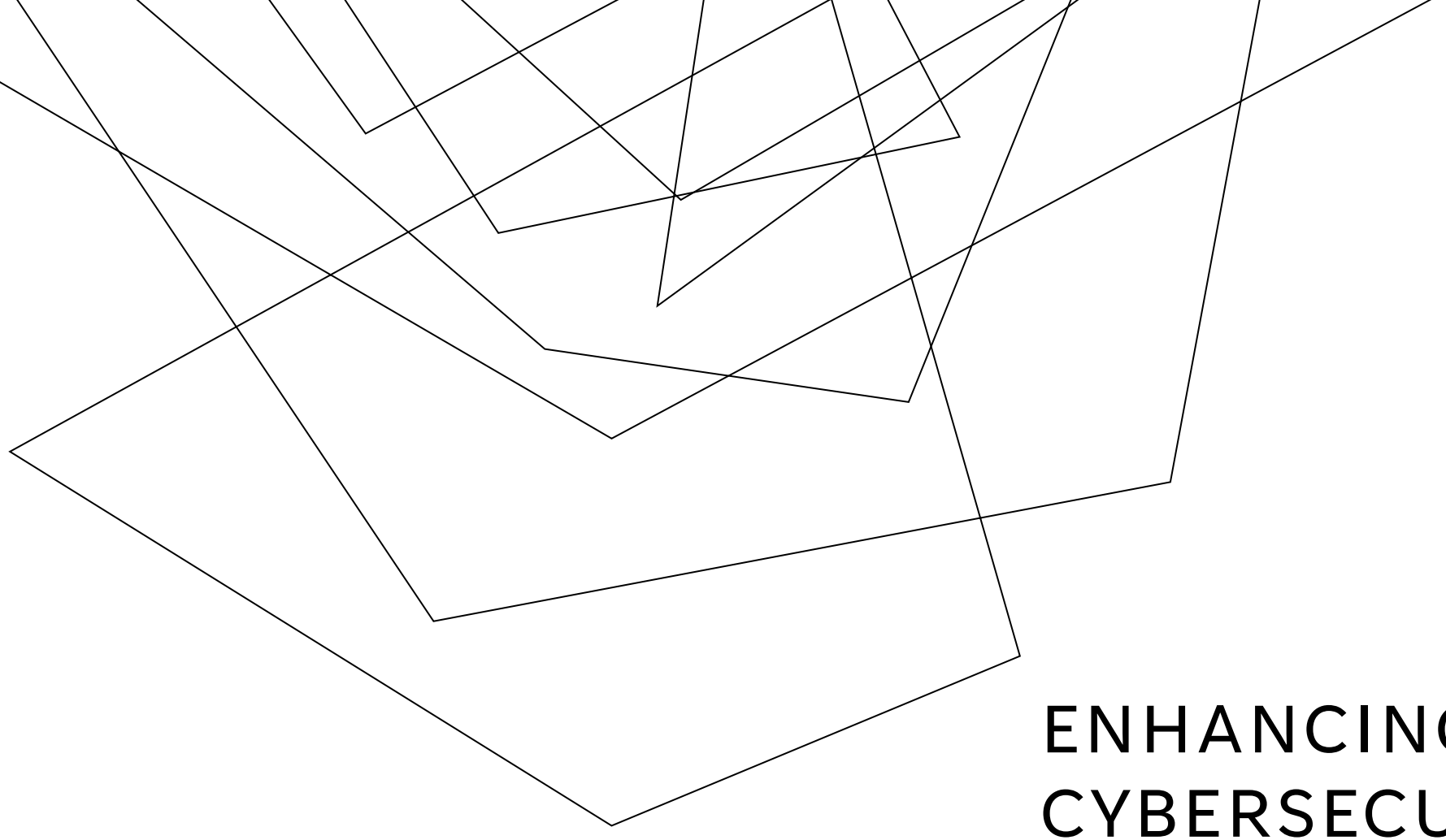


ENHANCING CYBERSECURITY FOR LOCAL GOVERNMENT

Shuchi Wadhwa | Chief Information Officer | Racine County

2023

AGENDA

introduction

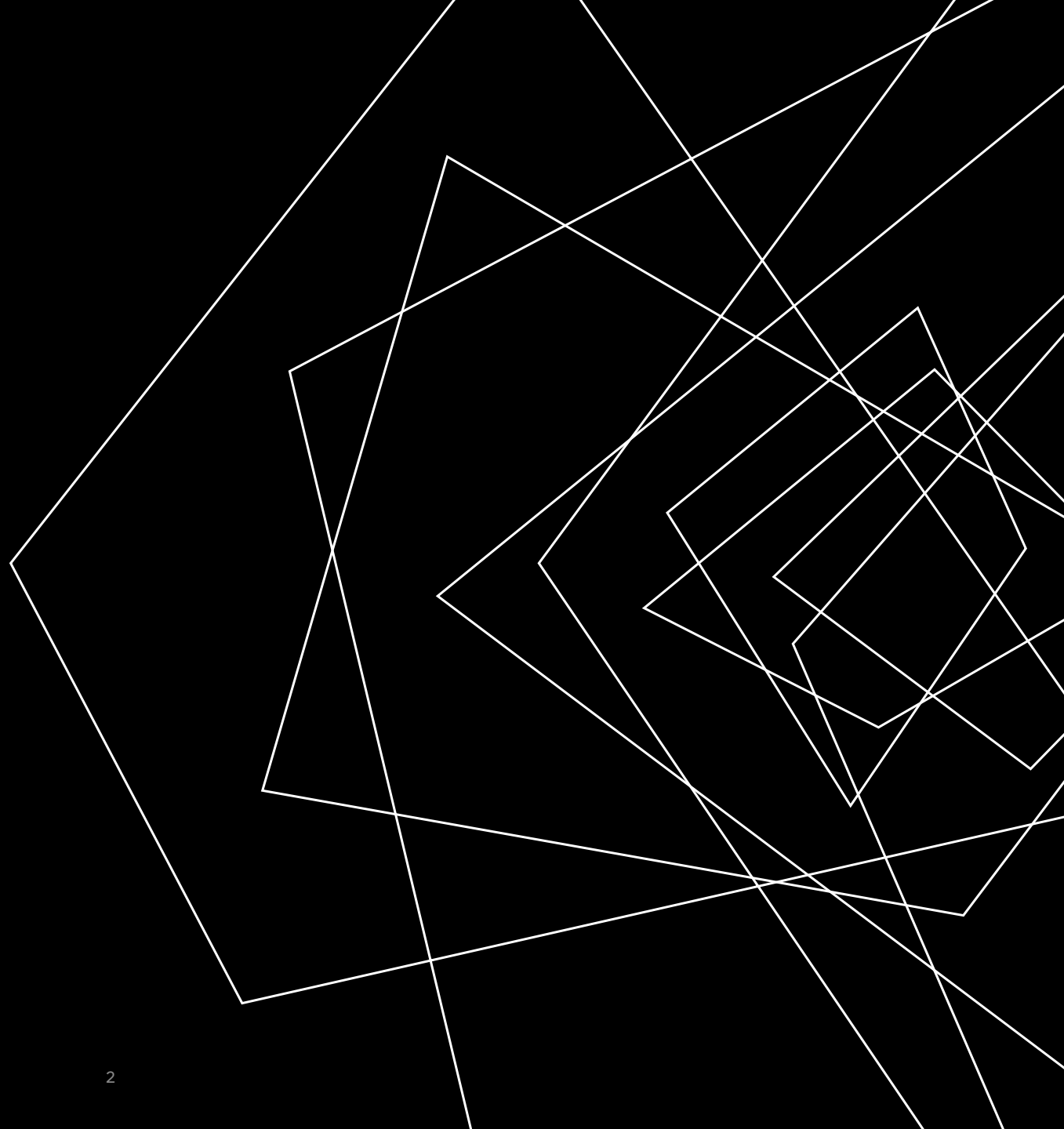
the fundamentals

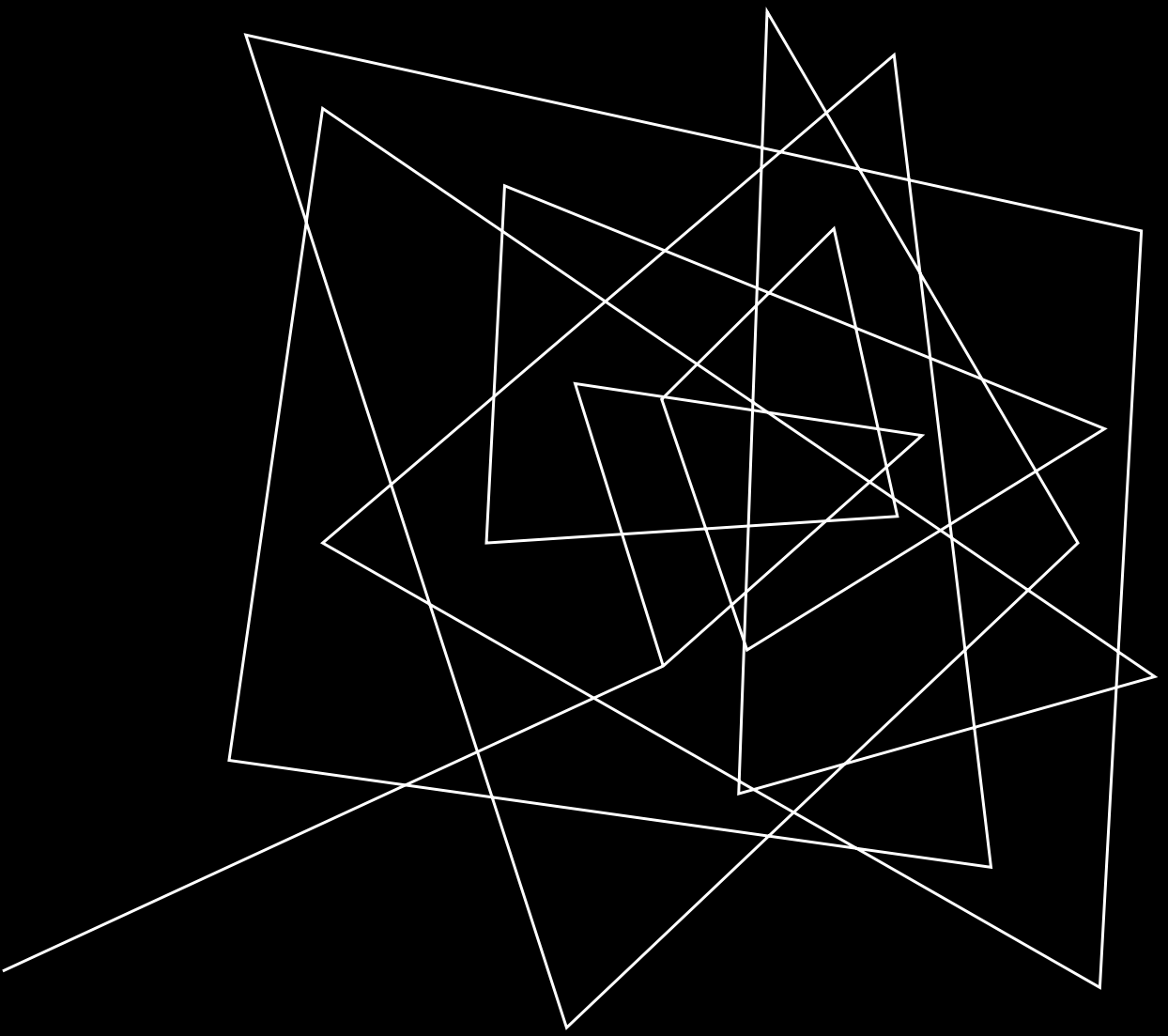
we upped our security...up yours!

interagency security model - consortium

summary

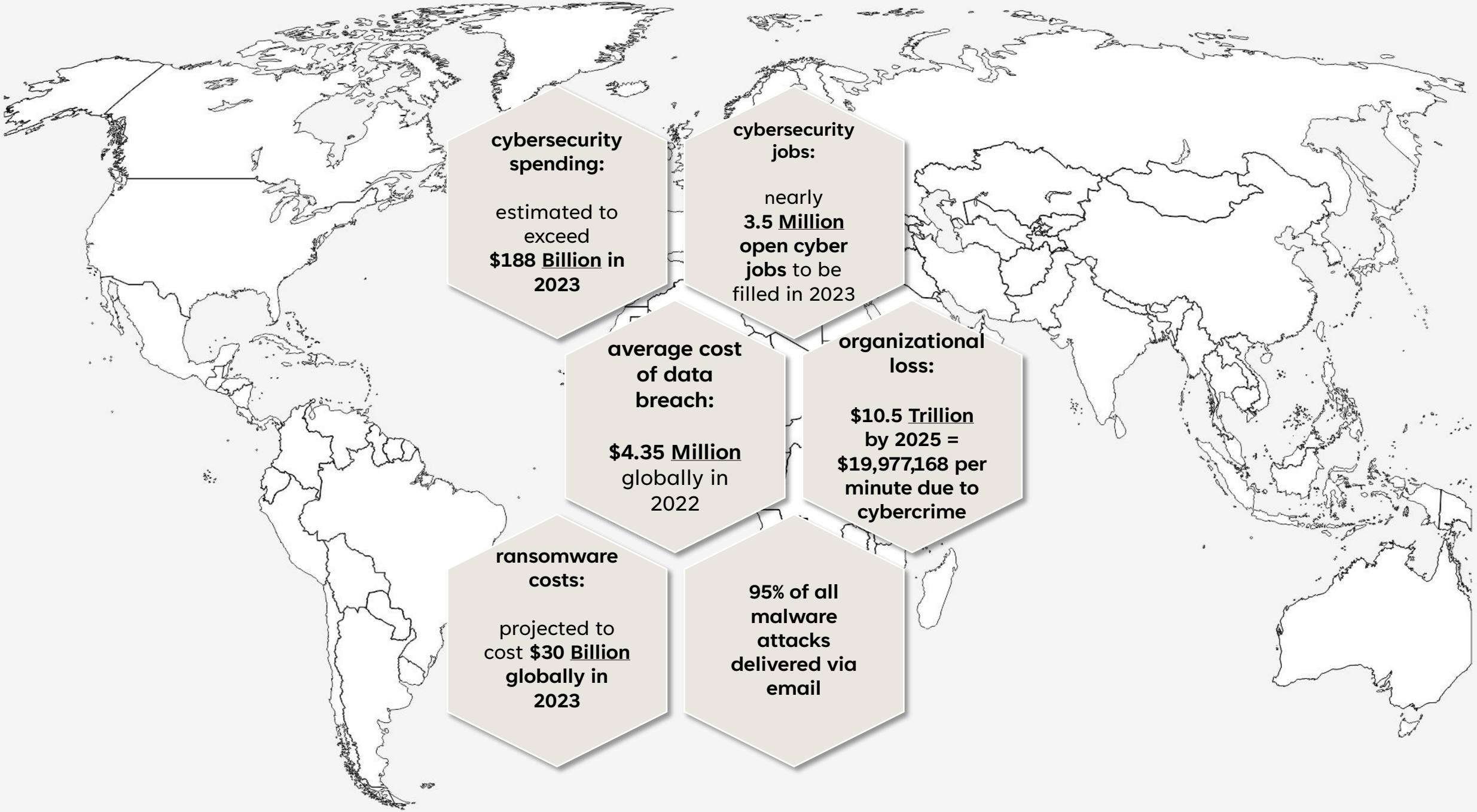
call to action





INTRODUCTION

Who am I?


cybersecurity spending:
estimated to exceed **$188 Billion in 2023**
cybersecurity jobs:
nearly **3.5 Million open cyber jobs** to be filled in 2023
average cost of data breach:
$4.35 Million globally in 2022
organizational loss:
$10.5 Trillion by 2025 = $19,977,168 per minute due to cybercrime
ransomware costs:
projected to cost **$30 Billion globally in 2023**
95% of all malware attacks delivered via email

The Journal Times

Ransomware infects City of Racine computer systems

RACINE — City of Racine computer systems were infected by ransomware early

FIRST ALERT WBAY.com

City of Oshkosh computer system hit by virus

The City of Oshkosh been hit by a com virus that's imp website, ema

FOX6 MILWAUKEE

As Kenosha responds to historic protests, the city faces cyberattacks or 'hacktivism'

KENOSHA, Wis. - The City Kenosha has been fight cyberattacks since the of Jacob Blake. They're "denial of service" atta which either flood a v it harr mak

milwaukee journal sentinel

Confidential information of 9,500 patients at the Medical College Wisconsin compromised

The compromised email acc one or more of the follo information: patien addresses, date numbers, health dates of service, su diagnosis or medica treatment informatio

FIRST ALERT WBAY.com

City of Fond du Lac online water payment system hacked

Officials with the City of Fond du Lac say its Water Payment Portal has been hacked, and people who pay their water bill online through the system should check their credit card statements.

ik - sports

CBS 58 YOURHOMETOWN AWARDED BEST WEBSITE by the Wisconsin Bro

Village of Whitefish Bay targeted by cyber security attack

WHITEFISH BAY, Wis. (CBS 58 According to a news release, t Village of Whitefish Bay was targeted by a "malicious and sophisticated cyber security attack" on Saturday, July 31.

The Record. Recorded Future® News

Ransomware group claims attack on Wisconsin school district

A ransomware group took responsibility for a cyberattack on school district in Wisconsin serving nearly 20,000 students.

The Snatch ransomware group added the Kenosha Unified School District

milw

Wisconsin's statewide court system slowed by denial-of-service cyberattack

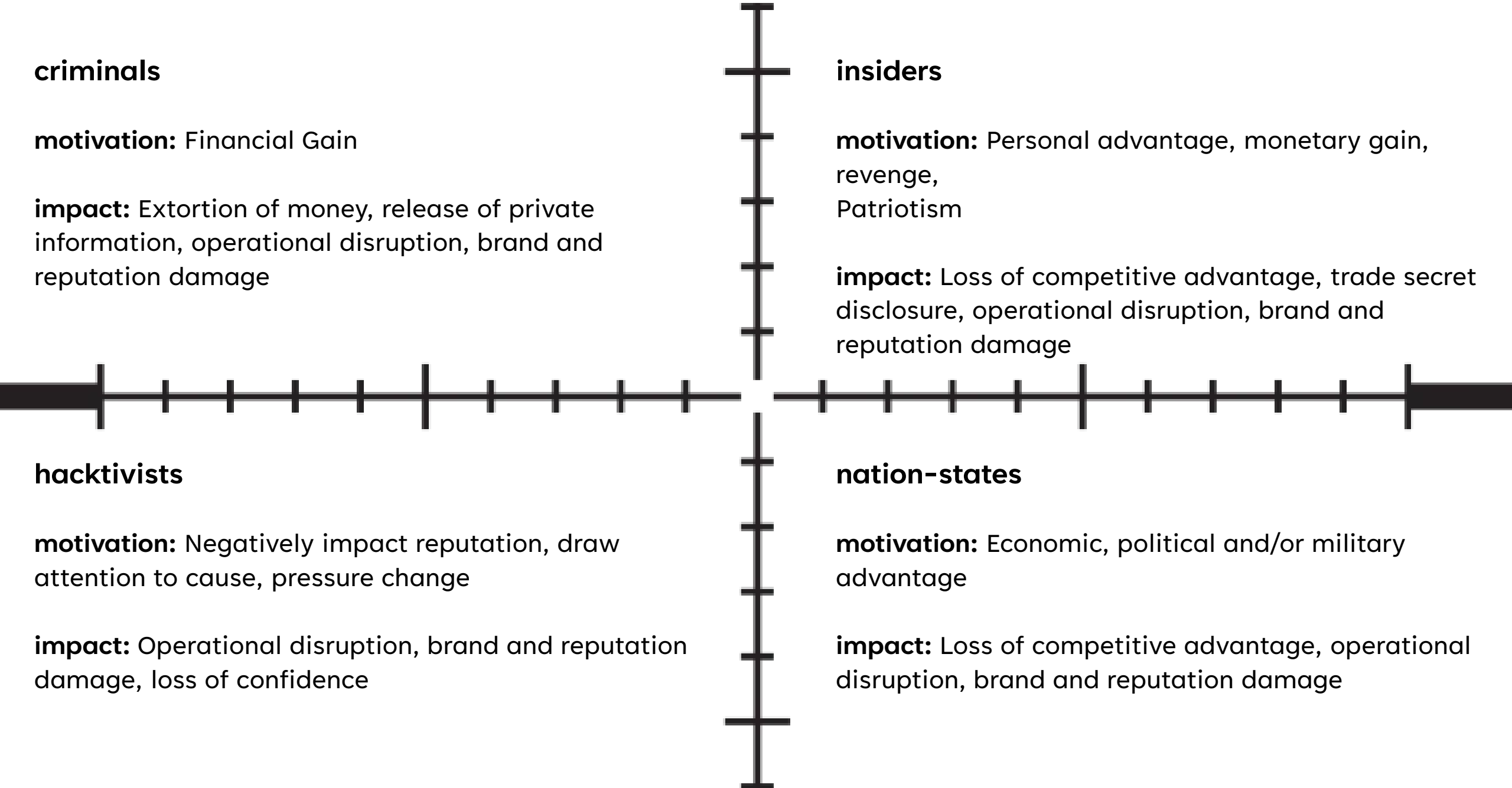
An attempted cyberattack on the Wisconsin court system's computer network caused intermittent delays and slower response times earlier this week.

rnal sent

Rock County Services suffers cybersecurity incident

A phishing scam earlier this year led to a security breach within Rock County Human Services. County Administrator Josh Smith says all affected parties have been contacted

WHO HAS YOU IN THEIR CROSSHAIRS?



criminals

motivation: Financial Gain

impact: Extortion of money, release of private information, operational disruption, brand and reputation damage

insiders

motivation: Personal advantage, monetary gain, revenge,
Patriotism

impact: Loss of competitive advantage, trade secret disclosure, operational disruption, brand and reputation damage

hacktivists

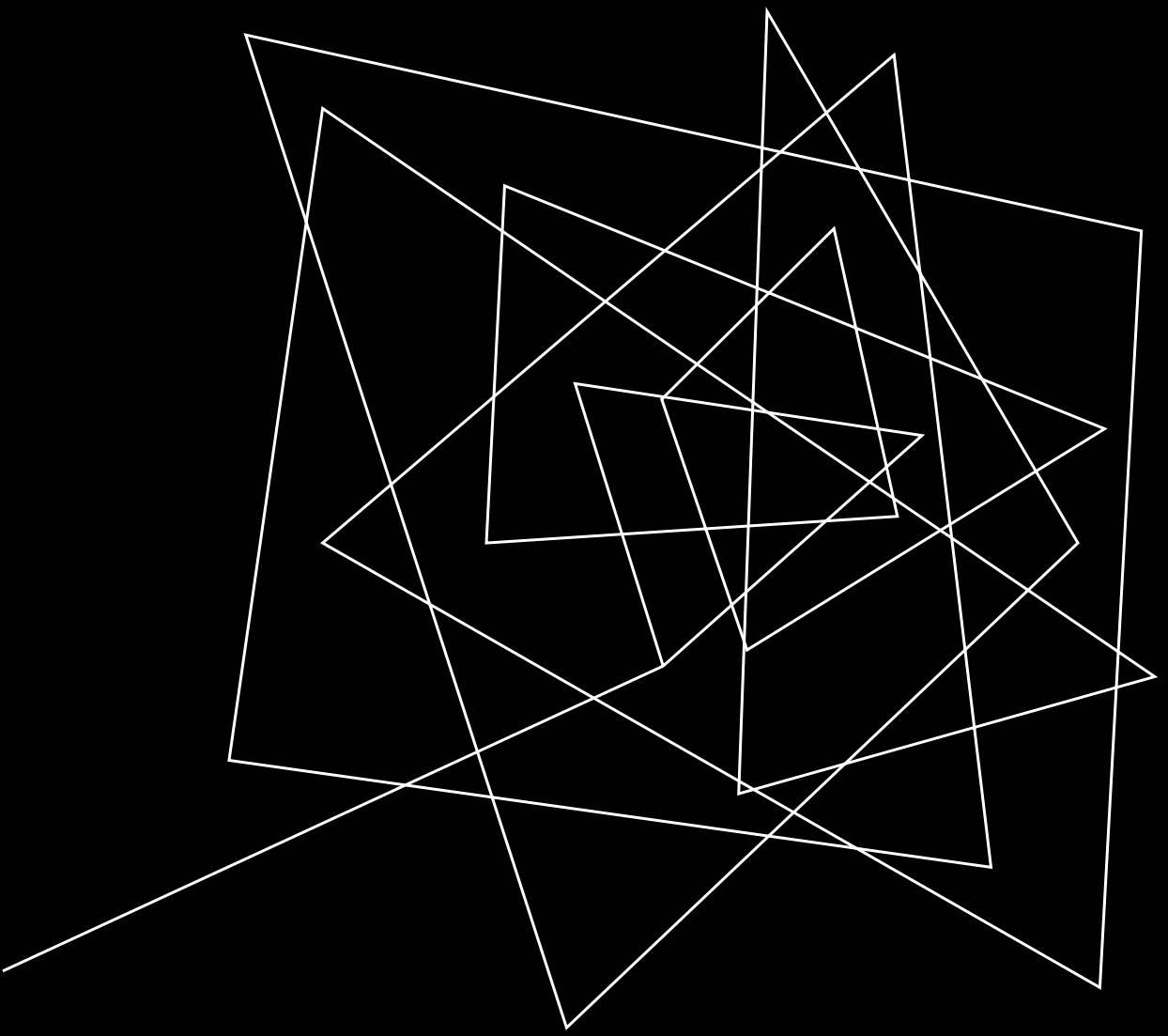
motivation: Negatively impact reputation, draw attention to cause, pressure change

impact: Operational disruption, brand and reputation damage, loss of confidence

nation-states

motivation: Economic, political and/or military advantage

impact: Loss of competitive advantage, operational disruption, brand and reputation damage



THE FUNDAMENTALS

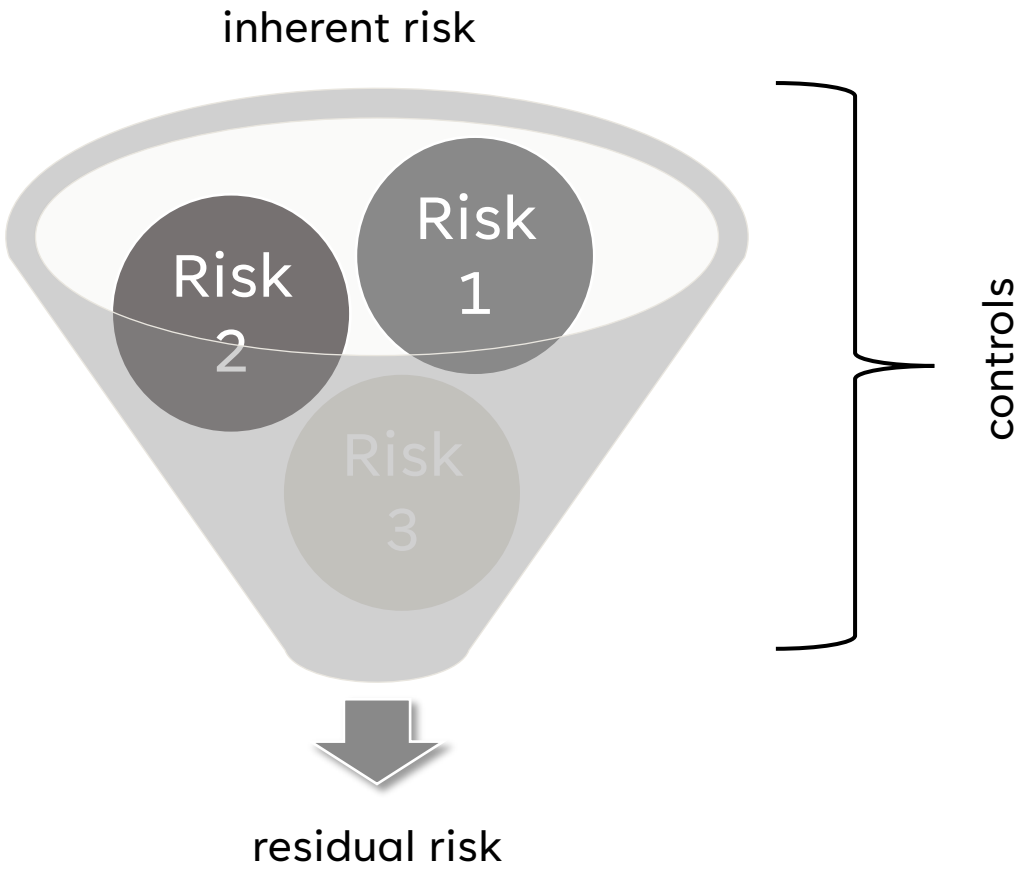
Cybersecurity IS Risk Management

COMPLEXITY OF A MODERN ORGANIZATION

- email
- mobile devices
- website
- social media
- credit card transactions
- BYOD and office policy
- network management
- backup and remote access

MANAGING CYBER RISK

MITIGATION VS. ELIMINATION OF RISK



MAIN CYBER THREATS AFFECTING LOCAL GOVERNMENT

phishing

Social engineering attack involving trickery

Designed to gain access to systems or steal data

Targeted phishing is "spear phishing"

Variants include "vishing" – attacks by telephone and "smishing" those using SMS or text

ransomware

Type of software with malicious intent and a threat to harm your data

The author or distributor requires a ransom to undo the damage

No guarantee the ransom payment will work

Ransom often needs to be paid in cryptocurrency

hacking

Unauthorized access to systems and information

Website attack such as DDOS (distributed denial of service)

Access denied to authorized users

Stolen funds or intellectual property

environmental threats

Natural threats such as fire, earthquake, flood can cause harm to computers or disrupt business access

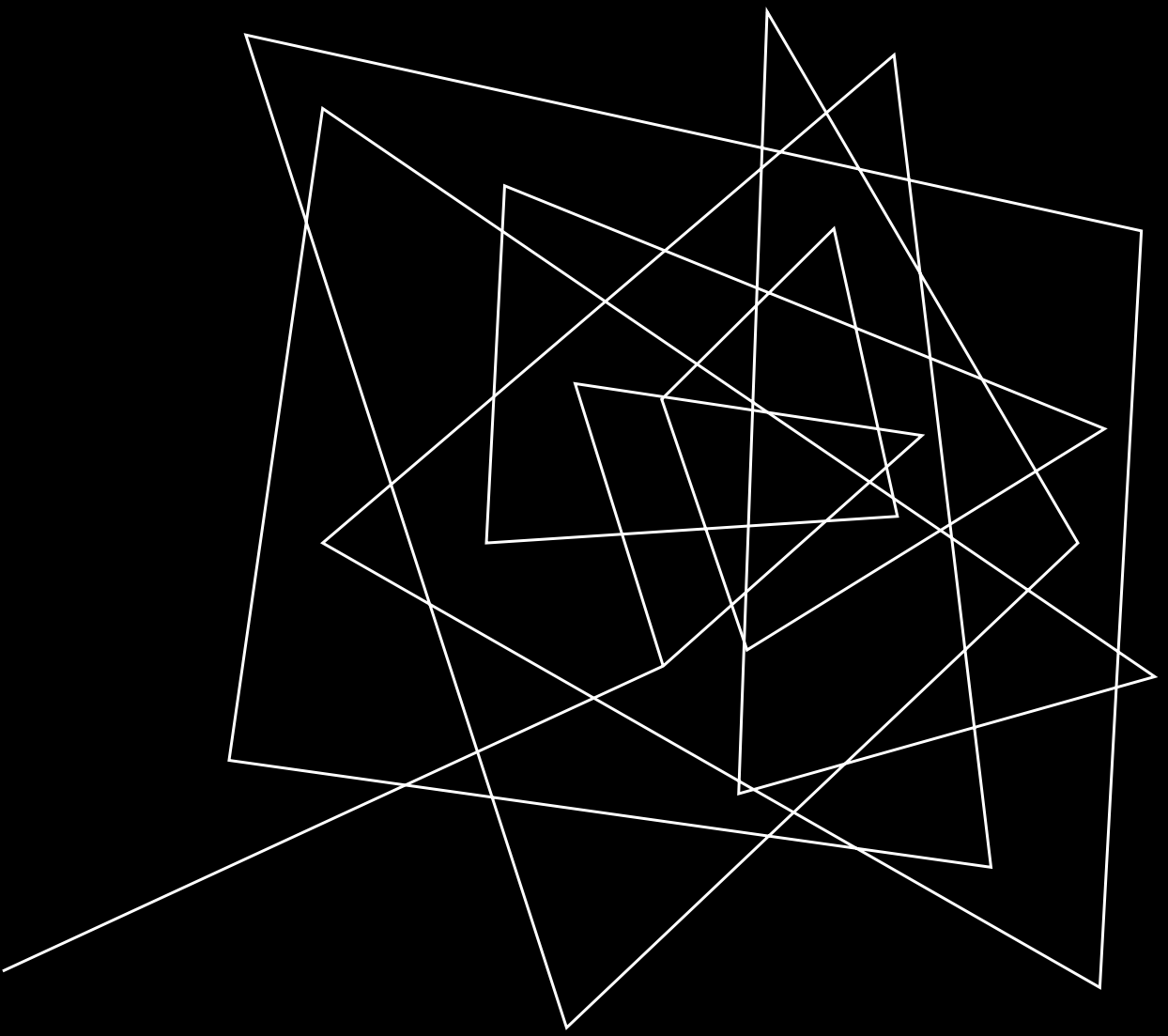
Recovery efforts attract scams such as financial fraud

Downtime can lose customers, clients who can't wait

SMALL ORGANIZATION, BIG IMPACT

why put your already limited resources into preparing for and protecting against cybersecurity attacks?

vulnerability	business costs	reputation
Attackers can see small organization as easy targets	Attacks can be extremely costly and threaten the viability of your organization	Residents and employees expect and trust you to keep their information secure



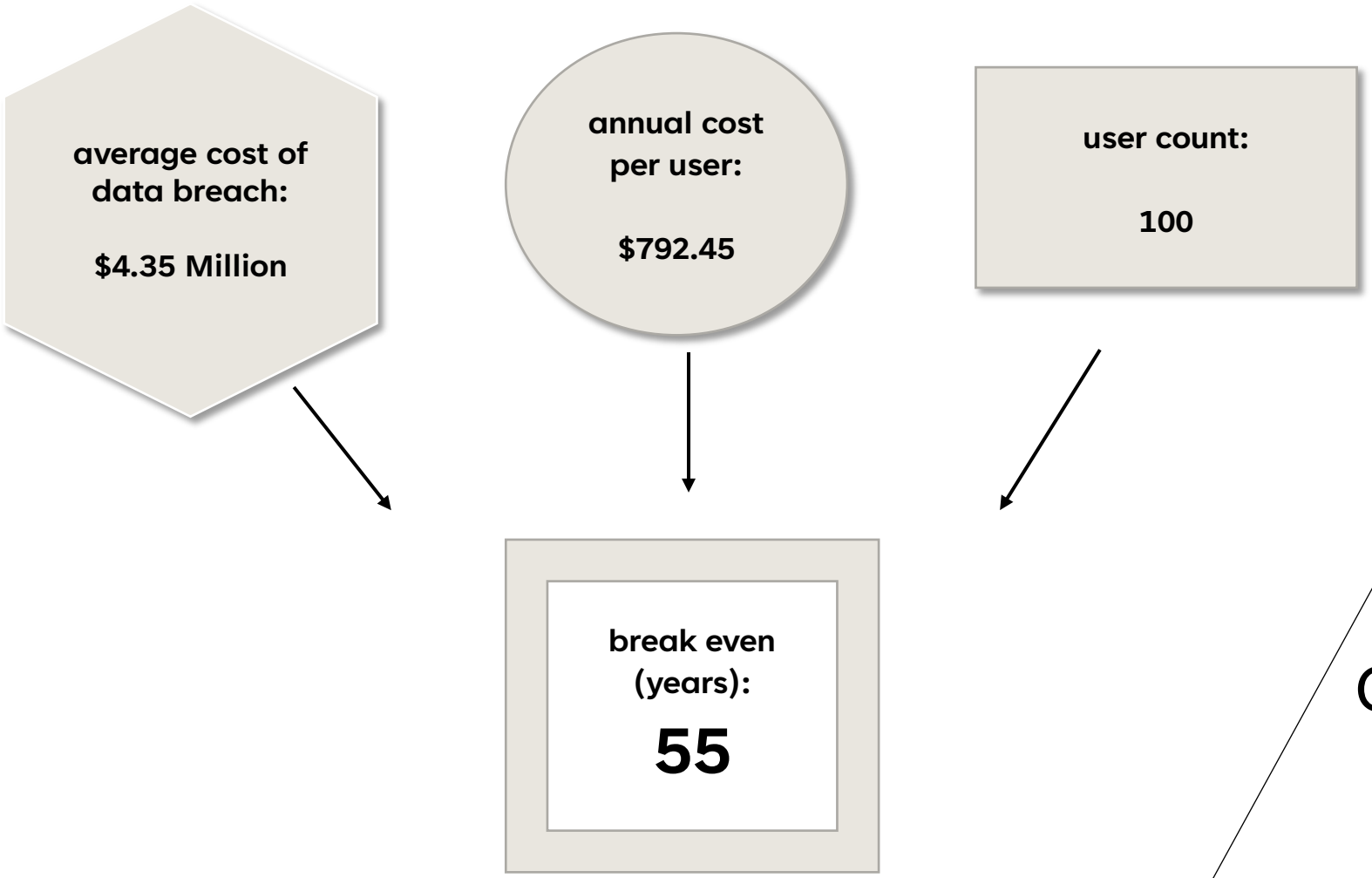
WE UPPED OUR SECURITY...UP YOURS!

CYBER MEASURES TAKEN AND COST PER PERSON

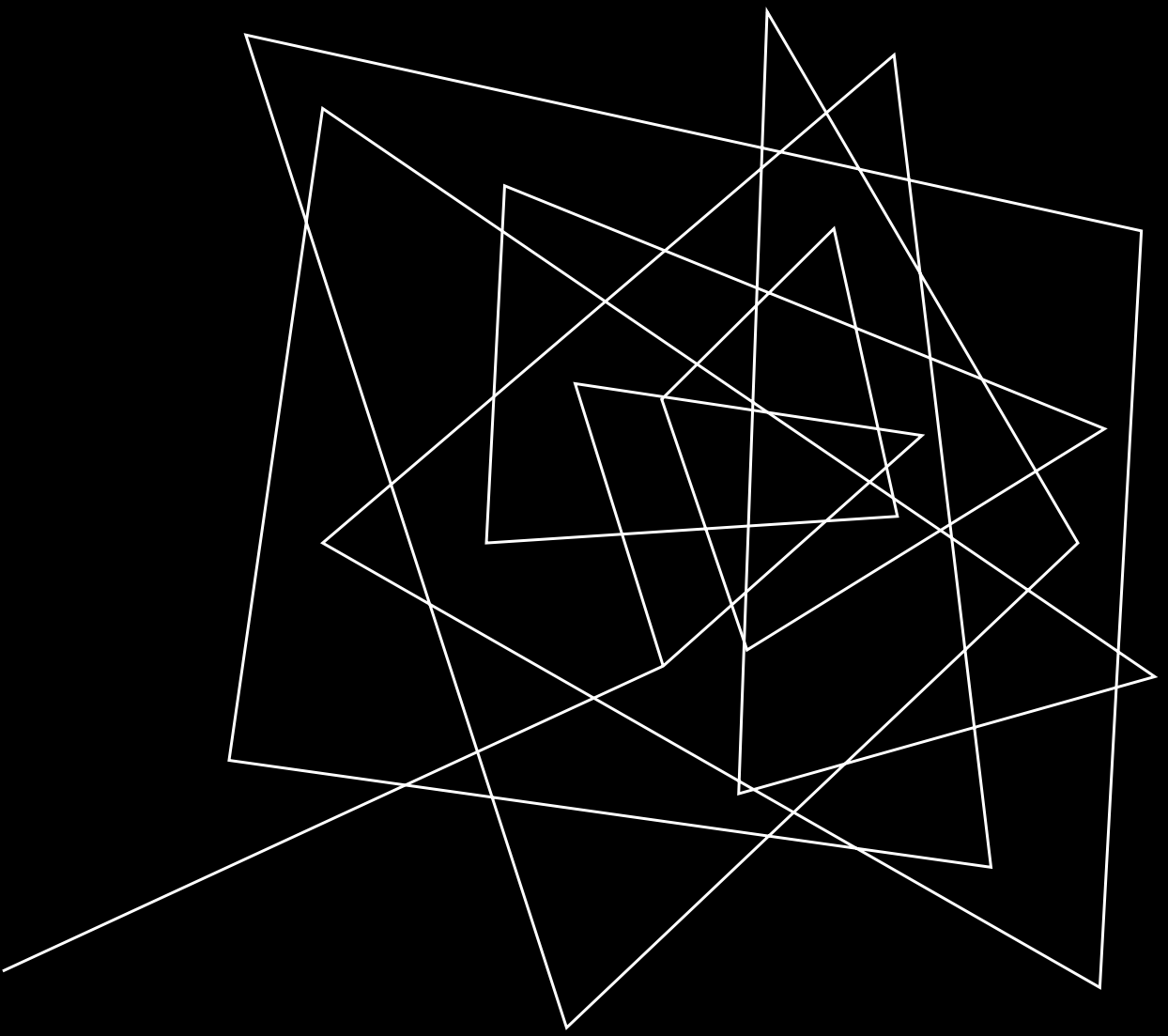
description	annual cost per user – msrp	annual cost per user – negotiated
microsoft applications & security tools	$538.46	$538.46
email filter & security training	$140.77	38.46
file/network scanning	$190.00	$61.54
firewall	$86.67	$45.38
anti-virus/policies	$47.44	$33.08
multifactor authentication	$55.00	$55.00
active directory auditing/management	$2.49	$2.07
network vulnerability scanning	$62.05	$18.46
annual cost per user	$1,122.88	$792.45
monthly cost per user	$93.57	$66.04

average discount = **29.4%**

ILLUSTRATION



Can your organization go 55 years without an incident?



INTERAGENCY SECURITY MODEL | CONSORTIUM

CHALLENGES AFFECTING LOCAL GOVERNMENTS

money

resources

competing priorities

PROBLEM STATEMENTS

economies of scale

What if we could leverage existing tool sets used in local government (and/or the State) and make them available to our partners so that they could enable capabilities they did not previously have due to costs, limited resources, and other general challenges?

achieve efficiencies

What if we could achieve economies of scale, reduce overall costs, maximize efficiencies, improve knowledge transfer, reduce duplication of work, and remove the haves and have-nots which has historically been one of the most significant challenges facing local governments.

enhance cybersecurity for all

How can we bring local governments and organizations above the cyber poverty line, so it protects everyone in the ecosystem?

GOAL:

To seed the creation of this community, it is imperative that the effort has broad support from key industry partners who are interested in securing their products, services, and data. Service providers are an integral resource as well.

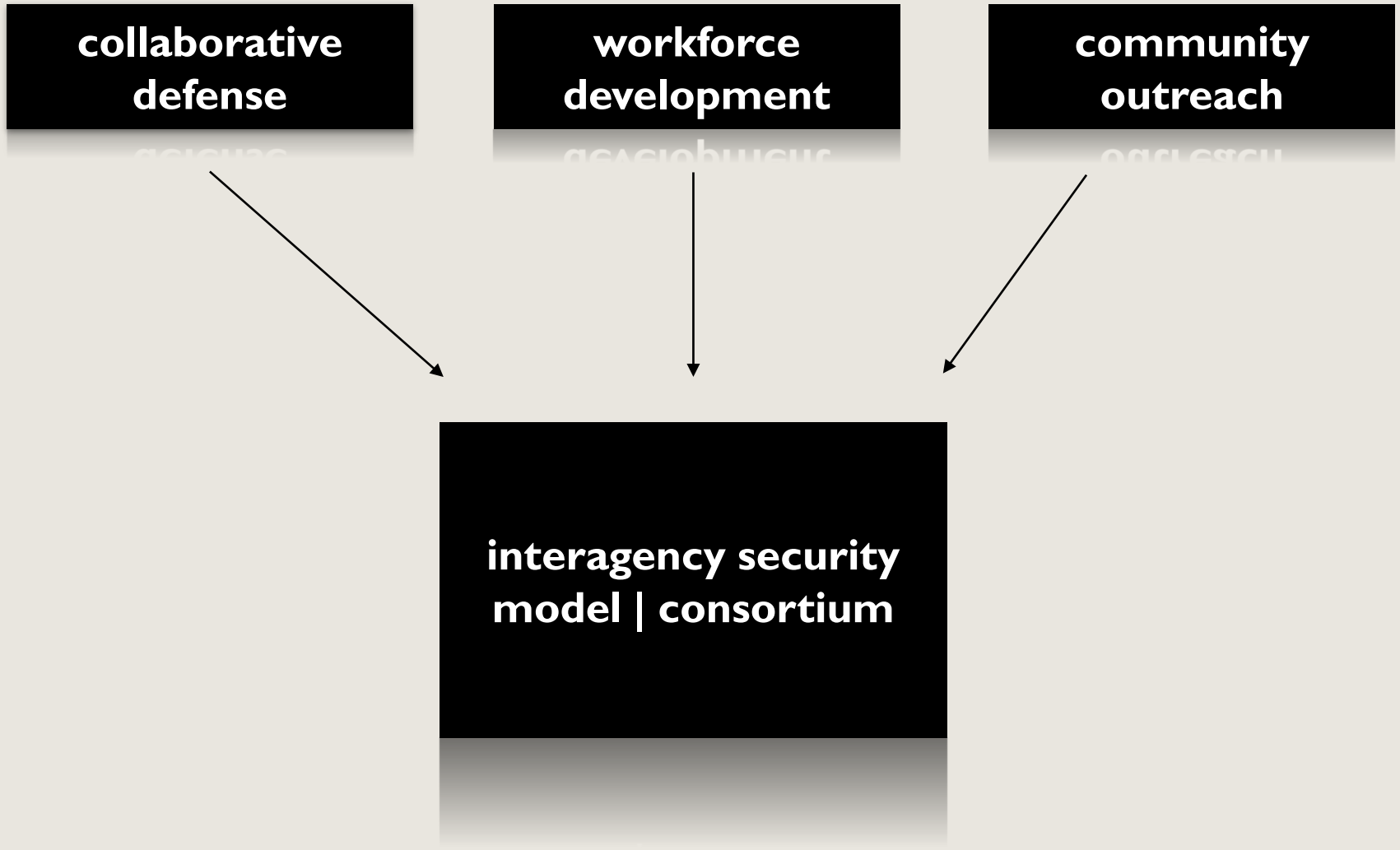
MISSION:

Build an active, trusted network of local governments and academia to enhance cybersecurity resilience and response, better protect digital and physical assets, create safer and stronger communities, and advance the technology leadership of southeastern Wisconsin and Wisconsin in general.

VISION:

- Reduction of overall costs through economies of scale
- Increase resilience and visibility
- Develop long-term strategy to prepare participating members for emerging and long-term cyber security challenges
- Maximized efficiencies and reduced duplication of work
- Increased knowledge sharing through engaging network of cybersecurity professionals
- Stimulate open innovation and impact throughout consortium

AVENUES


collaborative defense
workforce development
community outreach
interagency security model | consortium

COLLABORATIVE DEFENSE

Members share (in private community composed of vetted, trusted peers) practical cybersecurity defense information that can be put to immediate use. This includes best practices, proven methods and approaches, incident information, techniques/policies/procedures, indicators of compromise, etc. Due to diverse membership consisting of local government and academia, it will provide unique cross industry perspectives.

- Facilitate joint government contract pricing and/or grant applications among members on technology related to cyber defense
- Develop a secure web-based forum and resource library for members to collaborate on technologies, share best practices, and gather resources/information
- Host events focused on cybersecurity
- Develop and facilitate Executive Peer Forum for members

WORKFORCE DEVELOPMENT

Work across member organizations to build internal cybersecurity expertise and create local and regional employment opportunities. Due to academia being engaged with this effort, we will be able to create and support programs that expand the cybersecurity talent pool and help to create cyber-ready graduates to meet industry need.

- Establish and grow graduate level expertise in educational institutions within southeastern Wisconsin
- Facilitate a pipeline of adjunct instructors from industry to teach up-to-date technology/cybersecurity courses
- Recruit and/or establish private cyber training companies

COMMUNITY OUTREACH

Collaborate with a variety of partners to improve community and regional cybersecurity preparedness and response ensuring that cybersecurity is a business development priority within southeastern Wisconsin's economic growth strategy.

- Meet with state/federal representatives to educate them on our specific cyber challenges for our area
- Develop educational and best practices document for distribution to member's constituencies/customers
- Assist member executives in raising awareness of the realities and risks to their organizations regarding likely cyber-attacks

RETURN ON INVESTMENT

cybersecurity help now!

The near-term objective and work plan include immediate benefits in peer-to-peer communications and information sharing, workforce development, and education for the public and policymakers

- Increase visibility and access to more resources!

community investment

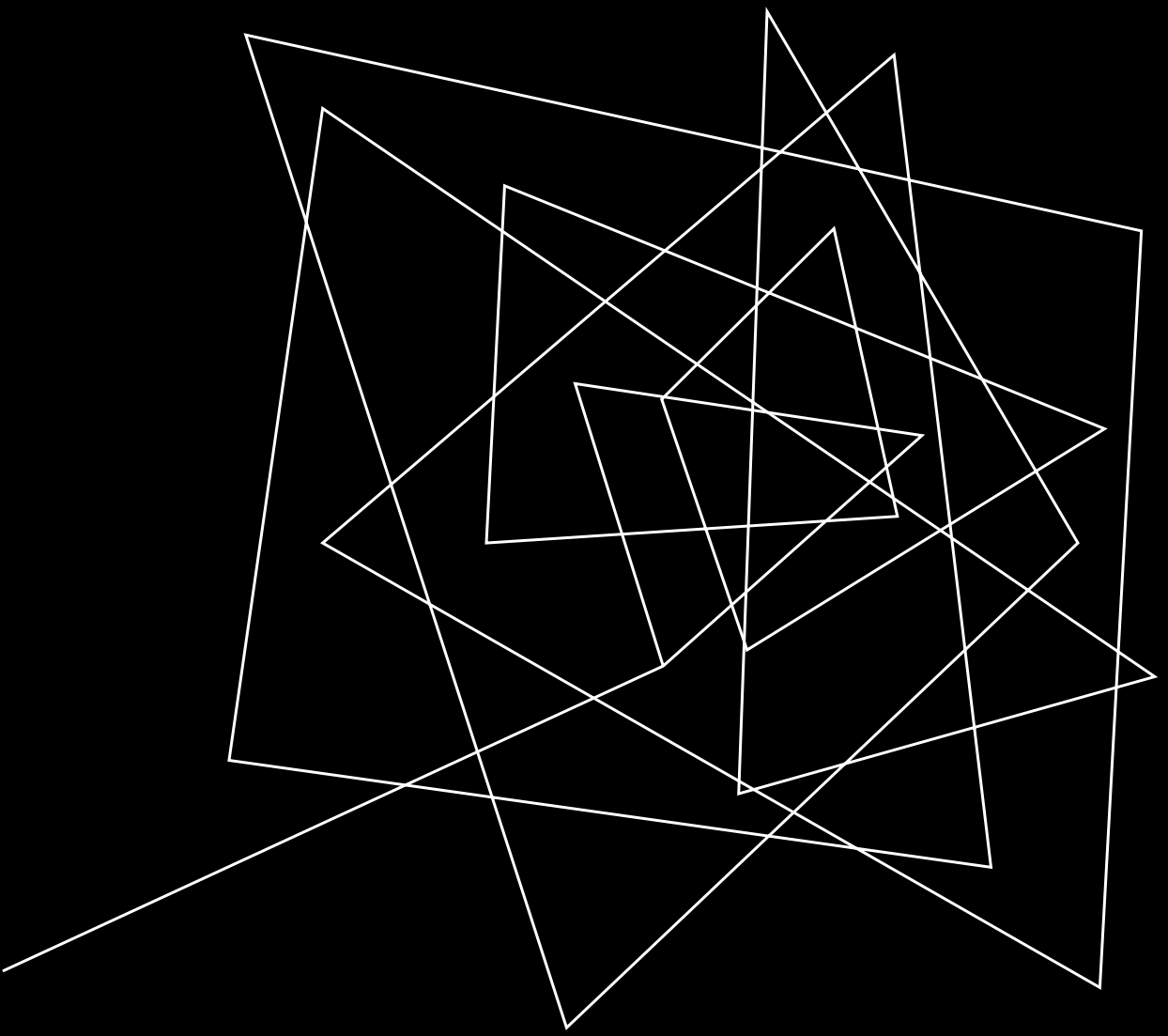
The cybersecurity challenge is a long-term war. Joining the consortium as a member strengthens the effort and strengthens your own individual efforts within your respective organizations

recruitment investment

A strong cyber ecosystem will consist of a strong pipeline of talented people. Developing the pipeline in your own backyard is a cost-effective recruitment strategy

HOW TO MEASURE SUCCESS

ESTABLISH FRAMEWORK	ESTABLISH METRICS	INCREASED PARTICIPATION	ECONOMIES OF SCALE
With establishing key principles, policies, tools it will result in better protection of digital assets and creation of stronger safer communities	With establishing key metrics (uptime, time to remediate, number of incidents) it will establish baseline measures, identify areas for improvement and promote ongoing learning	As more regional partner participate the consortium becomes a powerful network leveraging a wide range of expertise, resources, and perspectives	Through leveraging economies of scale through shared resources, tools and technologies the consortium reduces overall costs and more efficiently allocates resources towards cybersecurity for each partner



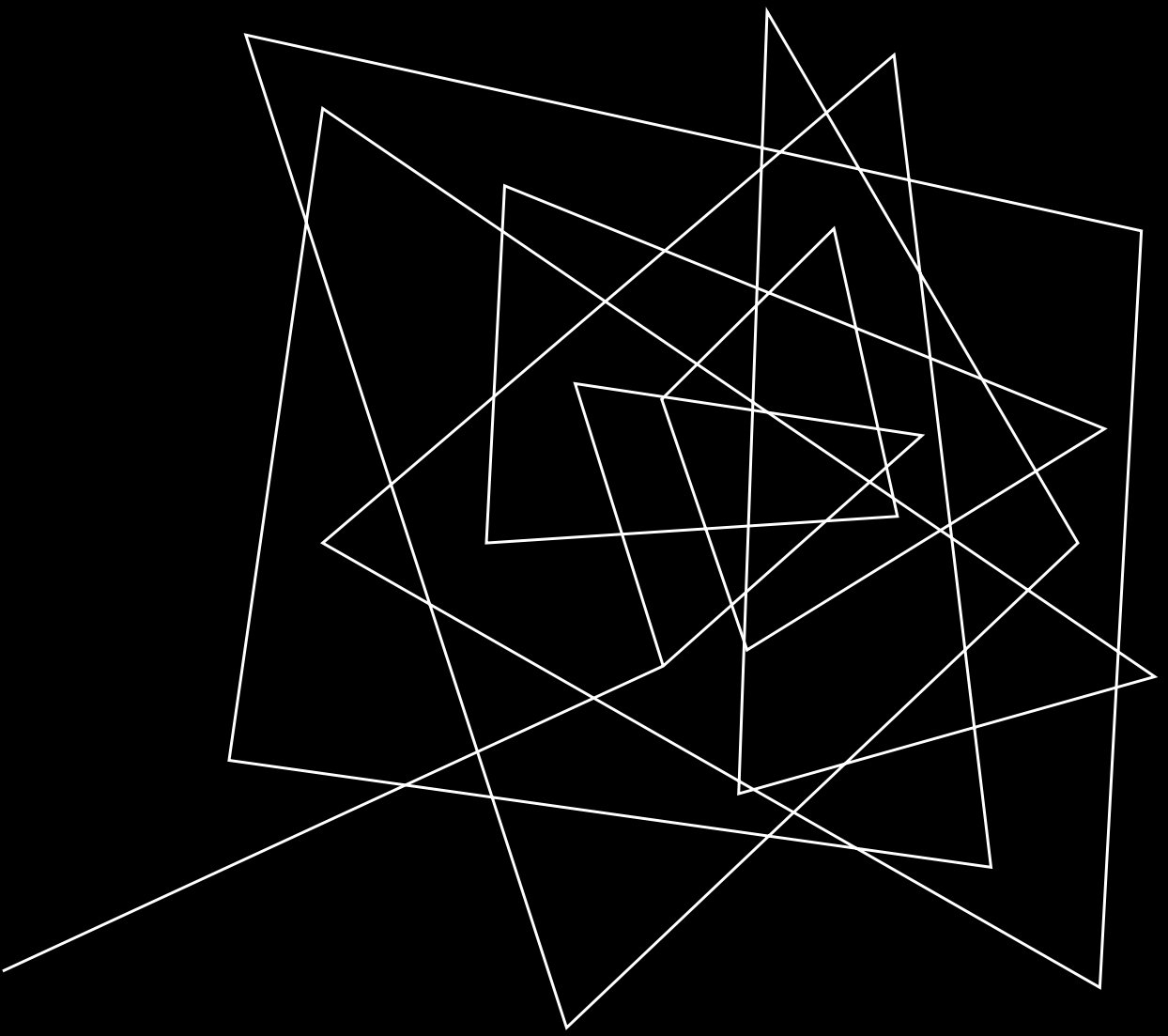
SUMMARY

KEY TAKE-AWAYS

Decreased costs due to economies of scale on complete services from ***segment leaders deploying high-tier package***

Enhanced cybersecurity for all, due to our ***duty*** to protect our own

Investment in community by building relationships and fostering workforce development



CALL TO ACTION

ESSENTIAL ELEMENTS TO BUILD A *"CULTURE OF CYBER READINESS"*

...ACTION FOR LEADERS...

Yourself	Your Staff	Your Systems	Your Surroundings	Your Data	Your Crisis Response
Lead Investment in basic cybersecurity Determine how much of your organization's ops are dependent on technology Build trusted network of relationships Approach cyber as a business risk	Develop a culture of awareness to encourage employees to make good choices online Learn about risks: phishing, business email compromise, etc Maintain awareness on current events	Learn what is on your network. Maintain inventories of hardware and software assets to know what is in play and at-risk from attack	Work in conjunction with your technology department to implement basic cyber measures (ie/MFA, policies and procedures, etc)	Learn how your data is protected	Lead development on: - Incident response/DR planning - Prioritization of resources and identification of critical systems that must be recovered first - Internal reporting structure to detect, communicate, and contain attacks Learn who to call for help (relationships matter!)

THANK YOU

Shuchi Wadhwa

Shuchi.Wadhwa@racinecounty.com