Advancing Cyber Resilience in Operational Technology

Jonathon Grant, PE, CISSP, CISM
ECL-USA Virtual Summit
March 19, 2024

About the Presenter

Jonathon Grant, PE, CISSP, CISM

US OT Cyber Security Engineering Manager

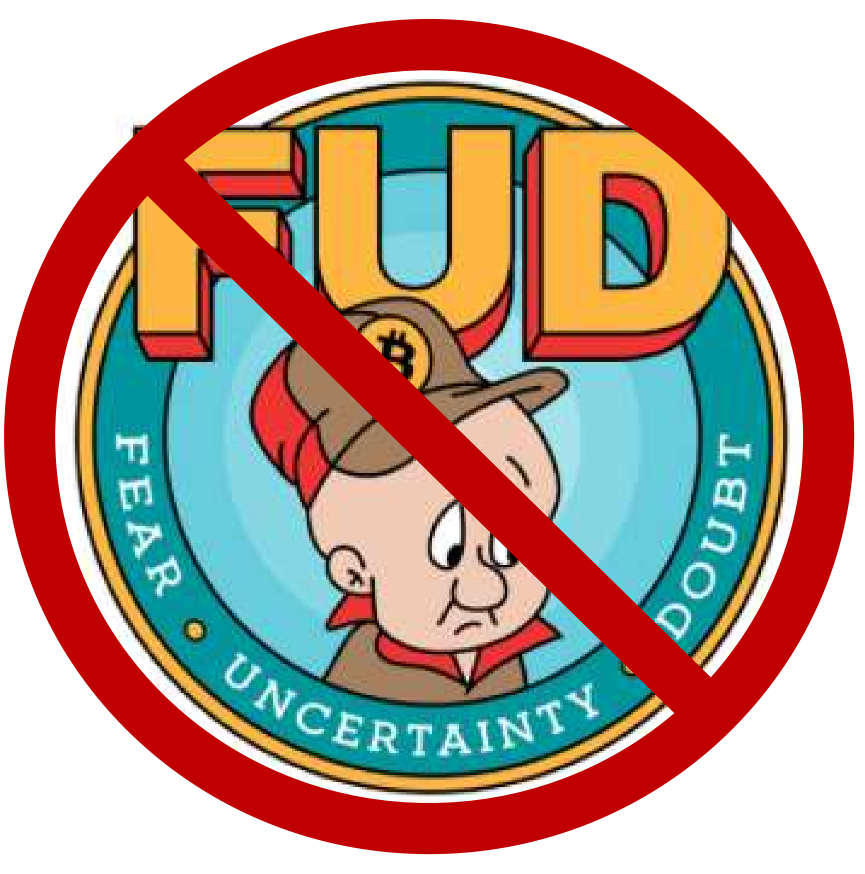
- 25 Years in SCADA/ICS Design and OT Cybersecurity
- B.S. Chemical Engineering, University of Maine
- Professional Engineer, Multiple Jurisdictions
- (ISC)^2 Certified Information Systems Security Professional (CISSP)
- ISACA Certified Information Security Manager (CISM)
- International Society of Automation (ISA) - ISA/IEC 62443 Cybersecurity Expert

Agenda

- Setting the Scene
- Barriers to Progress
- Engineering Community Actions
- Conclusion and Takeaways

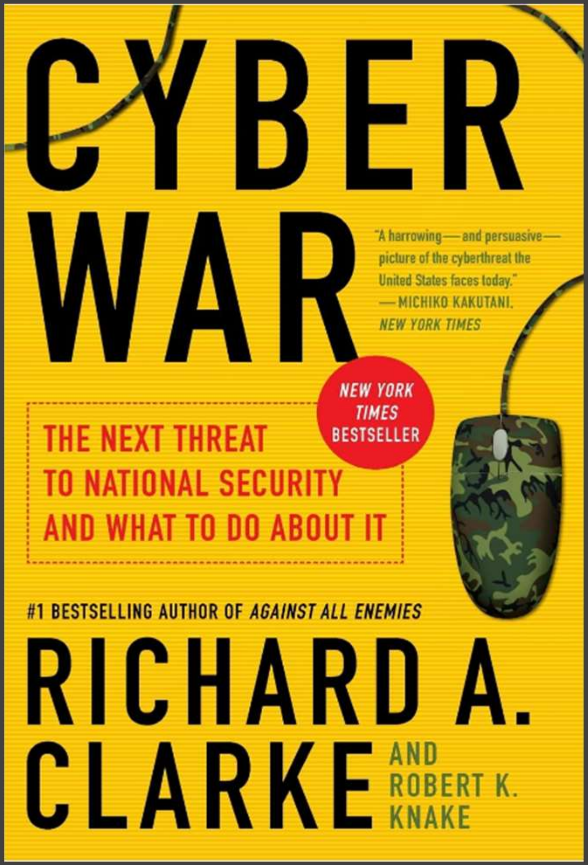
Setting the Scene

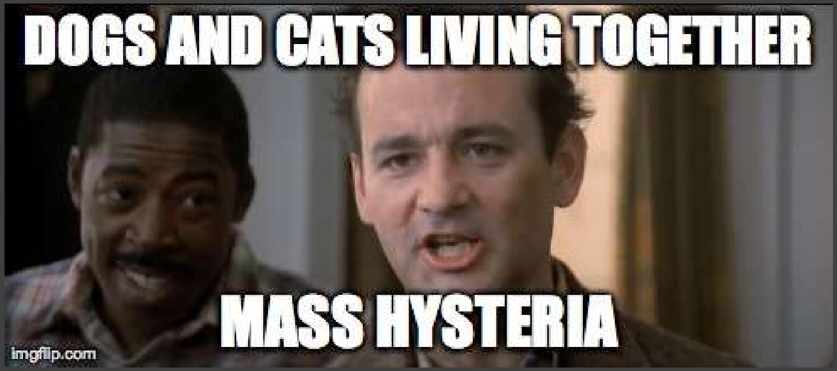
No FUD Allowed



The Hypothetical

- Chapter 2, pgs 64-68
- Theoretical scenario impacting:
  - Power
  - Transportation
  - Finance
  - Water
  - Shipping and logistics


CYBER WAR
"A harrowing—and persuasive—picture of the cyberthreat the United States faces today." —MICHIKO KAKUTANI, NEW YORK TIMES
NEW YORK TIMES BESTSELLER
THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT
#1 BESTSELLING AUTHOR OF AGAINST ALL ENEMIES
RICHARD A. CLARKE
AND ROBERT K. KNAKE



The Reality

- AA24-038A, 2/7/2024
- Contributions from all members the Five Eyes[1]
- Describes methods utilized by nation state actors to pre-position tools to be deployed later
- ‘Groundwork’

JOINT
CYBERSECURITY
ADVISORY

Co-Authored by:

TLP:CLEAR

Product ID: AA24-038A

February 7, 2024

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC

Communications Security Establishment
Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications
Centre canadien pour la cybersécurité

National Cyber Security Centre
PART OF THE GCSB

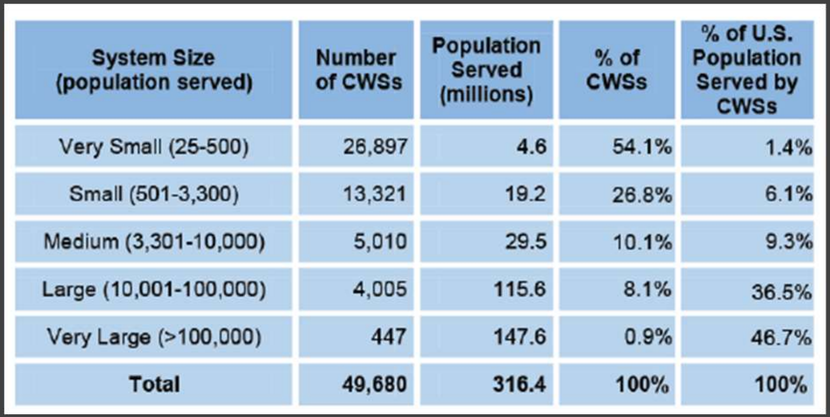
National Cyber Security Centre
a part of GCHQ

PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure

[1] - Five Eyes Intelligence Oversight and Review Council, with membership from the US, UK, Canada, Australia and New Zealand

US OT Critical Infrastructure

- Water Systems (see table)[1]
- Wastewater treatment [1]
  - Estimated 14,748 treatment systems support 238 million people
- Nearly 3,000 electric utilities[2]
- 292,825 manufacturing facilities (est.)[3]



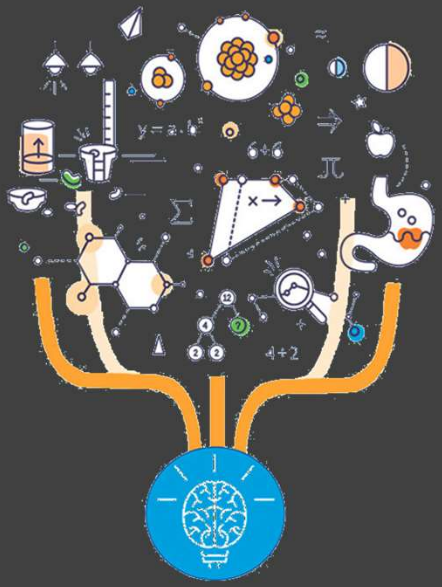
System Size (population served)	Number of CWSs	Population Served (millions)	% of CWSs	% of U.S. Population Served by CWSs
Very Small (25-500)	26,897	4.6	54.1%	1.4%
Small (501-3,300)	13,321	19.2	26.8%	6.1%
Medium (3,301-10,000)	5,010	29.5	10.1%	9.3%
Large (10,001-100,000)	4,005	115.6	8.1%	36.5%
Very Large (>100,000)	447	147.6	0.9%	46.7%
Total	**49,680**	**316.4**	**100%**	**100%**

[1] – Michigan Center for Sustainable Systems (water) (wastewater)
[2] – US Energy Information Administration, 2019
[3] – American Manufacturing Statistics, 2021 (Link)

Barriers to Progress

Mindset and Landscape

- Thought process:
  - “Our system is air-gapped.”
  - “We’re too small to be a target.”
  - “There’s nothing of value here for someone to waste their time.”
  - “We have insurance to cover it.”
- Cannot count on government intervention
- Cyber insurance is costly and becoming difficult to secure



ECL-USA

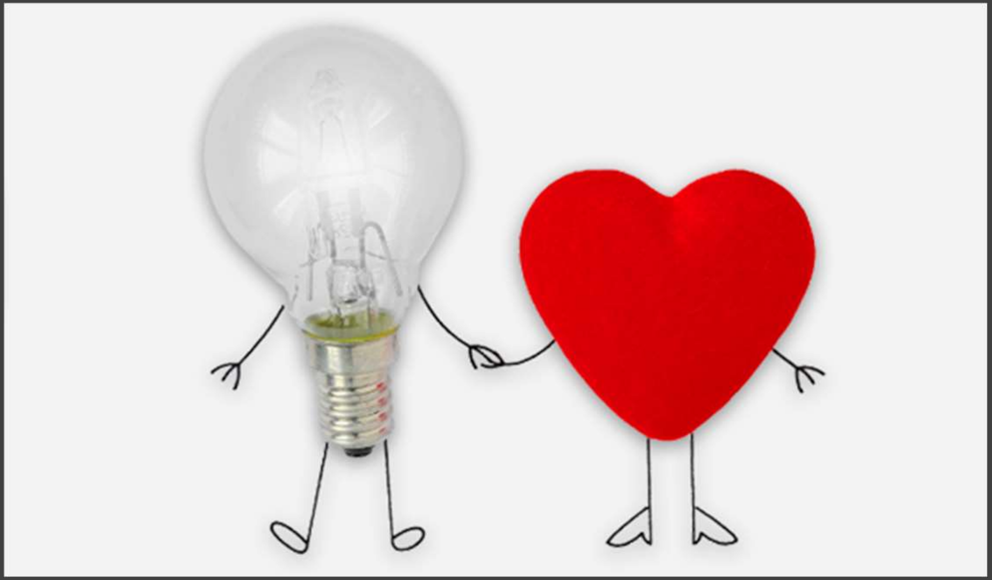
Lack of Meaningful Enforcement

- Guidelines and frameworks
  - NIST SP800-82
  - ISA/IEC 62443
  - NERC CIP
- Most CI sectors in the US have no OT cybersecurity requirements
  - EPA recently called off regulations for water sector
  - NERC CIP standards are a notable exception (compliance)

Engineering Community Actions

Changing Hearts and Minds

- Continue educating organizations/decision makers on the impact of cyber events, regardless of organizational size
- Ensure that cyber risk mitigation is considered in budgeting cycles
- Inform (don’t surprise) that cybersecurity is an ongoing process, not a destination



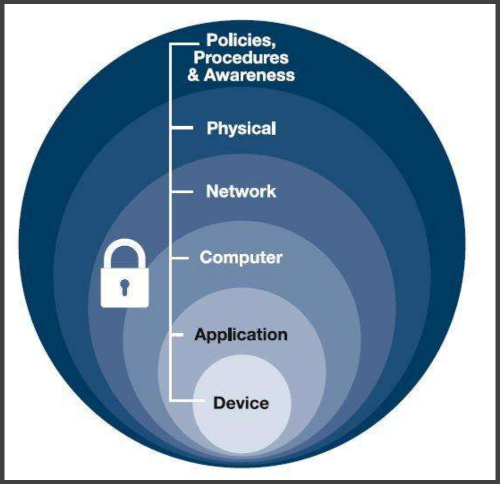
Automation Vendors

- Use influence as professionals
- Advocate for‘baked in’ security controls
- Reduce the dependency on compensating controls

Rockwell Automation
ABB
SEL SCHWEITZER ENGINEERING LABORATORIES
SIEMENS
Honeywell
paloalto NETWORKS
EMERSON
GE
FORTINET
PHOENIX CONTACT

Elevate the Standard of Care

- Basic cybersecurity knowledge for all disciplines
- Utilize CCE framework and process
- Don’t just ‘make it work’; also ‘make it secure’
  - Defense in Depth



Conclusion and Takeaways

Conclusion and Takeaways

- US OT critical infrastructure is particularly vulnerable
- There is opportunity to make meaningful change
- Don’t try to ‘boil the ocean’

ECL-USA

Jonathon Grant, PE, CISSP, CISM
Manager, OT Cyber Security Engineering
jonathon.grant@nationalgrid.com
C: 781.856.3367