# The Battle for New York:

## A Case Study of Applied Digital Threat Modeling at the Enterprise Level

**Rock Stevens**, Daniel Votipka, Elissa Redmiles, Michelle Mazurek | University of Maryland

Patrick Sweeney | Wake Forest University

Colin Ahern | New York City Cyber Command

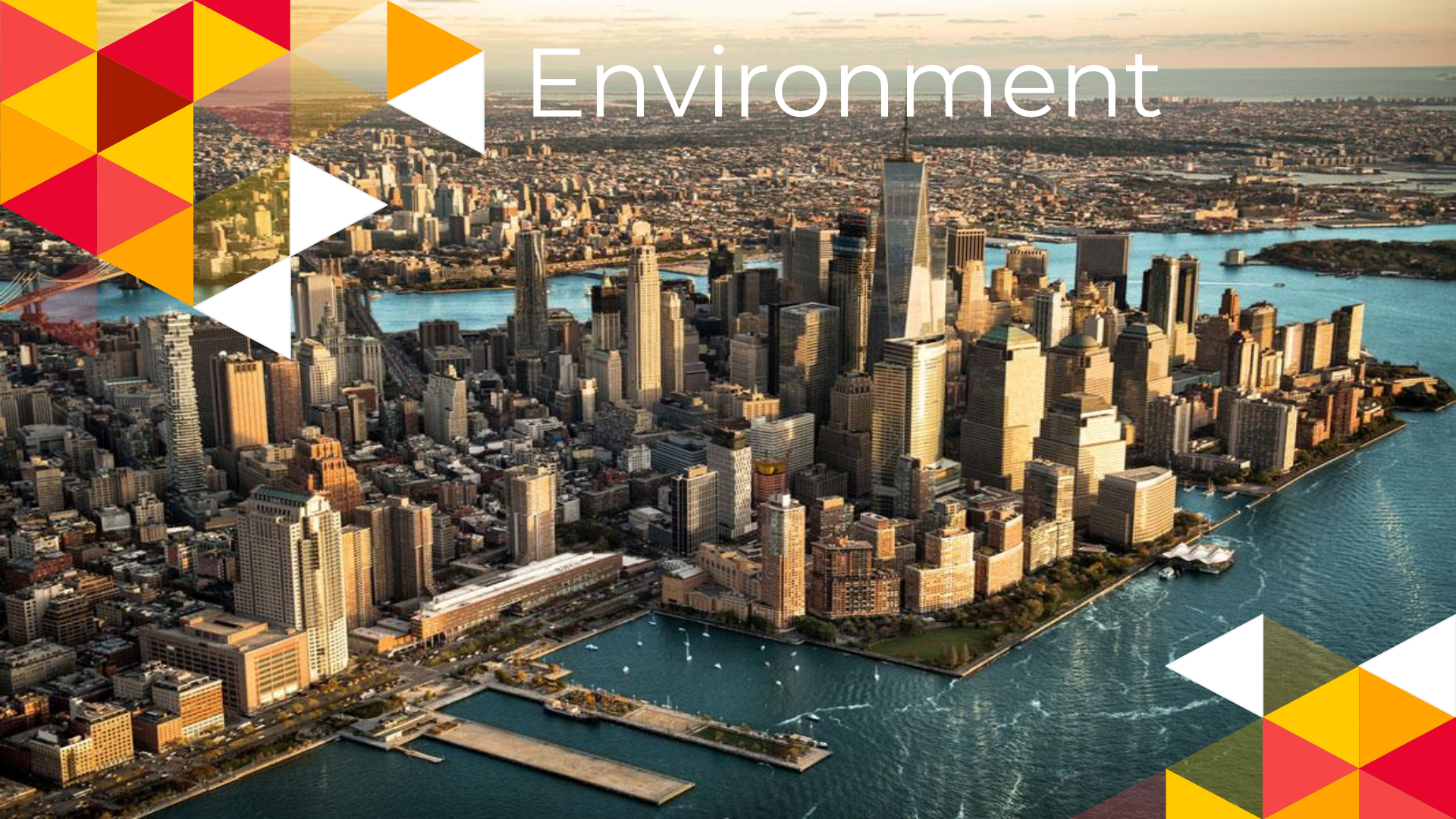
# Threat Modeling

- What is it?
- Why do it?
- Where's the proof?

# Threat Modeling

This study is the **first** empirical evaluation of a digital threat modeling framework at the enterprise level

# Environment



# Study Methods


Six-part process over the span of 120 days

# Baseline Survey

# 1-hour Educational Intervention

# Center of Gravity

Actionable Defense Plan

# Center of Gravity

## Center of Gravity Worksheet

| | |
|---|---|
| Please state your work section's objective/mission:<br>1<br>What assets are used to accomplish this mission?<br>2<br>What is your center of gravity?<br>3 | **Critical Capabilities**<br>4 |
| **Critical Requirements**<br>5 | **Critical Vulnerabilities**<br>6 |
| **Threat Capabilities**<br>7 | **Threat Requirements**<br>8 |
| **Defense Plan**<br>9 | |

# 1-on-1 TMF Application Session

# Immediate Post-training Survey

# Export Output for Validation

# 30-Day Follow-up Survey

# 120-day Analysis of Logs

# Perceived Efficacy
# Accuracy
# Actual Adoption
# Actual Efficacy

# Perceived Efficacy

What did participants think about the threat modeling framework?

# Accuracy

Did participants produce relevant mitigating strategies?

# Actual Adoption

What remained with the organization beyond initial training?

# Actual Efficacy

What impact did changes have on the enterprise?

# Results

# Baseline

- 25 participants (37% of workforce)
- Commercial services
- Compliance standards
- Industry best practices

# Perceived Efficacy

- 12/25 identified new aspects never before considered
- More confident in their abilities
- Empowered to communicate

*“Plan effectively, document, track, monitor progress, and essentially understand our security posture”*

# Accuracy

- 96% ADP accuracy
- 147 unique mitigation strategies (64% new)
- 16/25 ADPs ready for immediate implementation

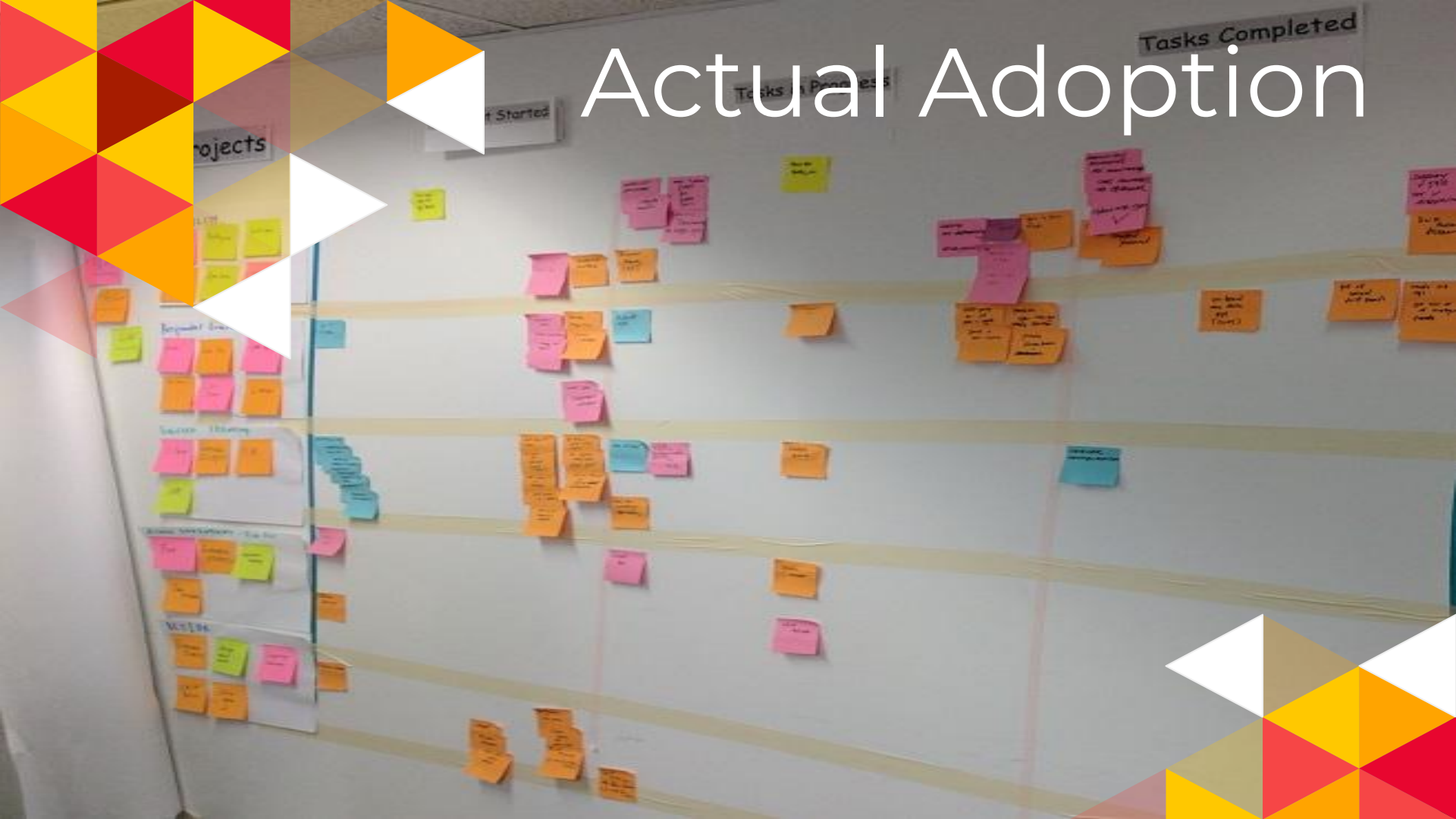
# Accuracy

- No work role, amount of education, IT experience, or combination thereof enjoyed a statistically significant advantage

# Actual Adoption

- Securing accounts
- Crowdsourcing assessments
- Improving sensor coverage
- Reducing human error

# Actual Adoption



# Actual Efficacy

- **Securing accounts**
- Crowdsourcing assessments
- Improving sensor coverage
- Reducing human error

Blocked account hijackings of five privileged user accounts

# Actual Efficacy

- Securing accounts
- **Crowdsourcing assessments**
- Improving sensor coverage
- Reducing human error

Discovered and remedied three vulnerabilities in public-facing web servers

# Actual Efficacy

- Securing accounts
- Crowdsourcing assessments
- **Improving sensor coverage**
- Reducing human error

Blocked 541 unique intrusion attempts

# Limitations

- No TMF comparison
- Demand characteristics
- Representative environment?

# Summary

- <2-hr training made an immediate impact without additional costs
- Identified 147 unique mitigation strategies
- Quantitatively improved security over 120 days
- Useful for empowering and communicating

> Questions / Feedback? rstevens@cs.umd.edu | @ada95ftw