gocyber

COLLECTIVE

July Announcements

- Follow GoCyber Collective on LinkedIn and help grow the Collective
  - LinkedIn

- August 16th Proofpoint (Clay Gregord and Andy Boggess)
  - People-Centric Approach to Security
  - Security Awareness Training
  - Data Loss Prevention Technology

Special Interest Groups

- Special Interest Groups (SIGs)
  - Defense Industrial Base – Led by Dr. Thomas Autry
  - Local Government – Led by Darren Davey
  - Public Safety – Led by Gary Estes
- Public Safety
  - August 16th Patch Management Process

Event Sponsors

SECURECYBER
DEFENSE

July Speaker

Dr. Kevin Jackson

CEO, Level 6 Cybersecurity

“Artificial Intelligence-Driven Analytics for Cybersecurity Strategy Development”

Artificial Intelligence-Driven Analytics for Cybersecurity Strategy Development

Kevin E. Jackson, BSEE, MBA

AGENDA

- The Ever-Growing Challenge of Cybersecurity
- A Brief History of AI Applications to Cybersecurity
- Cyber Strategy: What is it, and Why Does Every Company Have One?
- Comparing Sources of Cyber Strategy
- The World-Wide Cybersecurity Lab and Business Poly-Intelligence
- Business Poly-Intelligence and AI Applied to Cyber Strategy Data

CYBERSECURITY IS A MULTIDIMENSIONAL CHALLENGE INVOLVING:

HUMAN FACTORS

- Security Culture
- Change Management
- Behavior Management
- Emotional Intelligence
- Communication
- Cyber Education
  & Awareness
- Cyber Branding

OPERATIONS FACTORS

- Business Process Alignment
- Compliance Management
- Policies and Procedures
- Cybersecurity Insurance
- Vendor Risk Management
- Audit & Review
- Business Continuity Planning
- Incident Response Planning
- Disaster Recovery Planning
- Audit and Review
- And more…

TECHNOLOGY FACTORS

- EDR / MDR / XDR Tools
- Vulnerability Management Tools
  IDS/IPS
- Wireless Security
- Cloud Security Services
- IAM solutions
- Perimeter Defense Tools
- Email and Spam Protection
- SIEM/SOC-as-a-Service
- Disaster Recovery/Backup solutions
  And more…

EXTRAORDINARY SECURITY COMPLEXITY

+

EXTREMELY MOTIVATED ATTACKERS

=

HORRIFIC BREACH STATISTICS

FURTHER CONTRIBUTING FACTORS

The Global Coronavirus Pandemic and Mass Work-from-Home Transitions.

The Explosive Growth of Anonymous Crypto-based Financial Markets.

Dramatic Advances in Computing Power Leveraging Cloud Capabilities.

TO SOLVE THE CYBER PUZZLE, MANY TECHNOLOGIES HAVE EMERGED

At the forefront we have Data Analytics and the related disciplines of Artificial Intelligence and Machine Learning. Artificial Intelligence & Machine Learning raise Data Analytics to performance levels human analysts can not achieve.

DATA ANALYTICS

Data analytics is the pursuit of extracting meaning from raw data using software. These systems transform, organize, and model the data to draw conclusions and identify patterns.

ARTIFICIAL INTELLIGENCE

Artificial intelligence leverages computers and machines to mimic the problem-solving and decision-making capabilities of the human mind.

MACHINE LEARNING

Machine learning is a subfield of artificial intelligence, which is broadly defined as the capability of a machine to imitate intelligent human behavior.

Informatica.com, IBM.com, MIT.edu

AI AND ML HAVE BROAD USAGE WITHIN MULTIPLE CYBER DOMAINS:

EMAIL PROTECTION

BREACH INVESTIGATION & FORENSICS

INTRUSION DETECTION & PREVENTION / THREAT HUNTING

VULNERABILITY MANAGEMENT

FRAUD DETECTION

SECURITY INFORMATION & EVENT MANAGEMENT / DATA CORRELATION

BEHAVIORAL ANALYTICS / INSIDER THREAT DETECTION

BUT NOTICE,

Each of these applications live within a specific cybersecurity DOMAIN.
As such, they are very TACTICAL in nature. Is there a STRATEGIC application for the power of AI?

CYBER STRATEGY:
WHAT IS IT, AND WHY EVERY ORGANIZATION HAS ONE

Cyber Strategies Seek to Manage the Complexity of Modern Information Security

Some see cyber strategies as:

- Information Security Mission and Vision Statements
- Comprehensive Lists of Objectives
- Detailed Long-term Project Plans
- Risk-based Programming and Initiative Creation

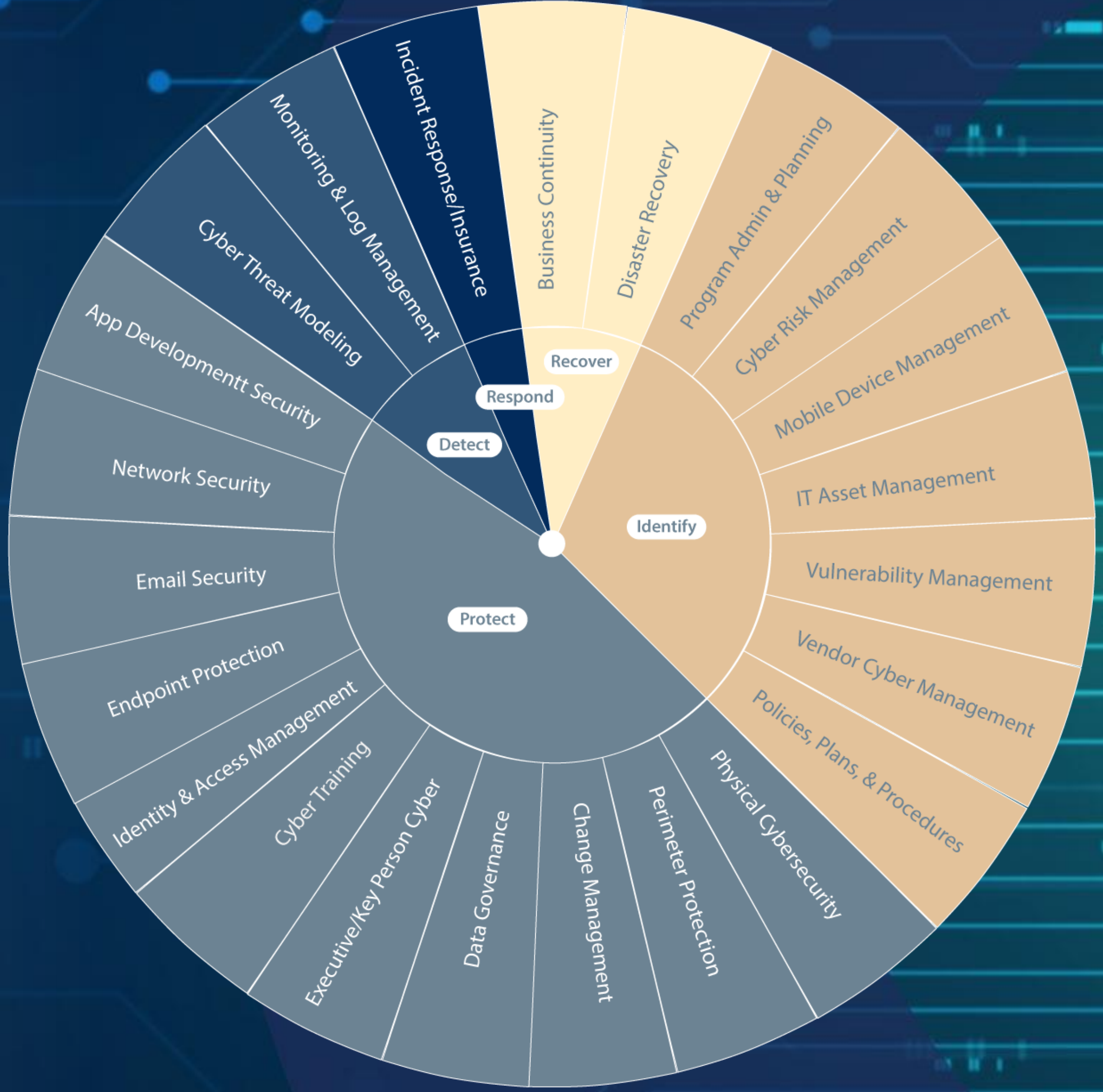
But there is another way to look at cyber strategy, a much more pragmatic way:

An organization's cyber strategy is the sum of all its information security decisions. Including affirmative decisions, omissions, gaps, and plans.

EVERY organization has a cybersecurity strategy! Even if it’s a very, very poor one.

Remember our cyber domains?

Someone in charge makes (or fails to make) organizational decisions in EVERY relevant category. For good or ill, those decisions define your organization’s cyber strategy!



Recover

Business Continuity

Disaster Recovery

Identify

Program Admin & Planning

Cyber Risk Management

Mobile Device Management

IT Asset Management

Vulnerability Management

Vendor Cyber Management

Policies, Plans, & Procedures

Protect

Physical Cybersecurity

Perimeter Protection

Change Management

Data Governance

Executive/Key Person Cyber

Cyber Training

Identity & Access Management

Endpoint Protection

Email Security

Network Security

App Developmentt Security

Detect

Cyber Threat Modeling

Monitoring & Log Management

Respond

Incident Response/Insurance

COMPARING SOURCES OF CYBER STRATEGY

Most companies get their cyber strategy information from anywhere and everywhere. Therefore, strategies (collections of decisions) vary widely.

STANDARDS	CONFERENCES	HEADLINES & ARTICLES	PROFESSIONAL COUNCILS	FRIENDLY ADVICE	TREND OF THE DAY
NIST, ISO, & CIS Are Good But Not Prescriptive	Big & Small. Great But Also Questionable	Right or Wrong? Fear-Mongering Coverage Leads to Panic	Experienced-Based But From Narrow Perspectives	They Probably Know What They're Doing?	Yikes

What is missing? *OUTCOMES*. Data-centric performance information. Not for tactics, but for strategy.

Wouldn’t it be GREAT if there was a way to base cyber decisions on what actually works best?

Not what has worked for some…

Not what’s trendy… but on results?

What if we had an enormous laboratory for testing cyber decisions. We could determine what actually results in fewer incidents and breaches, faster incident management, lower losses, faster recovery, and more!

THE WORLD-WIDE CYBERSECURITY LAB

Every organization with a domain name, an email address, or a connected computer is a testbed for cyber strategy.

Leadership makes (or fails to make) many critical security decisions… and outcomes (good and bad) naturally result.

What if we leveraged tools that *excel at processing massive amounts of data to determine correlations and make predictions?*

What if there was a way to base cyber decisions on the results from *real* cyber outcomes played out in *real* time?

What decisions *actually* result in fewer incidents and breaches, faster incident management, lower loses, faster recovery, and more?

The World-Wide Cybersecurity Lab and Business Poly-Intelligence

Cyber Strategies Seek to Manage the Complexity of Modern Information Security

- Some see cyber strategies as:
  - Information Security Mission and Vision Statements
  - Comprehensive Lists of Objectives
  - Detailed long-term project plans
  - Risk-based Programming and Initiative Creation
- But there is another way to look at cyber strategy, a much more pragmatic way:

An organization’s cyber strategy is the sum of all its information security decisions. Including affirmative decisions, omissions, gaps, and future plans.

If we can amass the World Wide Labs cyber strategy DATA, we can analyze it via business poly-intelligence!

THE GOALS:

Business Poly-Intelligence & AI Applied to Cyber Strategy Data

1

Gather massive amounts of Worldwide Lab data on cyber strategy.

(Decisions made on information security)

2

Gather resulting cyber outcome information from the same sources.

3

Perform business poly-intelligence analysis on the data to determine what *decisions* lead to the best *outcomes* based on the amassed data.

Business Poly-Intelligence & AI Applied to Cyber Strategy Data

How Do We Get There?

To analyze the Worldwide Lab's cyber strategy data, we need it in a consistent, repeatable format.

We must parameterize cyber decision-making and the results of cyber strategy research. In each cyber domain.

SOME EXAMPLES:

Business Poly-Intelligence & AI Applied to Cyber Strategy Data

Identity & Access Management

- Is strict RBAC enforced for all user access?
- Are exceptions allowed?
- Is a PAM tool in place within the organization?
- Is a formal IAM policy in place?
- Are temporary accounts automatically time-limited?
- How many times per year is Active Directory audited?
- Are password management tools mandated?
- How is MFA implemented?
- And so many more decisions…

Cybersecurity Training

- How many times per year is each end user required to complete general cyber awareness training?
- Is live training required? Are canned video trainings supported?
- Are separate training events held for privileged access users and/or executives?
- Is role-based cyber training in place?
- Is training completion strictly enforced?
- And so on…

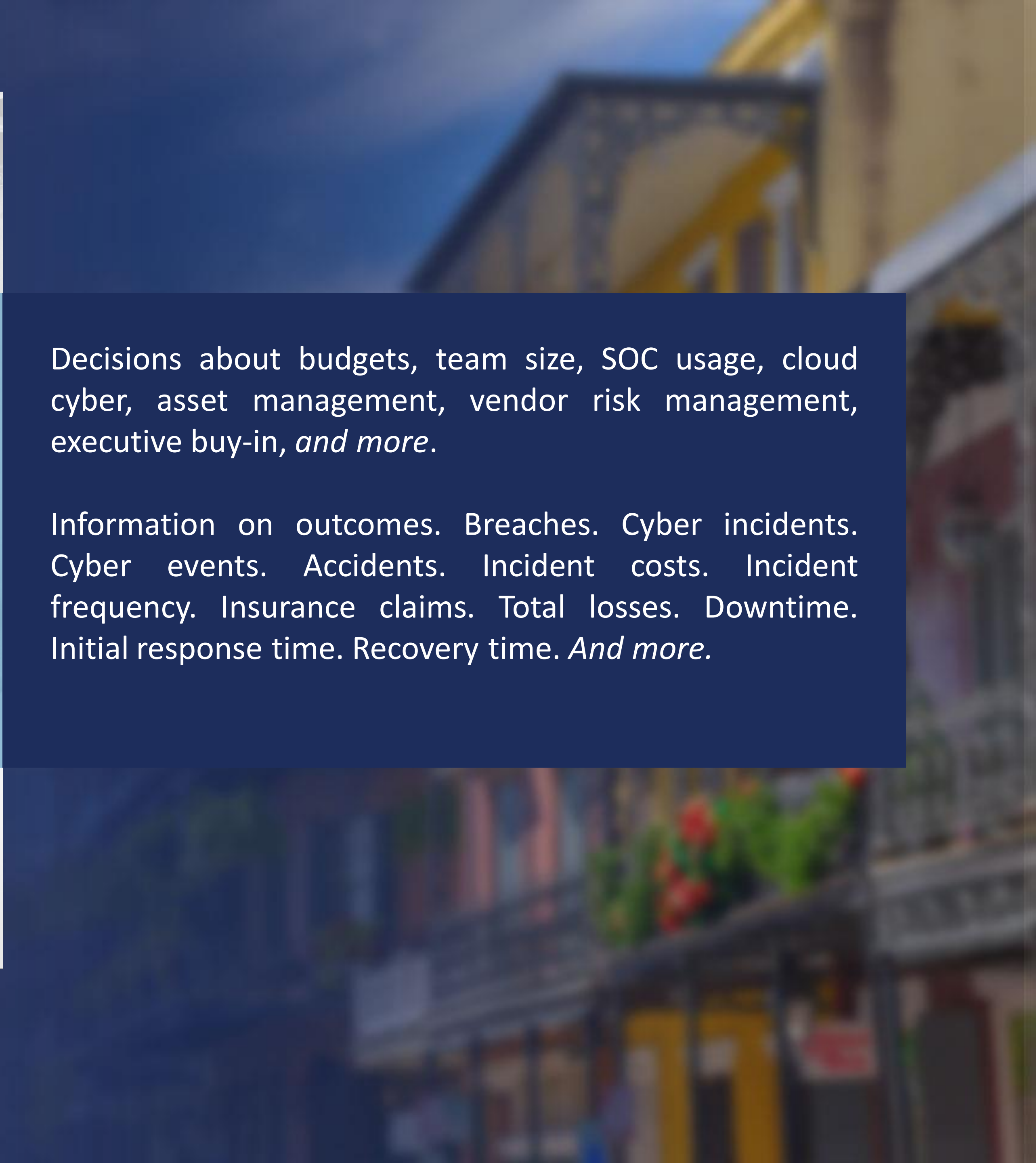
Incident Response

- Is a documented plan in place?
- Is an outside IR firm kept on retainer?
- Are all end users trained on the IR plan?
- How many times per year is the plan live tested?
- How many times per year is the plan tabletop tested?
- Are legal and insurance included in-the-loop during testing?
- Are IR, DR, and BC testing coordinated?
- And so many more decisions…

Endpoint Protection

- Is FDE enforced on all endpoints?
- Is EDR in use?
- Is a third-party organization managing and monitoring EDR operations or is it managed in-house?
- Is local admin granted to end users?
- Are local admin exceptions allowed?
- Are USB ports disabled?
- And on, and on…

AND EVEN MORE…



Decisions about budgets, team size, SOC usage, cloud cyber, asset management, vendor risk management, executive buy-in, *and more*.

Information on outcomes. Breaches. Cyber incidents. Cyber events. Accidents. Incident costs. Incident frequency. Insurance claims. Total losses. Downtime. Initial response time. Recovery time. *And more.*

Business Poly-Intelligence and AI Applied to Cyber Strategy Data

The power of AI can then be used to *gamify* our cyber strategy analyses. *Based on data from the Worldwide Lab of actual cyber experiences!*

Advanced Testing

What-If scenarios and testing of decision variables.

Specified Outcomes

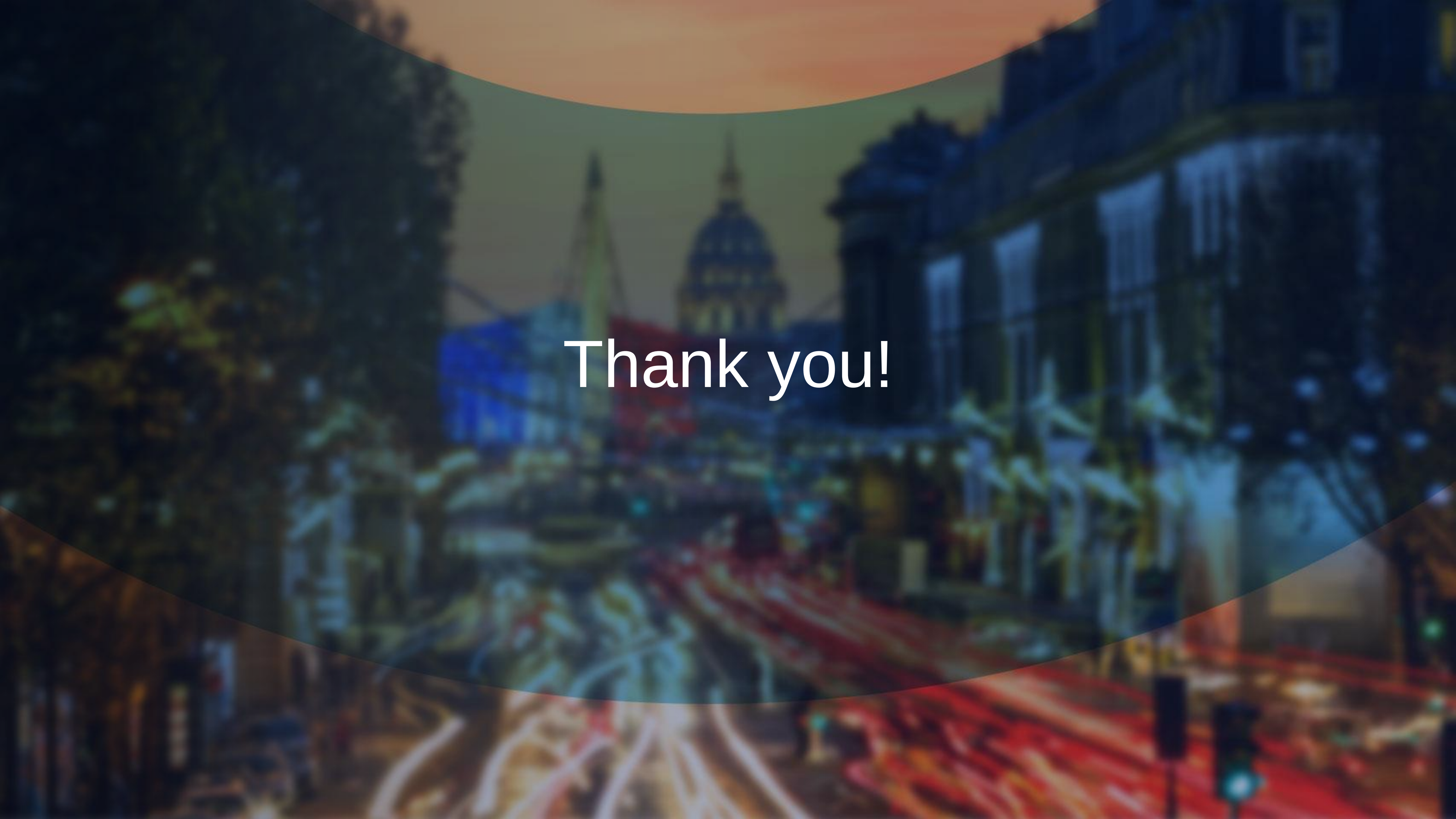
Reverse engineering of cyber decision sets based on a required set of outcomes.

Better Simulations

Full-scale, lifecycle simulations of cyber strategies and results.

Data-Based Roadmaps

Creation of cyber strategy roadmaps designed to achieve specific outcome goals.



Thank you!