

RSAConference2022

San Francisco & Digital | June 6 – 9

SESSION ID: AIR-T02

Cyber Range on a Budget (For Any Organization)

Rick Trilling

Professor of Cybersecurity Management
Wentworth Institute of Technology, Boston

TRANSFORM



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

©2022 RSA Conference LLC or its affiliates. The RSA Conference logo and other trademarks are proprietary. All rights reserved.

RSA®Conference2022

INTRODUCTION

Why “Cyber Ranges”?



Cyber Range on a Budget (for any organization)



Cyber Range on a Budget (for any organization)

- Cyber Ranges (CRs) prepare individuals to deal with cyber incidents
- CRs can be expensive to build & operate (or lease)
 - shared CRs offer limited access
- Instead, we need *DIY* (Do-It-Yourself) CRs that can be set up easily at little or no expense
- Almost any organization can accomplish this, even with limited time, money or other resources

Cyber Range on a Budget (for any organization)

How Easy is All of This to Apply to *Your* Real-World Organization?

I will show you how this has actually been done in various organizations

You will view that “how” through the lens of your own particular organization

Whatever questions arise, remember, professors love to answer questions: ask!

...then you can take this back and promptly/easily test it in your own organization!

RSA®Conference2022

PHYSICAL ASSETS

Repurpose, Reuse, and Return



Cyber Range on a Budget (for any organization)

General concept of a low-resource DIY CR involves temporarily repurposing existing resources which, in-between such usages, can be returned to regular functions

- 1) instead of dedicated space, use existing conference rooms, classrooms, or similar spaces
- 2) instead of dedicated computers, use employees / students existing laptops
- 3) instead of dedicated display technology, use either the room's existing fixtures (like wall mounted TV monitors/projectors) or rolling stock (like tv monitors on wheels / portable projectors)

Cyber Range on a Budget (for any organization)



Cyber Range on a Budget (for any organization)

- 4) instead of dedicated servers with high-power computing capacity, rely upon existing medium-power desktop
- 5) instead of a dedicated intranet network, use the Internet, or (if available) an alternative intranet
- 6) instead of customized scenario content, create home-grown content or share / trade with other DIY CRs

These are all used *only* during a CR exercise
and then returned to regular usage afterwards

Cyber Range on a Budget (for any organization)



RSA®Conference2022

CYBER INCIDENT SCENARIO CONTENT

You Don't Need to Make This Stuff Up



Cyber Range on a Budget (for any organization)

Making lemonade out of lemons:

There is a seemingly unending supply of real-world breaches and attacks in the news almost every day

- As wide-ranging examples for us to use
 - various types of “bad actors”
 - using various methods
 - against various targets / sectors
 - as well as responses by those targets
 - and typical results of those responses
- Simply adapting these real examples yields a variety of scenario content, reducing the effort required to generate such scenarios

Cyber Range on a Budget (for any organization)

Instead of movie-quality visualization of such scenarios (using professional actors, expensive scripts, high-quality cameras, etc.)



such scenarios can be initially rendered simply through PowerPoint slide shows containing decision trees that follow various alternative results (MS software that is available in most organizations)

Cyber Range on a Budget (for any organization)

Why “reinvent the wheel”?

- Sharing such scenario content, as DIY CRs increasingly proliferate, allows organizations to share and trade scenarios (in various formats, including PowerPoints, videos, VR, etc.) amongst themselves
- One or more central exchanges / clearing houses as trading hubs
- Eventually traditional paper & videogame publishers could assess this new / growing market and create scenarios for sale at affordable prices

RSA[®]Conference2022

SUMMARY

**Repurposed Resources + Real-World Content =
High Value Cyber Ranges for Low Cost**



Cyber Range on a Budget (for any organization)



Cyber Range on a Budget (for any organization)

Apply What You Have Learned Today:

- Next week you should:
 - Assess the resources that you have that can be temporarily repurposed (space, computers, networks, PowerPoint / video) – you may have more than you realize!
- In the first three months following this presentation you should:
 - Test the use of those resources
 - Using a real-world cyber breach and/or attack, create a simple PowerPoint decision tree using the events, responses and impacts
- Within six months you should:
 - Fine-tune your DIY Cyber Range
 - Improve the quality, quantity and sophistication of your content
 - Explore opportunities for content sharing with others in your target sector

Cyber Range on a Budget (for any organization)

- The proven value of Cyber Ranges can now be made available to the widest number of companies, schools and other organizations at little or no resource cost
- Use the process and examples identified in this presentation on how to create a practical Cyber Range at little or no cost in your *own* organization!

RSAConference2022

San Francisco & Digital | June 6 – 9

SESSION ID: AIR-T02

Cyber Range on a Budget (For Any Organization) Thank You! Questions?

Rick Trilling

Professor of Cybersecurity Management
Wentworth Institute of Technology, Boston

TRANSFORM

