
TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE
trustedci.org

Evidence Based Cybersecurity

Grayson F. Harbour
Student Policy Analyst, Trusted CI/CACR

2018 NSF Cybersecurity Summit for Large Facilities and Cyberinfrastructure

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Outline

1. Define evidence based cybersecurity
2. Discuss research methodology
3. Examine the application of evidence based practice to cybersecurity

The need for change

Lack of evidentiary support in many cybersecurity standards and compliance regimes.

Black box approach to control set production.

“Because we said so” is not and should not be enough.

Cybersecurity evidence based practice

Evidence based cybersecurity is an approach to cybersecurity practice that prioritizes the use of rigorous research products, real world facts, and direct observation to drive decision-making.

Evidence Based Practice Research

What is evidence?

ev·i·dence

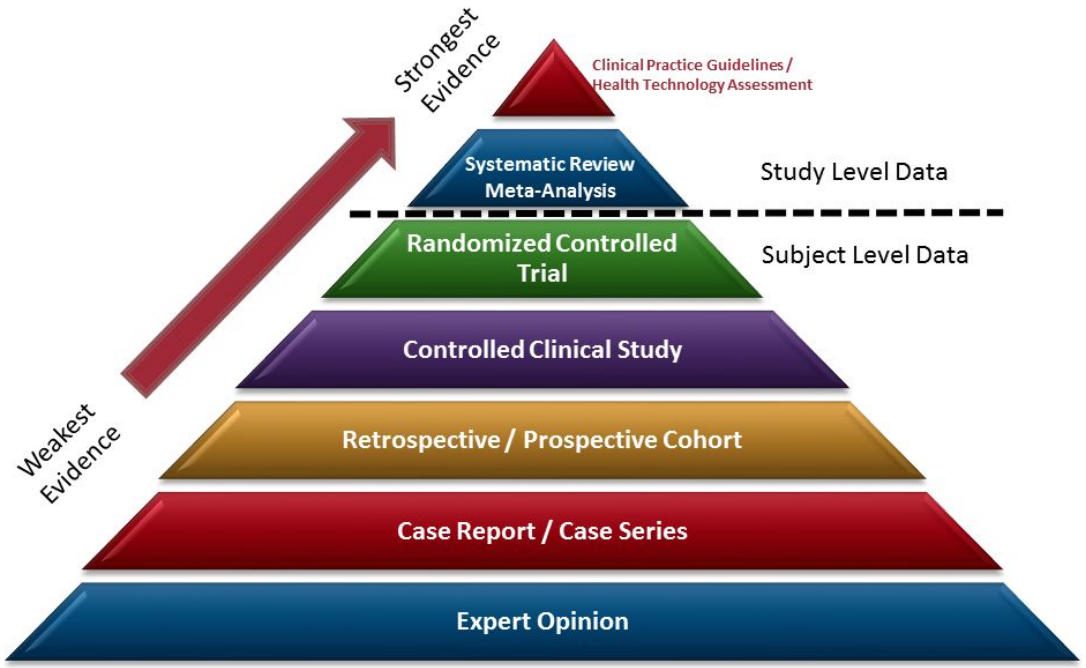
ˈevədəns/ *noun*

the available body of facts or information indicating whether a belief or proposition is true or valid.

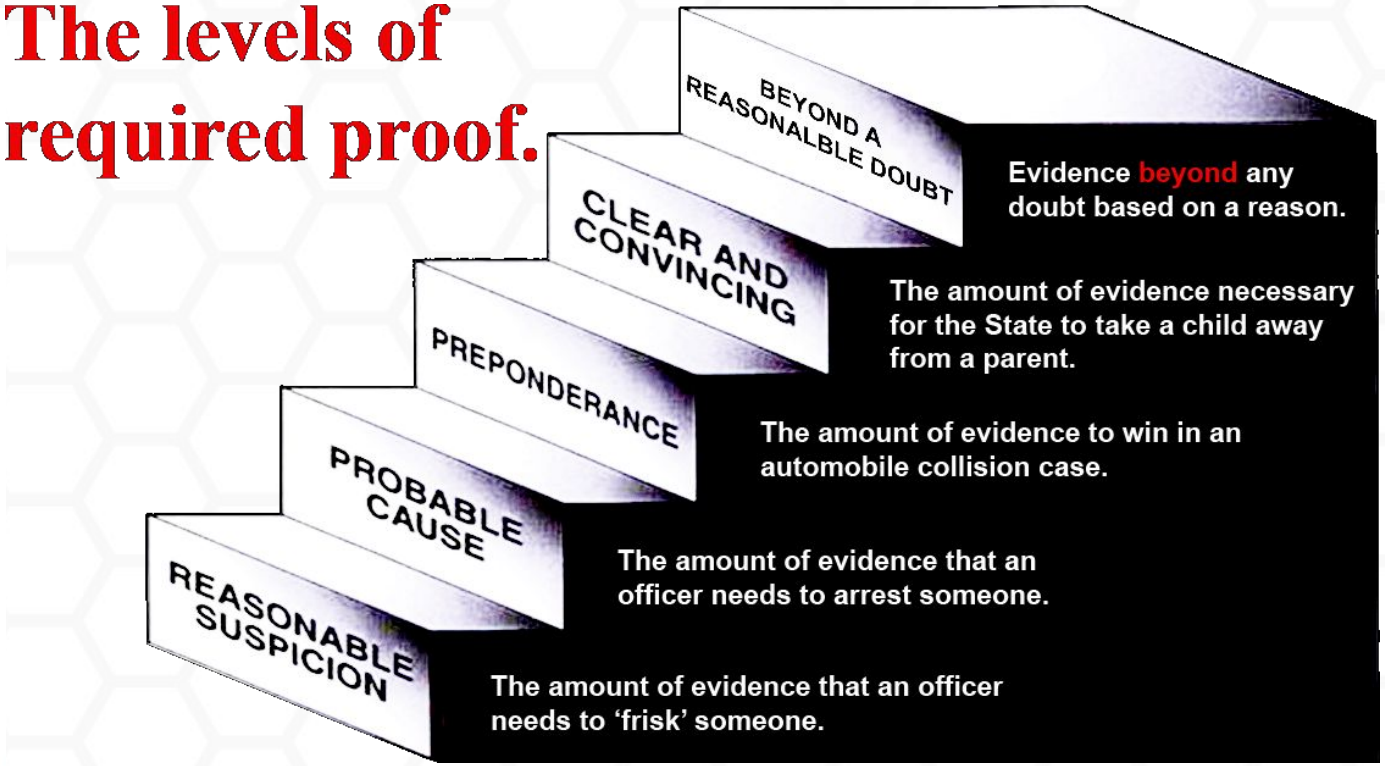
TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Source: Oxford English Dictionary (OED)

Models of evidence



Source: USF Shimberg Health Sciences Library Guides, *Levels of Evidence*

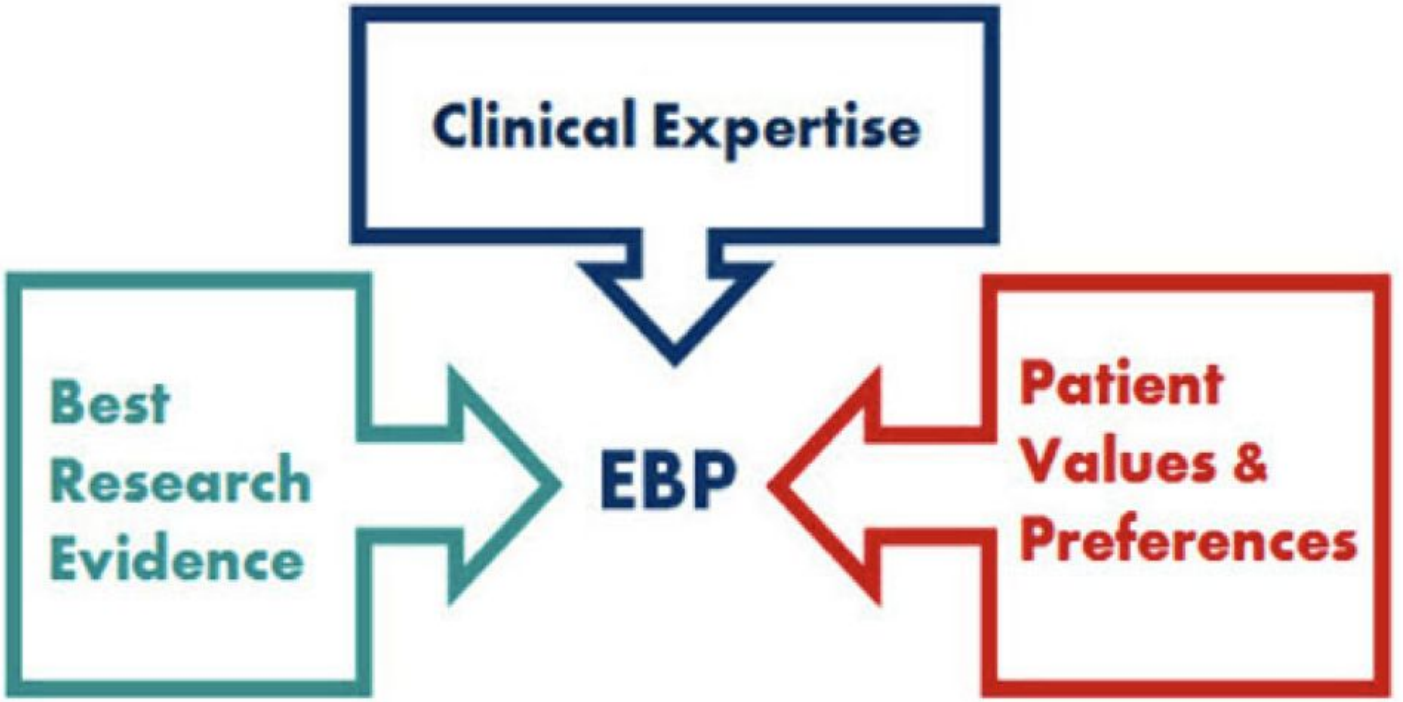


Source: Scott Key, *Georgia Criminal Appellate Law Blog*

What is Evidence Based Practice?

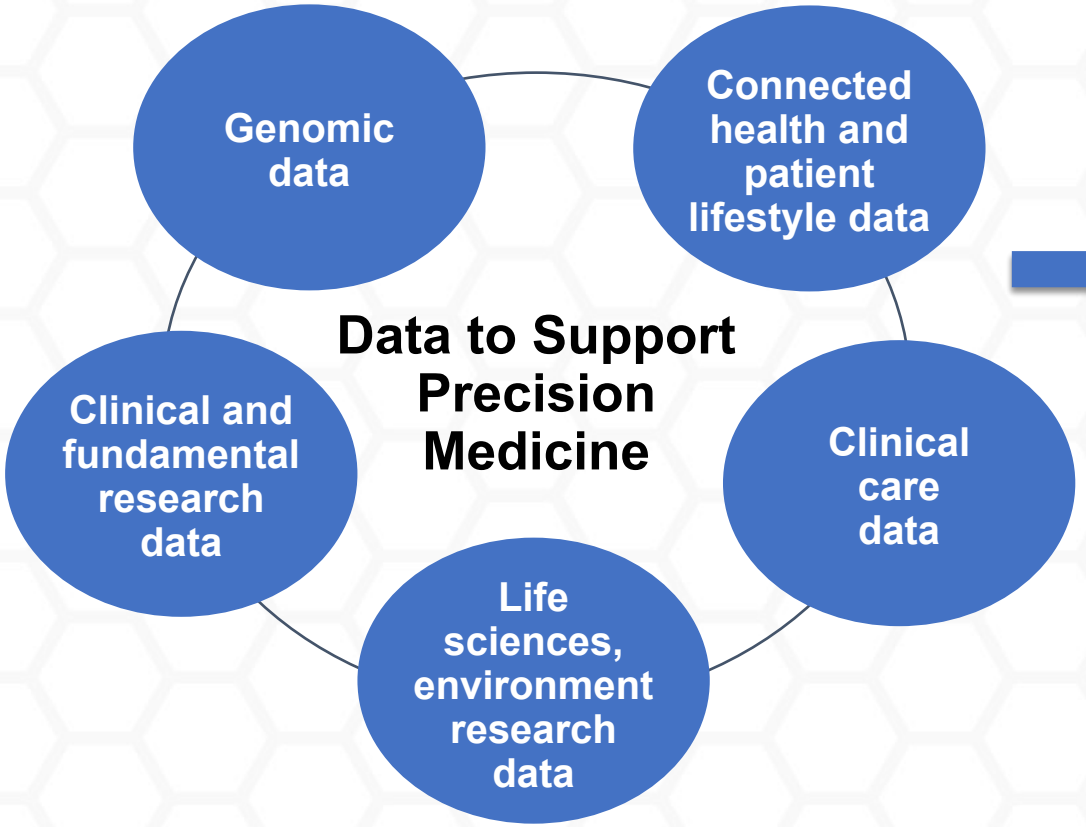
"the conscientious, explicit and judicious use of current best evidence in making decisions about the care of the individual patient. It means integrating individual clinical expertise with the best available external clinical evidence from systematic research." (Sackett D, 1996)

1996 model



Source: Duke Library Guides, *Introduction to Evidence Based Practice*

Precision medicine will leverage large volumes and varieties of data to improve insight & outcomes.



Many data sources and types…

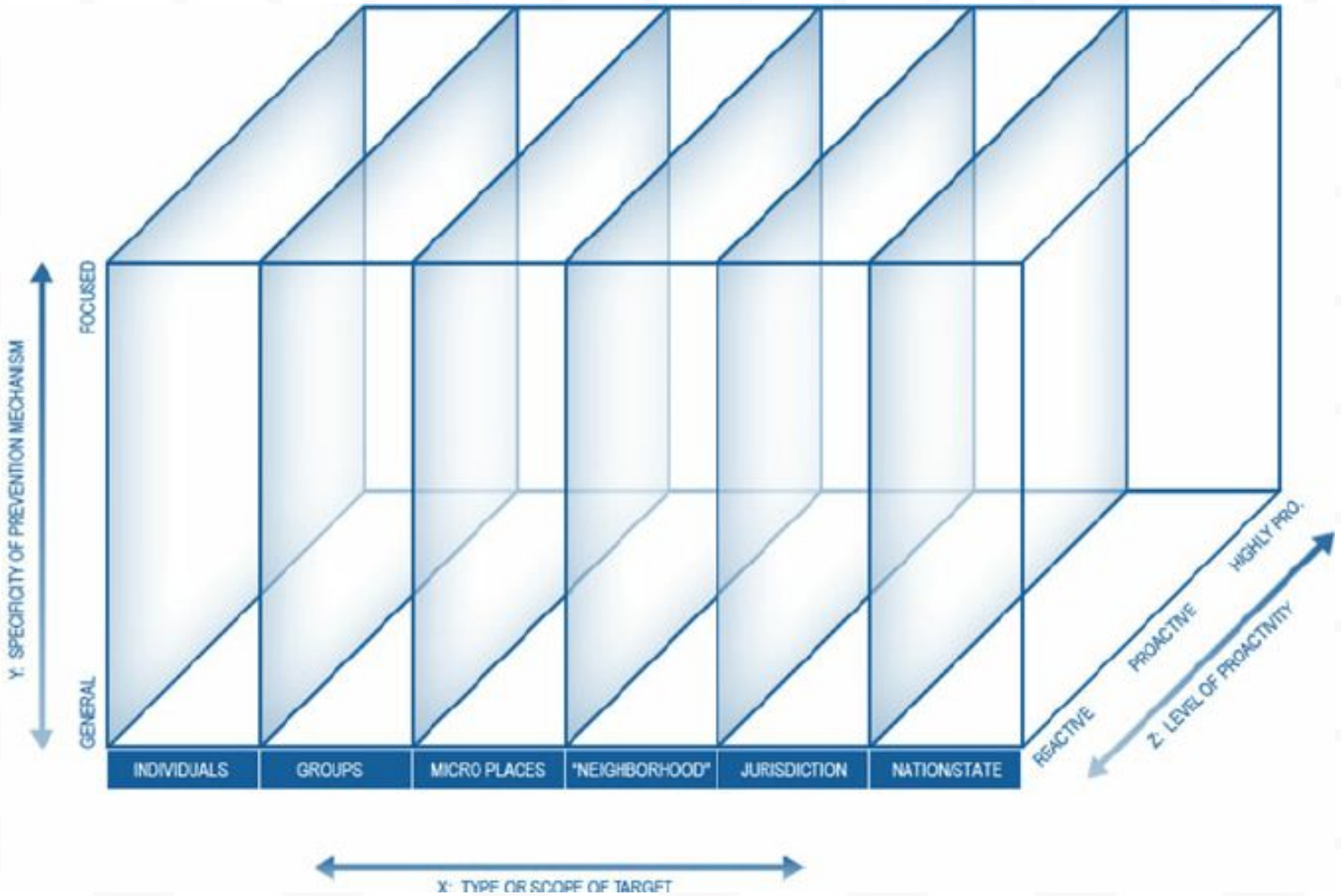
- Connected health and wearables data
- Real World Evidence (RWE) leveraging UDIs (medical device Unique Device Identifiers)
- Clinical care data and observations – image, text, numerical, video, audio, holograms?, etc.
- Clinical and fundamental research data
- Genomic data

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Source: Florence D. Hudson

*Source: NIH 2015; *The New England Journal of Medicine, Vol. 378, No. 7, February 15, 2018 "Medical Devices in the Real World"*

Evidence based policing



- Reactive vs. Proactive
- Different levels of jurisdiction
- Specificity of targeting

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Source: Lum, Cynthia *The Evidence-Based Policing Matrix,* J Exp Criminol (2011) 7:3–26.

Evidence based education

- Robust research and development enterprise
- Government policies demanding solid evidence of effectiveness
- Genuine, generational progress instead of the usual pendulum swings of opinion and fashion

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Source: Robert E. Slavin, *Evidence-Based Education Policies: Transforming Educational Practice and Research* Educational Researcher, Vol. 31, No. 7, pp. 15–21

Evidence Based Cybersecurity

Evidence based cybersecurity definition

Evidence based cybersecurity is an approach to cybersecurity practice that prioritizes the use of rigorous research products, real world facts, and direct observation to drive decision-making.

What evidence based cybersecurity is NOT

1. Making decisions based on generalized information
2. Failing to know thyself (e.g., inventory) and the environment (e.g., monitoring)
3. Applying controls without considering the value added
4. Blindly accepting external opinion

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Weigh the evidence

- variety of evidence available
- type of evidence isn’t as imperative as its use in decision making
- practitioner has to:
  - weigh the evidence
  - use the best stuff she can find

Future Sources of Evidence

- Central database
- Increased auditability
  - Auditing tools on a user level
- Peer review of rigorous applied research
- Research published with accessibility in mind
- Cybersecurity treated as a public health issue

What can the community demand now?

1. Proactively search for weighty evidence.
2. When not available, signal demand better evidence.
3. Be a voice for the practice side -- tell the research side what scholarship is needed.
4. Ask policymakers to back up decisions with evidence, or ask why they cannot.

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Acknowledgments

Special thanks to (alphabetically):

Florence D. Hudson

Craig Jackson

Scott Russell

Trusted CI, the NSF Cybersecurity Center of Excellence is supported by the National Science Foundation under Grant ACI-1547272. The views expressed do not necessarily reflect the views of the National Science Foundation or any other organization.

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Trusted CI can help

Contact us to request help, from small questions to month-long engagements:

https://trustedci.org/help/

See also:

https://trustedci.org/situational-awareness/

https://trustedci.org/webinars/

https://trustedci.org/ctsc-email-lists/

http://blog.trustedci.org/

@TrustedCI

TRUSTED CI THE NSF CYBERSECURITY CENTER OF EXCELLENCE

CENTER FOR APPLIED CYBERSECURITY RESEARCH INDIANA UNIVERSITY Pervasive Technology Institute

NCSA

PITTSBURGH SUPERCOMPUTING CENTER

THE UNIVERSITY of WISCONSIN MADISON

NSF

Questions?

Grayson Harbour
gharbour@indiana.edu
317-771-2301

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE