vulnerability Assessment

Considerations

- IP and wireless security devices can be hacked and blocked
- Insider threat / misuse of knowledge / failure to protect information
- Physical attack elsewhere to divert emergency responders and result in a delay to a primary site
- A staged incident that would delay an emergency response
- Actions to render your critical facility inoperable or uninhabitable by impacting:

Communications
Electric

HVAC
Water

Fire
Sewer



Vulnerability Considerations

- Lack of available significant/high-value replacement components
- Lack of secured off-site storage for significant spare components
- Overall culture of security / Gaps in or lack of security mitigations
- Gaps in or lack of physical security policies and procedures
- Visitor and tour restrictions (prohibited, who can authorize, hours permitted)
- Key / access management
- Procedural controls for vehicles, identification badges, uniforms, personal protective equipment (PPE) which could be used to gain access or "blend in"
- On-site personnel or security personnel

Site Related Target Attractiveness

- Consider substations which may be impacted by a generation facility attack
- Will Circuit breakers and relays mitigate the impact and risk
- Consider substations needed for black start
- Distance from features such as trees, hills, tall buildings with windows, etc.
- Line of sight distance of target from approach avenues
- Distance from and speed of vehicle traffic (vehicle or VBIED attack)
- Is there easy vehicle access to the site? Egress?
- Can the site be impacted as collateral damage due to proximity to other targets?
- Number of key components at the location
- Proximity to law enforcement or emergency personnel
- Consider historical & proximate attacks at similar facilities



Vulnerability Assessment 101

*Who determines site
criticality?*



Vulnerability Assessment 101

WHAT are we protecting?

WHAT are we protecting AGAINST?

Vulnerability Assessment



EISAC VISA Vulnerability Assessment Tool

Ameren utilized the VISA for a variety of sites: substation, generation, and gas facilities

- SMEs identified “unacceptable consequences”
- Through the base case scenarios developed by our team to achieve the “unacceptable consequences,” we assessed each layer of the site’s physical security strength and weaknesses
- Our team developed security upgrade cases to test the site’s physical security effectiveness against the threats in our DBT

Key Takeaways:

- Offered an invaluable team building experience for success and engagement
- Myth busters on how to achieve the unacceptable consequences
- Provided the confidence that the threat can be mitigated
- Mapped out the justification for upgrades (“shows the work”)
- Developed a sound business case to make informed risk-based decisions
- E-ISAC provided excellent facilitation of the workshop; single POC, start to finish.

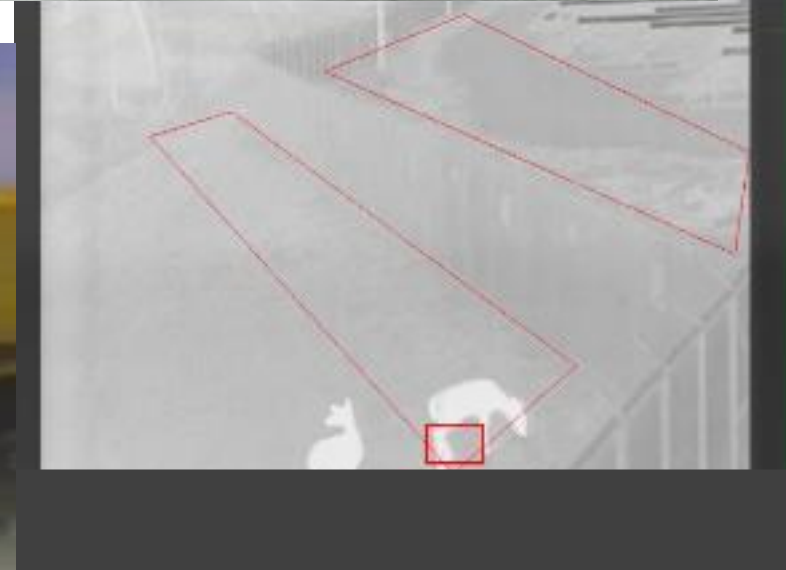
Vulnerability Mitigation Process

- Identify Vulnerabilities and the Most Critical Path
- Identify Resiliency or Security Measures in Place
- Define Resiliency or Security Measures to be Added
- Identify Ownership for the Resiliency or Security Measures



Protection

Vulnerability Mitigation Does Not Need to be Costly – Be Creative



Performance Testing



Performance Testing – Test It Until You Defeat It

Test what is not expected

Test both what is written down and installed

Three things can Make Us or Break Us:

- Equipment Performance
- Security Ops Center Personnel / Response
- Law Enforcement Response

If any aspect of your system fails - the system fails

If you don't test your system – YOU fail





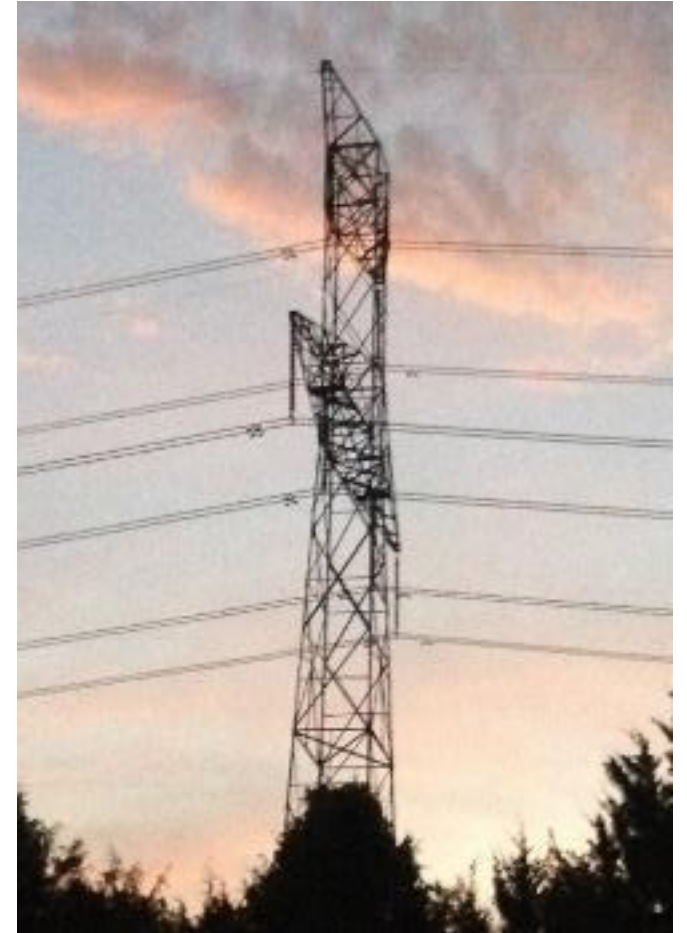
Single Point of Failure

Security Operations Centers

All alarm **detection**, **assessment**, **communication**, and **response** to a physical intrusion or attack occurs within your Security Operations Center.

Your Security Operations Center is **single-point of failure vulnerability** for all critical facilities...

- Procedures?
- Training?
- Contract security guards?
- Company personnel?



Resiliency



Resiliency Considerations

- Reputational risk can quickly become a matter of corporate trust.
- Spare components, facilities, & lines
- Ballistic protection & ballistic rated transformers
- Polymeric bushings
- “Strategic” ballistic protection for buildings containing BES assets
- The greatest resiliency is system design so that you are not dependent on any particular substation to maintain reliability.





Ameren
FOCUSED ENERGY. For life.

Norma Browne

nbrowne@ameren.com

314-541-6802

PHYSICAL SECURITY





MIDWEST
RELIABILITY
ORGANIZATION

Thank You!

2023 Security Conference Survey:



<https://www.surveymonkey.com/r/GTGH759>