

# Surviving Security Groundhog Day



Ron Woerner, CISSP, CISM

April 2024



# Who am I?

Ron Woerner<sup>1</sup>

- Hacker
- CyberSecurity Consultant / Trusted Advisor<sup>2</sup>
- Professor, Bellevue University
- 25+ years experience in IT / Security
- Blogger, writer, and podcaster

Slides available at <https://github.com/hackerron/SecurityGHD/>

<sup>1</sup> Who I'm claiming to be atm

<sup>2</sup> Can't say my employer



Websites & Social Media:

<https://linktr.ee/cyberron>



LinkedIn:

<https://www.linkedin.com/in/ronwoerner/>

# AI – 2024 Hottest tech topic

How “old” is AI?

[iow, how long has it been a thing?]

*Dartmouth Summer Research Project on Artificial Intelligence* (DSRPAI) in 1956.

Source: <https://sitn.hms.harvard.edu/flash/2017/history-artificial-intelligence/>

# AI Risks & Threats

# New?

**Prompt:** I'm building a presentation on cybersecurity and AI for a technical audience. Provide 5 ways ChatGPT and AI can be used maliciously.

- Automated social engineering
- Supercharged phishing
- Deepfakes and disinformation
- Enhanced cyber reconnaissance
- Malware automation & mutation

Discussions of artificial intelligence (AI) often swirl with mysticism regarding how an AI system functions. The reality is far more simple:

***AI is a type of software system.***

**CYBERSECURITY &  
INFRASTRUCTURE  
SECURITY AGENCY**

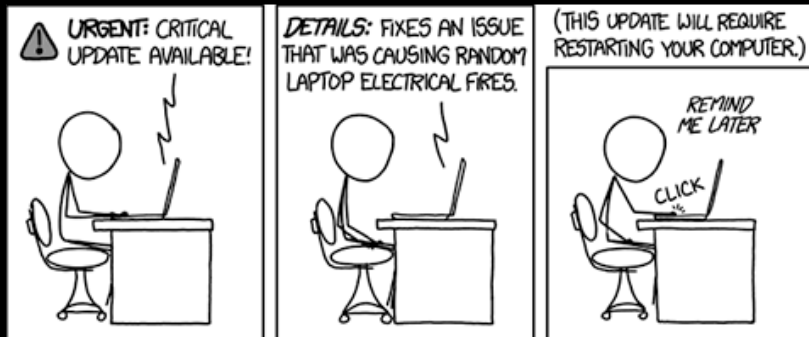
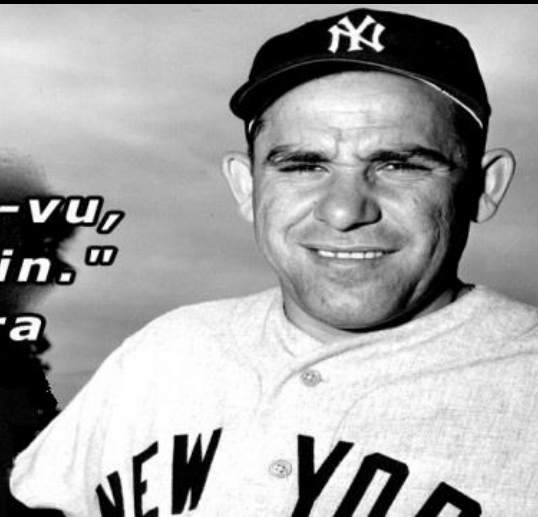


**AMERICA'S CYBER DEFENSE AGENCY**

<https://www.cisa.gov/news-events/news/software-must-be-secure-design-and-artificial-intelligence-no-exception>

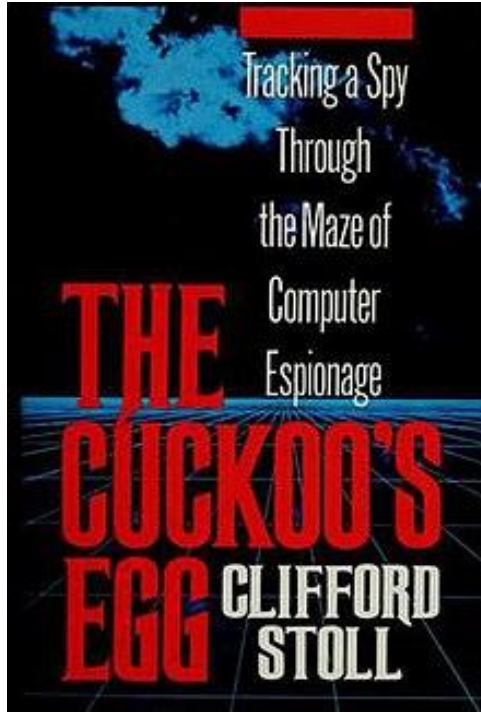


***It's like deja-vu,  
all over again."  
- Yogi Berra***



**BACK**  **TIME**





# When?

CTI Summit Keynote - Cliff Stoll - (Still) Stalking the Wily Hacker  
<https://www.youtube.com/watch?v=1h7rLHNXio8>

## Eight questions for 17 June briefing

- How does the bastard break into computers?
- Which computers did he slither into?
- How did the scoundrel become superuser?
- How did the SOB get Cray passwords?
- Did the skunk guard against detection?
- Can you audit a varmint who's sys manager?
- How do you trace an eggsucker back to his roost?

Why do we still work on this problem?



NCCIC | NATIONAL CYBERSECURITY &  
COMMUNICATIONS INTEGRATION CENTER

---

*AWARENESS BRIEFING:*

# RUSSIAN ACTIVITY AGAINST CRITICAL INFRASTRUCTURE



NCCIC

<https://www.cisa.gov/news-events/alerts/2018/03/15/russian-government-cyber-activity-targeting-energy-and-other-critical>

# National Debate

## Pineapple on Pizza?



# THE WAR ON PINEAPPLE: Understanding Foreign Interference in 5 Steps



To date, we have no evidence of Russia (or any nation) actively carrying out information operations against pizza toppings. This infographic is an ILLUSTRATION of how information operations have been carried out in the past to exploit divisions in the United States.

## 1. TARGETING DIVISIVE ISSUES

Foreign influencers are constantly on the lookout for opportunities to inflame hot button issues in the United States.



**They don't do this to win arguments; they want to see us divided.**



### American Opinion is Split: Does Pineapple Belong on Pizza?

An A-list celebrity announced their dislike of pineapples on pizza, prompting a new survey. No matter how you slice it, Americans disagree on the fruit topping.

[https://www.cisa.gov/sites/default/files/publications/19\\_1008\\_cisa\\_the-war-on-pineapple-understanding-foreign-interference-in-5-steps.pdf](https://www.cisa.gov/sites/default/files/publications/19_1008_cisa_the-war-on-pineapple-understanding-foreign-interference-in-5-steps.pdf)

# Midnight Blizzard



## EMERGENCY DIRECTIVE

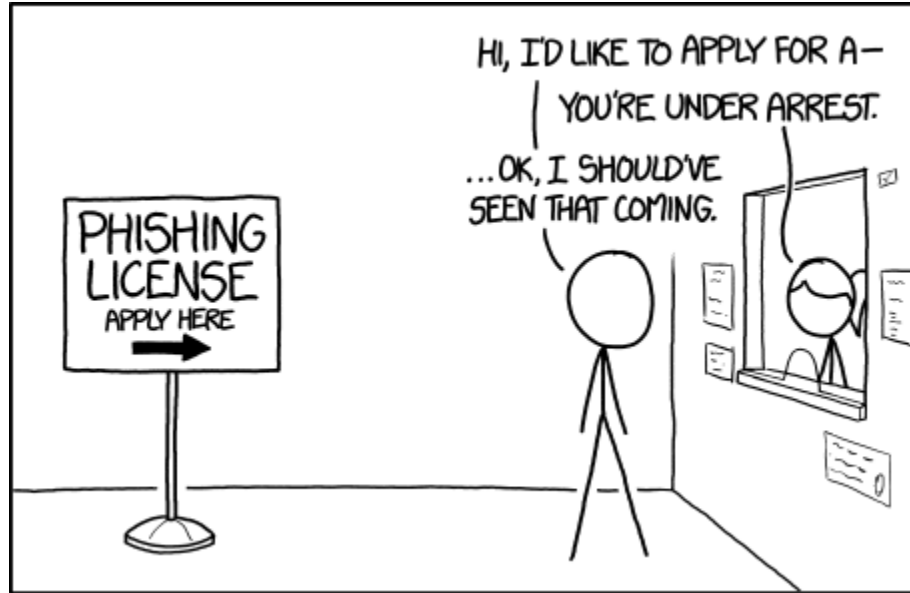
**ED 24-02:**

MITIGATING THE SIGNIFICANT  
RISK FROM NATION-STATE  
COMPROMISE OF MICROSOFT  
CORPORATE EMAIL SYSTEM

<https://www.cisa.gov/news-events/directives/ed-24-02-mitigating-significant-risk-nation-state-compromise-microsoft-corporate-email-system>



# Phishing Still Works



If it were only  
this easy...

<https://xkcd.com/1694>

And ransomware is still a problem.

<https://spin.ai/resources/ransomware-tracker/>



Eugene Spafford's first principal of security administration:

*If you have responsibility for security, but have no authority to set rules or punish violators, your role is to take the blame when something goes wrong.\**

\* Garfinkle & Spafford, ***Practical Unix & Internet Security***, O'Reilly & Associates, Inc, 1996, p.39.



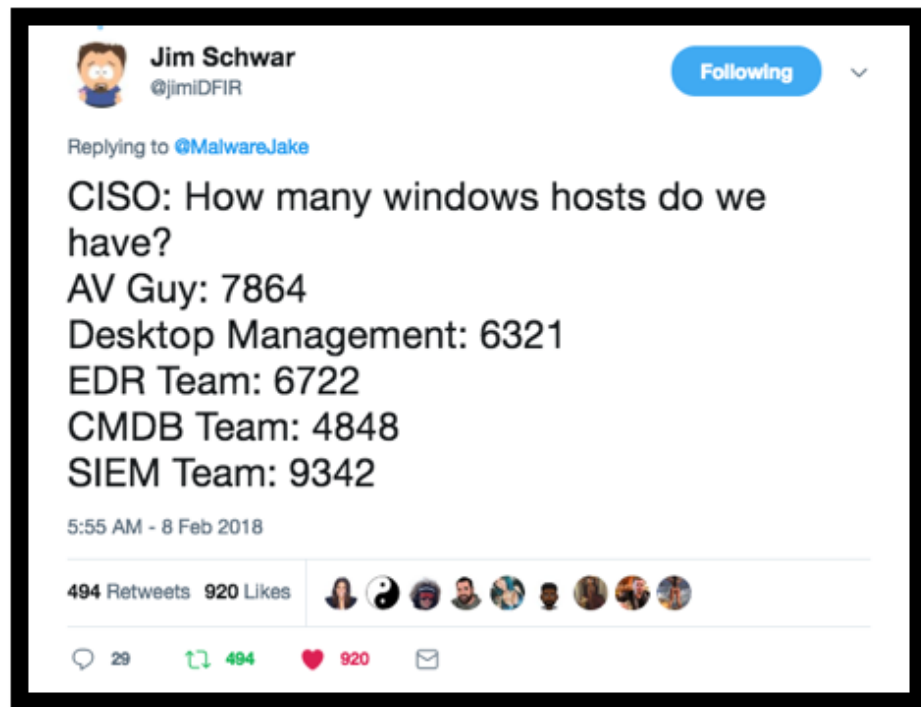
# Where's our stuff?

*"Asset management isn't sexy. Penetration testing and red team and analysis gets all the job reqs, because it's far more flashy. Effective security is boring."*

- Nathan W Burke



<https://nmap.org/>



Security Groundhog Day

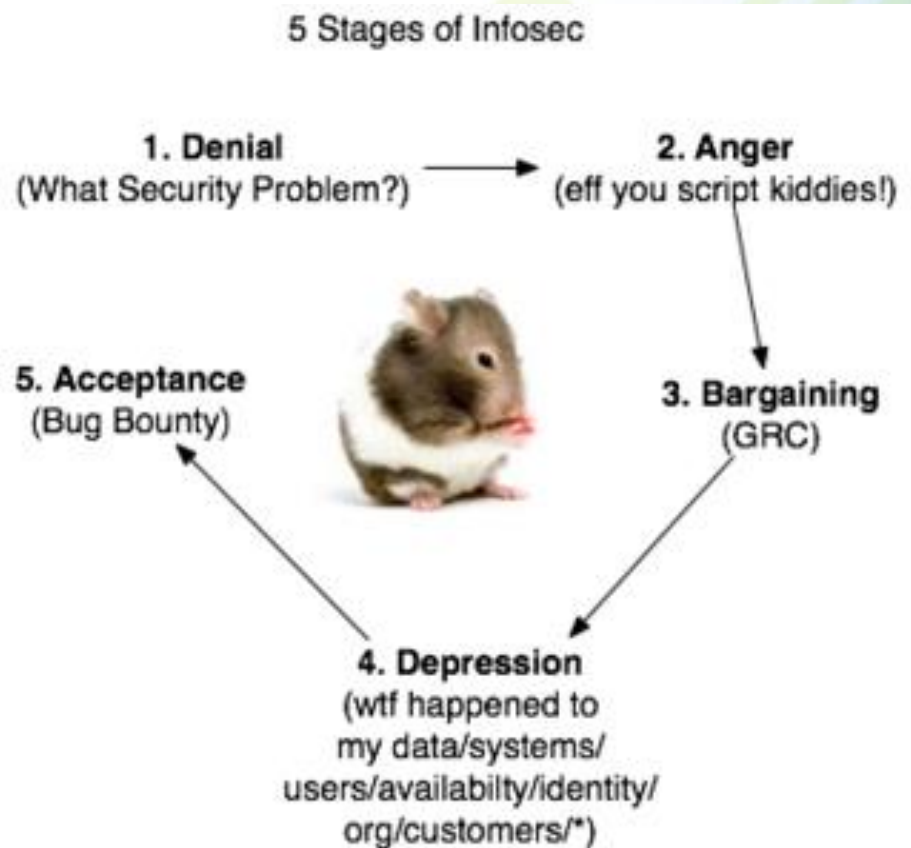
**STUCK!**



# STUCK!

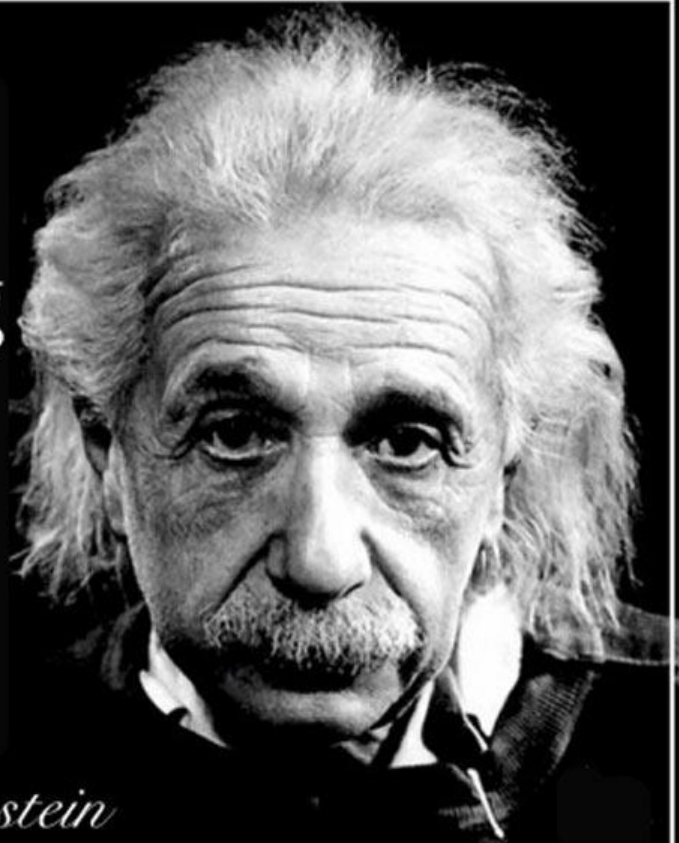
2. HT to Andrew Jacquith

<http://www.markerbench.com/blog/2005/05/04/Escaping-the-Hamster-Wheel-of-Pain/>



Insanity:  
doing the same thing  
over and over again  
and expecting  
different results.

*- Albert Einstein*









somewhere to sleep, somewhere to sleep, to rest my head.

# STUDY HISTORY



**“Those who don’t study history are doomed to repeat it.  
Yet those who *do* study history are doomed to stand by  
helplessly while everyone else repeats it.”**





**"It is said that if you know your enemies and know yourself, you will not be imperiled in a hundred battles;  
if you do not know your enemies but do know yourself, you will win one and lose one;  
if you do not know your enemies nor yourself, you will be imperiled in every single battle."**

# The Protection of Information in Computer Systems

JEROME H. SALTZER, SENIOR MEMBER, IEEE, AND MICHAEL D. SCHROEDER, MEMBER, IEEE

Manuscript received October 11, 1974; revised April 17, 1975. Copyright © 1975 by J. H. Saltzer.

- Least privilege
- Economy of mechanism
- Complete mediation
- Open design
- Separation of privilege
- Least common mechanism
- Psychological acceptability
- Fail-safe defaults

The Security Principles of Saltzer and Schroeder, as illustrated with Star Wars

[By Adam Shostack](#)

<https://shostack.org/blog/the-security-principles-of-saltzer-and-schroeder>

<https://www.cs.virginia.edu/~evans/cs551/saltzer/>

# Dr. Grace Murray Hopper

*"The only phrase I've ever disliked is, 'Why, we've always done it that way.' I always tell young people, 'Go ahead and do it. You can always apologize later.'"*

*"To me programming is more than an important practical art. It is also a gigantic undertaking in the foundations of knowledge."*

*"I've always been more interested in the future than in the past."*

[https://en.wikipedia.org/wiki/Grace\\_Hopper](https://en.wikipedia.org/wiki/Grace_Hopper)



Photograph from 1984

# Be a Hacker

## How To Become A Hacker

Eric Steven Raymond

[Thyrsus Enterprises](#)

<[esr@thyrsus.com](mailto:esr@thyrsus.com)>

Copyright © 2001 Eric S. Raymond

### Table of Contents

[Why This Document?](#)

[What Is a Hacker?](#)

[The Hacker Attitude](#)

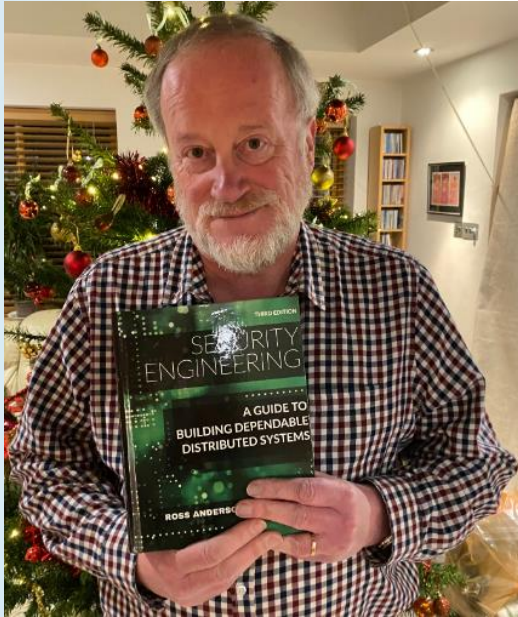
- [1. The world is full of fascinating problems waiting to be solved.](#)
- [2. No problem should ever have to be solved twice.](#)
- [3. Boredom and drudgery are evil.](#)
- [4. Freedom is good.](#)
- [5. Attitude is no substitute for competence.](#)

### [Basic Hacking Skills](#)

- [1. Learn how to program.](#)
- [2. Get one of the open-source Unixes and learn to use and run it.](#)
- [3. Learn how to use the World Wide Web and write HTML.](#)
- [4. If you don't have functional English, learn it.](#)

<http://www.catb.org/~esr/faqs/hacker-howto.html>

# Security Engineering



Dr. Ross Anderson

- [Lecture 1: who is our adversary?](#)
- [Lecture 2: threat models and security policies](#)
- [Lecture 3: banking security](#)
- [Lecture 4: payment security](#)
- [Lecture 5: security economics](#)
- [Lecture 6: security psychology](#)
- [Lecture 7: network security](#)
- [Lecture 8: hardware security](#)
- [Lecture 9: hardware security](#)
- [Lecture 10: operating system security](#)
- [Lecture 11: virtualisation, containers and sandboxes](#)
- [Lecture 12: app stores, supply chains and ecosystem security](#)
- [Lecture 13: safety and security](#)
- [Lecture 14: assurance and sustainability](#)
- [Lecture 15: governance and regulation](#)

<https://www.cl.cam.ac.uk/~rja14/book.html>

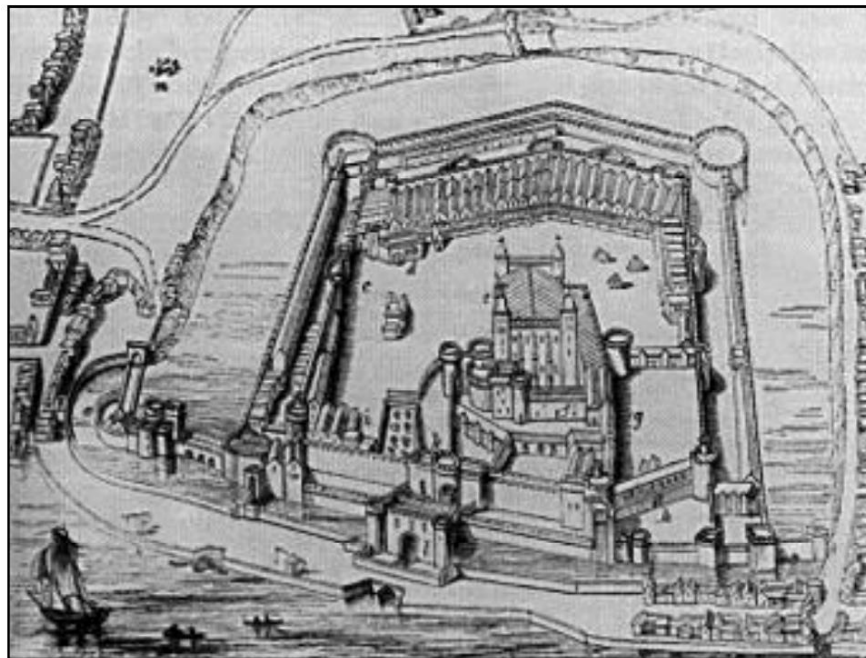
# *Everything I Needed to Know About Network Security I Learned at the Tower of London*

**Castle Lecture**

**April 10, 2002**

United States Military Academy  
West Point, NY

**William Hugh Murray, CISSP**  
[whmurray@sprynet.com](mailto:whmurray@sprynet.com)





## *Everything I Needed to Know About Network Security I Learned at the Tower of London*

### *New Recommendations*

#### Zero Trust

- ◆ Identify the “crown jewels”
- ◆ Encryption by default
- ◆ End-to-end encryption
- ◆ Terminate on the application, not the perimeter or the operating system
- ◆ Restrictive policy at every interface
- ◆ “bastion” between every system and its network
  - ❖ Hardware routers to change the policy to restrictive
  - ❖ Software to resist ex-filtration
- ◆ Know who you are talking to

# OpSec & Social Engineering

## *No-Tech Hacking (or) Ninja Skillz of the Underground*

*Johnny Long, CSC*



### DEFCON 15: No-Tech Hacking - Johnny Long

by [Johnny Long](#)

Publication date

2007-08-04

[https://archive.org/details/johnny-long-no-tech-hacking\\_DEFCON15](https://archive.org/details/johnny-long-no-tech-hacking_DEFCON15)



**The first principle  
is that you must  
not fool yourself  
and you are the  
easiest person  
to fool.**

*Richard P. Feynman*





“Just because you see something on the Internet with a quote, a picture and a date, it doesn’t mean it’s going to be true.”

- Abraham Lincoln, 2006

# Trust, AND Verify

aka Zero Trust

# Ask the right questions

- » What is the risk of a data breach?
- » How much risk is associated with an employee accidentally sharing client health details with the wrong party, worst case over the next year?

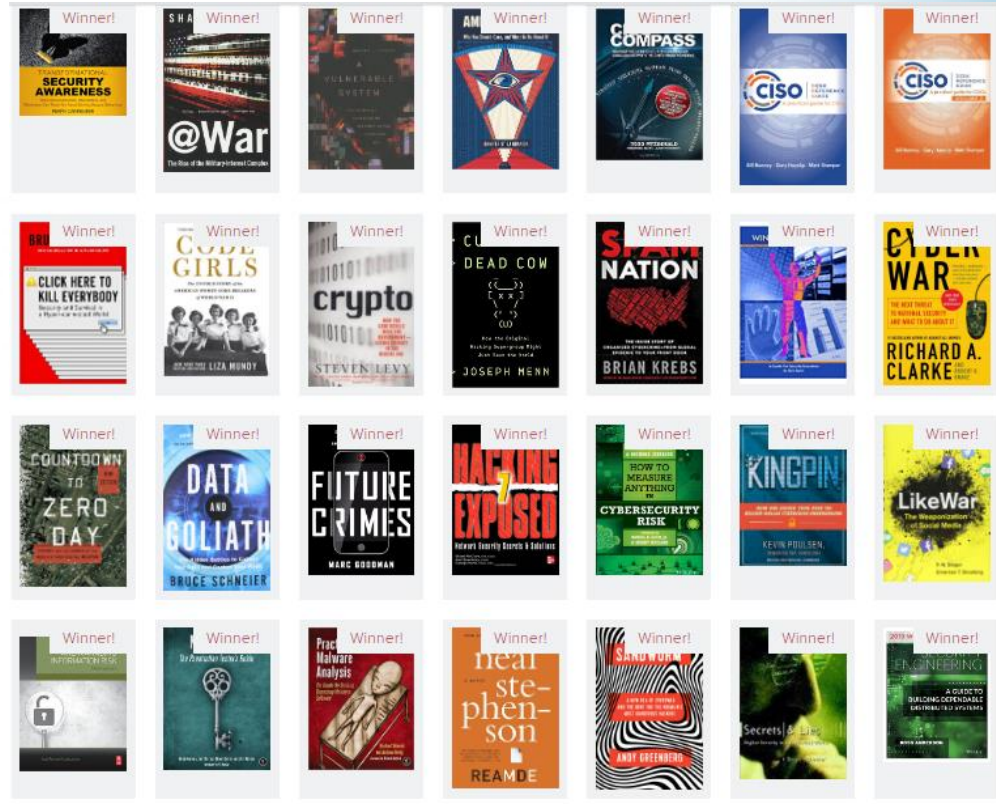


# Keep Learning

## CYBERSECURITY CANON

Cybersecurity Canon

<https://icdt.osu.edu/cybercanon>



<https://icdt.osu.edu/cybercanon/bookreviews>



# Solution = Kids



<https://www.nebraskagencyber.com/>



<http://www.uscyberpatriot.org>

# AI Use in Cybersecurity

**Prompt:** Provide 5 ways AI can help cybersecurity and technical professionals reduce risks of malicious use of AI.

- Threat Intelligence and Prediction
- Automated Threat Detection and Response
- Phishing and Social Engineering Detection
- Proactive Vulnerability Management
- Endpoint Security with Behavioral Analysis

<https://github.com/hackerron/AI-Cybersecurity>

# Apply what you learn (iow homework)

- » ABC = Always Be Curious
- » RTFM
- » Share!
- » If you see something, say something
- » In the next week, review these slides and use 2-3 resources

I HAVE NO SPECIAL  
TALENTS. I AM ONLY  
**PASSIONATELY  
CURIOUS.**  
-ALBERT EINSTEIN

# Cybersecurity Groundhog Day



**Ron Woerner, CISSP, CISM**

**Cyber-AAA, Founder**

**ronw@ Cyber-AAA.com**

**Linktr.ee: <https://linktr.ee/cyberron>**

**Slides: <https://github.com/hackerron/SecurityGHD/>**



<https://vetsec.org/>