Cyber-Security Resilience for Regional Economic Stability

Regional Economic Models, Inc.

May Lin, *Analyst*
Ian Spellane, *Economic Analyst Intern*

what does REMI say?℠

Agenda

- Introduction
- Resilience
- Economic Costs of Cyberattacks
- Critical Investments
- Live Model Demo & Notable Results
- Conclusion
- Q&A

About Us

We are the nation's leader in dynamic local, state and national policy modeling.

From the start, REMI has sought to improve public policy through economic modeling software that informs policies impacting our day-to-day lives.

We were founded in 1980 on a transformative idea: government decision-makers should test the economic effects of their policies before they're implemented.

At REMI, we're inspired by a single goal: *improving public policies*.

About Us

At REMI, we're inspired by a single goal: *improving public policies.*

Our models are built for any state, county, or combination of counties in the United States.

Our Representative Clients

Our model users and consulting clients use REMI software solutions
to perform rigorous economic analysis that critically influences policy.

UCONN
UNIVERSITY OF CONNECTICUT

Sandia National Laboratories

AARP

McKinsey & Company

North Carolina Department of Commerce

European Commission

UNIVERSITY OF MICHIGAN

EY

ITEP
INSTITUTE ON TAXATION AND ECONOMIC POLICY

nea
NATIONAL EDUCATION ASSOCIATION

what does REMI say? sm

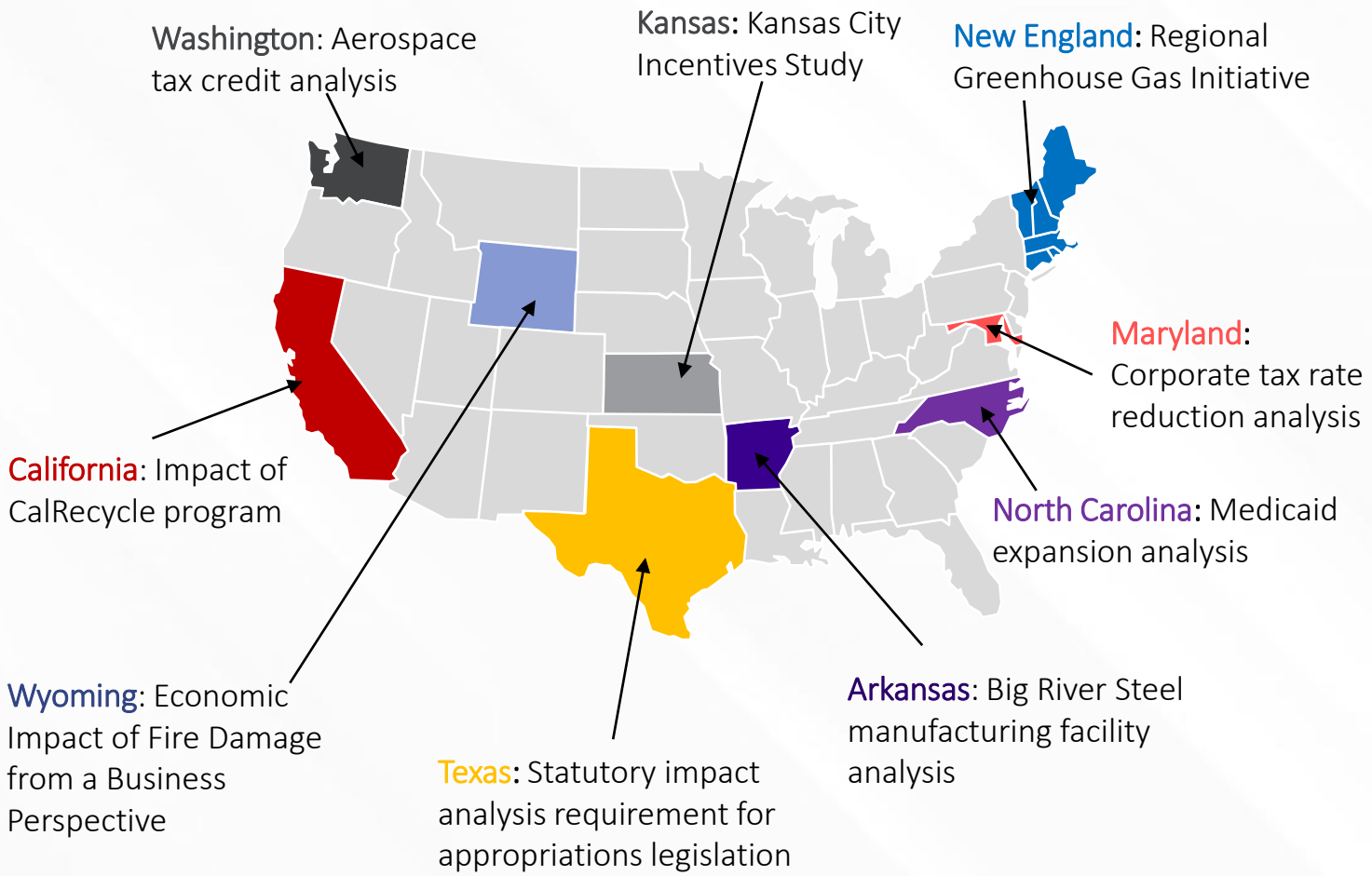
The REMI Model: Our Approach & Applications

Our Approach

You need a ***software solution*** that can clarify, calculate and communicate a ***quantitative narrative*** to policy makers and the general public about policies for your economy.

Rigorous Economic Analysis

- Since 1980
- Peer Reviewed
- Multiple Reputable Data Sources
- Public Equations



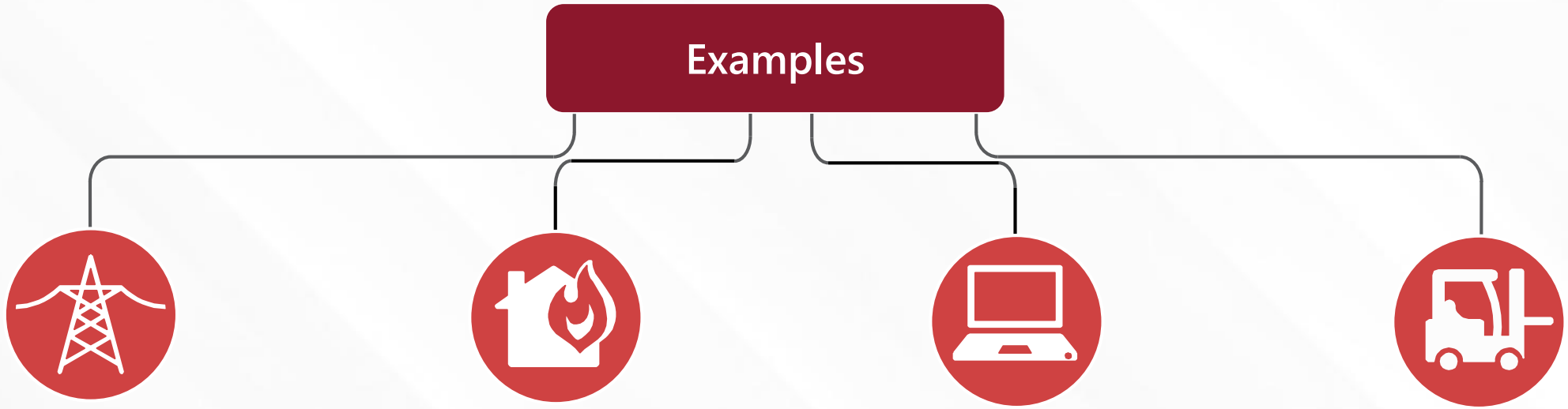
what does REMI say? sm

Agenda

- Introduction
- **Resilience**
- Economic Costs of Cyberattacks
- Critical Investments
- Live Model Demo & Notable Results
- Conclusion
- Q&A

Defining Resilience

Resilience: the ability to recover from or adjust quickly to a change in circumstances



Infrastructure failures

Power outage, bridge collapse

Natural Disasters

Flood, wildfire, earthquake

Cyber-Attack

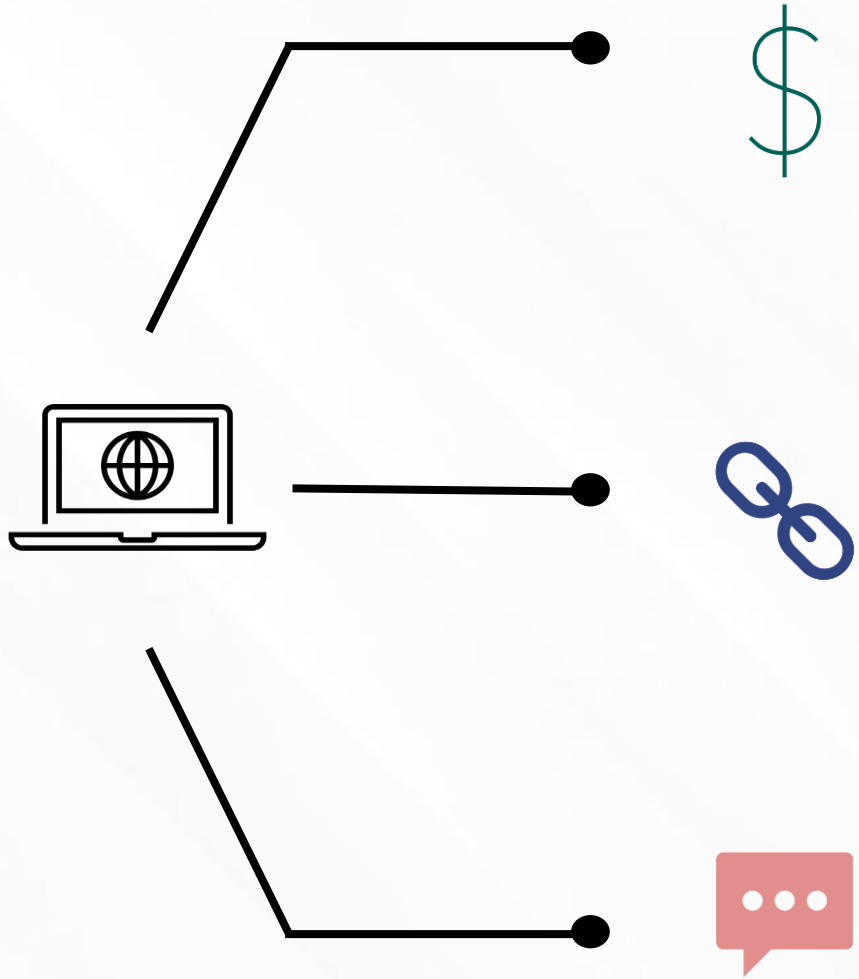
Malware, phishing

Recessions / Industry shifts

Loss of manufacturing jobs

Issues Related to Resilience

Cybersecurity Resilience



Upfront Costs
Resilience requires significant upfront costs, and the benefits are not always clear

Weakest Link
Agents will always target the least defended element

Ransom Incentives
Paying ransom sends the message that there is money to be made in hacking, negative externality

Critical Industries

Finance and insurance

Manufacturing

Energy

Retail

Frequency of attacks	Relative exposure	Public Threat
		

Agenda

- Introduction
- Resilience
- **Economic Costs of Cyberattacks**
- Critical Investments
- Live Model Demo & Notable Results
- Conclusion
- Q&A

Types of Cyberattacks

Variety of Cyberattacks

Perpetrators

- Nations
- Corporate competitors
- Organized criminal groups
- Company insiders
- Hacktivists

Cost Component

- Loss of IP
- Loss of revenue
- Increased cost of capital
- Settlements
- Reputational damage

Economic Cost of Cyberattacks

Exposure

- Common consensus that America is under resourced in cybersecurity

Investment

- Cybersecurity requires a significant upfront investment
- Mitigated losses are a massive ROI

Modeling & Planning

- Economic modeling is a useful tool to determine an efficient amount of investment in cybersecurity

Agenda

- Introduction
- Resilience
- Economic Costs of Cyberattacks
- **Critical Investments**
- Live Model Demo & Notable Results
- Conclusion
- Q&A

Winning the Fight Against Cybercrime

- Cybersecurity and cybercrime grow and build off each other in a never-ending cycle, driving a need for increased investment alongside them.

- *The Cybersecurity Technology Cycle:*

Critical Investments

- Critical industries

Finance and insurance

Manufacturing

Energy

Retail

- Case: regional economy hit by cyber attacks
  - Which industries should be prioritized for protection?
  - What is the proper amount of investment in cybersecurity?
  - What are economic impacts?

Modeling Resilience

- Efficiency vs Resilience

- It is critical to be aware of the potential results of cyber hacking, and REMI models would be a way to quantify that risk and figure out how to gauge the proper amount of investment in cybersecurity.
  - Economic modeling quantifies the value of creating and implementing resilient systems
  - Making the case to invest in resilience

- Policy makers can be proactive when establishing policies to promote resilience at the local, state, and regional levels

- Resilience modeling informs and alerts decision-makers of the potential dangers of a non-resilient system

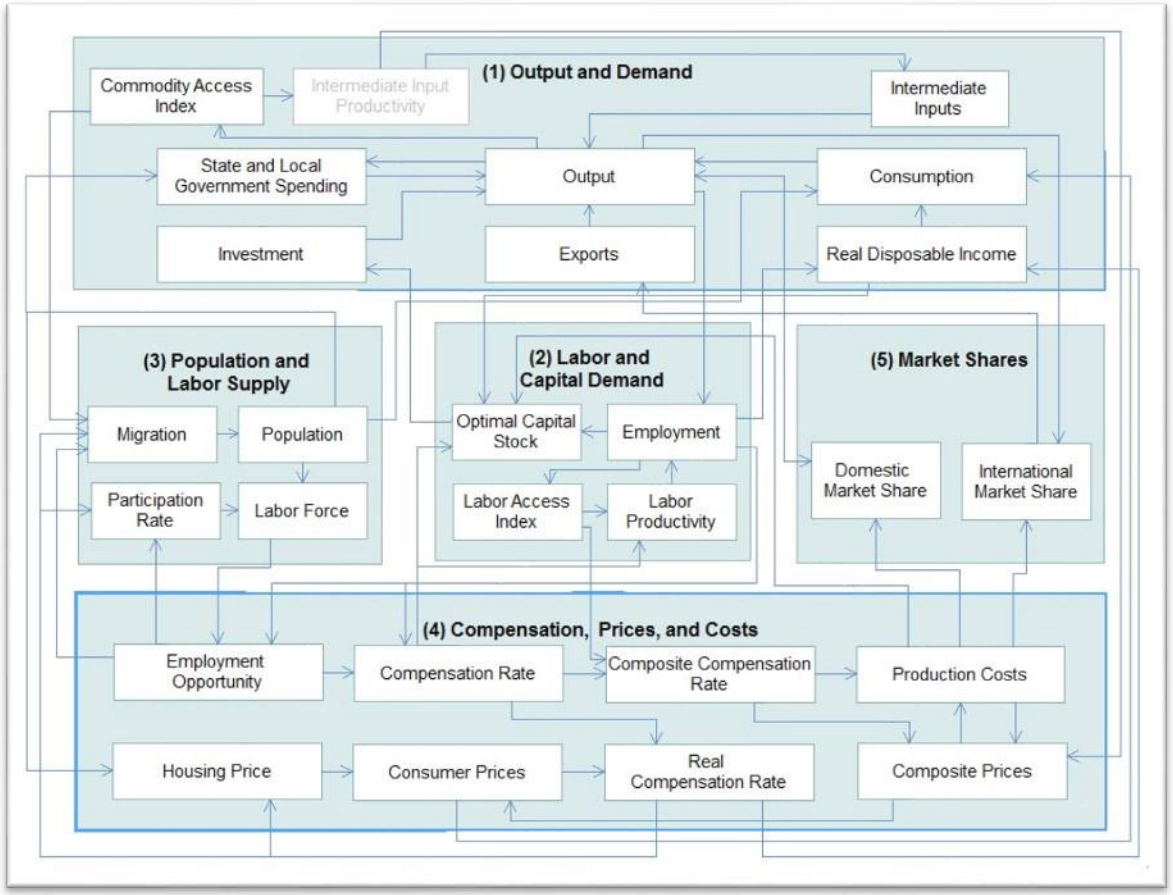
Agenda

- Introduction
- Resilience
- Economic Costs of Cyberattacks
- Critical Investments
- **Live Model Demo & Notable Results**
- Conclusion
- Q&A

Model Simulation: REMI E3+

E3+ is the premier software solution for analyzing the macroeconomic and demographic impacts of any initiatives related to the energy and environmental sectors.

Decision-makers depend on E3+ to provide comprehensive evaluations of the total economic impact of altering electric rates, introducing new power sources, investing in the production of energy, and other policy changes.



what does REMI say?sm

Measuring Resilience with E3+

- Disaster Resilience Study
  - Tool for evaluating the effectiveness of multiple disaster recovery and mitigation plans
  - E3+ can produce an automatic calculation discussing resilience through a forecast's "Resiliency Report"

- Concept: Cyber-attack shock with versus without resilient system
  - No-Action Baseline Control: Direct shock impact from cyber-attacks
  - Resilience Investment Scenario: Cushion from resilient system

- The model produces a Resilience Loss Reduction Potential figure:

$$RLRP = \frac{Avoided\ Losses}{Maximum\ Potential\ Losses}$$

Modeling Methodology

Cyber-Attack Loss in Far West

- **Control forecast:** $700 million downward revision in baseline Output for 2021-2022

Cyber-Attack Loss in Southwest

- **Control forecast:** $600 million downward revision in baseline Output for 2021-2022

Invest in Financial Sector

- **Resilient forecast:** $100 M Upward increase in simulation Output of Finance and Insurance for 2021-2022

Invest in Financial Sector

- **Resilient forecast:** $100 M Upward increase in simulation Output of Finance and Insurance for 2021-2022

Invest in Manufacturing Sector

- **Resilient forecast:** $100 M Upward increase in simulation Output of Manufacturing for 2021-2022

Invest in Manufacturing Sector

- **Resilient forecast:** $100 M Upward increase in simulation Output of Manufacturing for 2021-2022

Modeling Results

Cyber-Attack Loss in Far West

- Total Maximum Loss Potential: $2.9 Billion

Cyber-Attack Loss in Southwest

- Total Maximum Loss Potential: $3.2 Billion

Invest in Financial Sector

- Avoided Loss: $0.413 Billion
- Resilience Loss Reduction Potential: **14.17%**

Invest in Financial Sector

- Avoided Loss: $0.490 Billion
- Resilience Loss Reduction Potential: **15.54%**

Invest in Manufacturing Sector

- Avoided Loss: $0.481 Billion
- Resilience Loss Reduction Potential: **16.49%**

Invest in Manufacturing Sector

- Avoided Loss: $0.594 Billion
- Resilience Loss Reduction Potential: **18.83%**

Agenda

- Introduction
- Resilience
- Economic Costs of Cyberattacks
- Critical Investments
- Live Model Demo & Notable Results
- **Conclusion**
- Q&A

Conclusions and Notable Results

Cyberattacks Pose a Significant Threat

- Growing threat with ripple effects through the economy

Investment Can Mitigate the Losses

- Millions of dollars in initial upfront cost
- Potentially billions in avoided losses

Economic Modeling

- Robust modeling is a key step in effectively planning cybersecurity infrastructure
- Forecasting can generate accurate scenarios

Resource Allocation

- Size, scope, and location of cybersecurity infrastructure should be tailored to the threat risks

Economic Modeling: Why does it matter?

Clarify

- Understand economic, fiscal and demographic implications of policies before implementation
- Ensure that public policy serves the broad-based interests of the public

Predict

- Make predictions about the effects of policies before implementation
- Avoid unwanted negative impacts
- Make effective use of resources

Inform

- Inform policy with standard metrics rather than ideology or intention
- Address stakeholders with evidence that communicates how policy benefits or disadvantages their communities broadly

Thank you for attending!

For more information, please contact
info@remi.com

Citations

The Cost of Malicious Cyber Activity to the U.S. Economy. The Council on Economic Affairs, February 2018. Available at https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf.

Critical Infrastructure Protection. Government Accountability Office, September 2020. Available at https://www.gao.gov/assets/gao-20-631.pdf.

Wallach, Sponsored Content Article/Editing: Omri. "Investing in Core Cybersecurity Technology." *Visual Capitalist*, 20 July 2021, www.visualcapitalist.com/investing-in-core-cybersecurity-technology/.