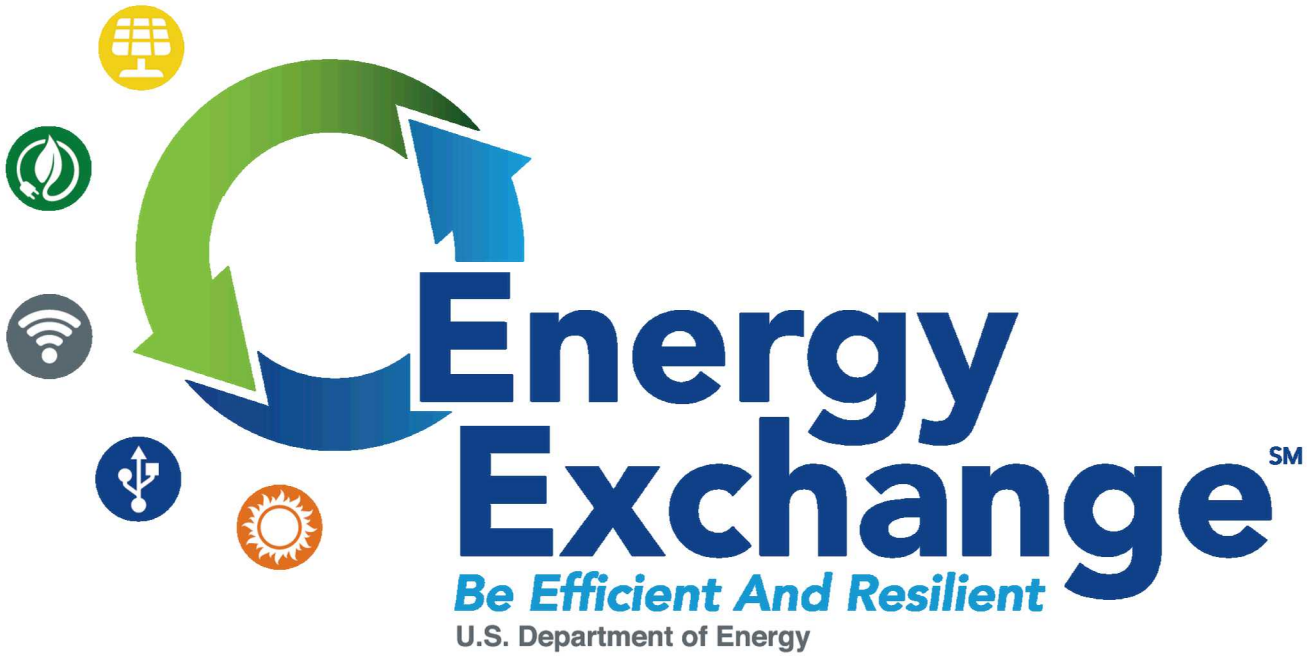
This paper describes objective technical results and analysis. Any subjective views or opinions that might be expressed in the paper do not necessarily represent the views of the U.S. Department of Energy or the United States Government.

SAND2019-9177C



Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Gregory Wyss

Distinguished Member of Technical Staff

Cyber Systems Security Research & Development

Sandia National Laboratories

This material was approved for unlimited release as SAND2019-XXXXXX by Sandia National Laboratories, a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Adversarial Risk Assessment

A Contrarian View

Which site are you more likely to attack?

Answer: It depends…

- Are you trying to steal gold? Or people's wallets and credit cards?
- Are you trying to make a "statement"? Or trying to cause casualties?
- Do you even care if you win the battle?

Review: Risk is…

Risk can be thought of as answers to 3 questions:

- *What can happen?* *(scenario)*
- *How likely is it?* *(probability / frequency)*
- *How bad is it?* *(consequence)*

Risk is the collection of these answers, *not a number!*

Scenario	Consequence	Likelihood
S_1	C_1	P_1
S_2	C_2	P_2
S_3	C_3	P_3
S_4	C_4	P_4
S_5	C_5	P_5
S_6	C_6	P_6
…	…	…

Safety and security risk assessments require different ways of thinking

Safety Analysis	
Hazard (likelihood)	*Tornado*
↓	↓
Sequence of System Events	*Power fails, Roof caves in*
↓	↓
Consequences	*Flooded, Damaged and Failed IT or OT Equipment*

Security Analysis	
Objectives (Consequences)	*Steal handgun ammo*
↓	↓
How someone could cause this (attack scenario)	*Break into gun store after hours to steal*
↓	↓
Who would want to	*List Candidates Here…*
↓	↓
Are there more attractive options for an adversary?	*Big-box store has less security??*
↓	↓
Likelihood I am targeted	*Gun store less likely??*

** Examples are notional and for illustration purposes only.*

Likelihood of attack is highly uncertain and can change rapidly

- Depends on attacker's capability, motivation & intent
- Depends on attacker's other opportunities inside *and* outside the system.
- Predicting likelihood makes risk hard to use for security decision making

A different way to think about security risk:

- An attack scenario is higher risk if:
  - It is easier for an adversary to confidently accomplish,
  - It results in a more desirable outcome for the adversary, and
  - An adversary does not have other alternatives that are obviously superior.

Attack scenarios:

Easy

&

High-Consequence

=

High Risk

One practical security risk management method

Be as systematic as possible!

1. Identify vulnerabilities – things an adversary could exploit in an attack
2. Work these into full attack scenarios that result in consequences
   - *Identify the expected consequences*
3. Identify other easier ways for adversary to cause same or greater consequences
   - *Looking for other more attractive options for the adversary – especially at your facility*
   - *Prioritize mitigation of "highest risks" – easier ways for adversary to cause each outcome of concern*
4. Use good systems engineering to find & rank mitigation options for higher risks
   - *Ways to ↓ consequence and/or ↑ difficulty of the attack scenario*
5. Continue throughout project lifecycle – keep track of all you have learned


Energy
Exchange℠