From Attacks to Action

Building a Usable Threat Model
To Drive
Defensive Choices

Tony Sager

Chief Technologist, the Council on CyberSecurity

August 2014

COUNCIL ON CYBERSECURITY
LE CONSEIL DE LA CYBERSÉCURITÉ

Classic Risk Equation

$$\text{Risk} = f\left\{\frac{\textbf{Vulnerability, Threat, Consequence}}{\text{countermeasures}}\right\}$$

The Security "Fog of More"

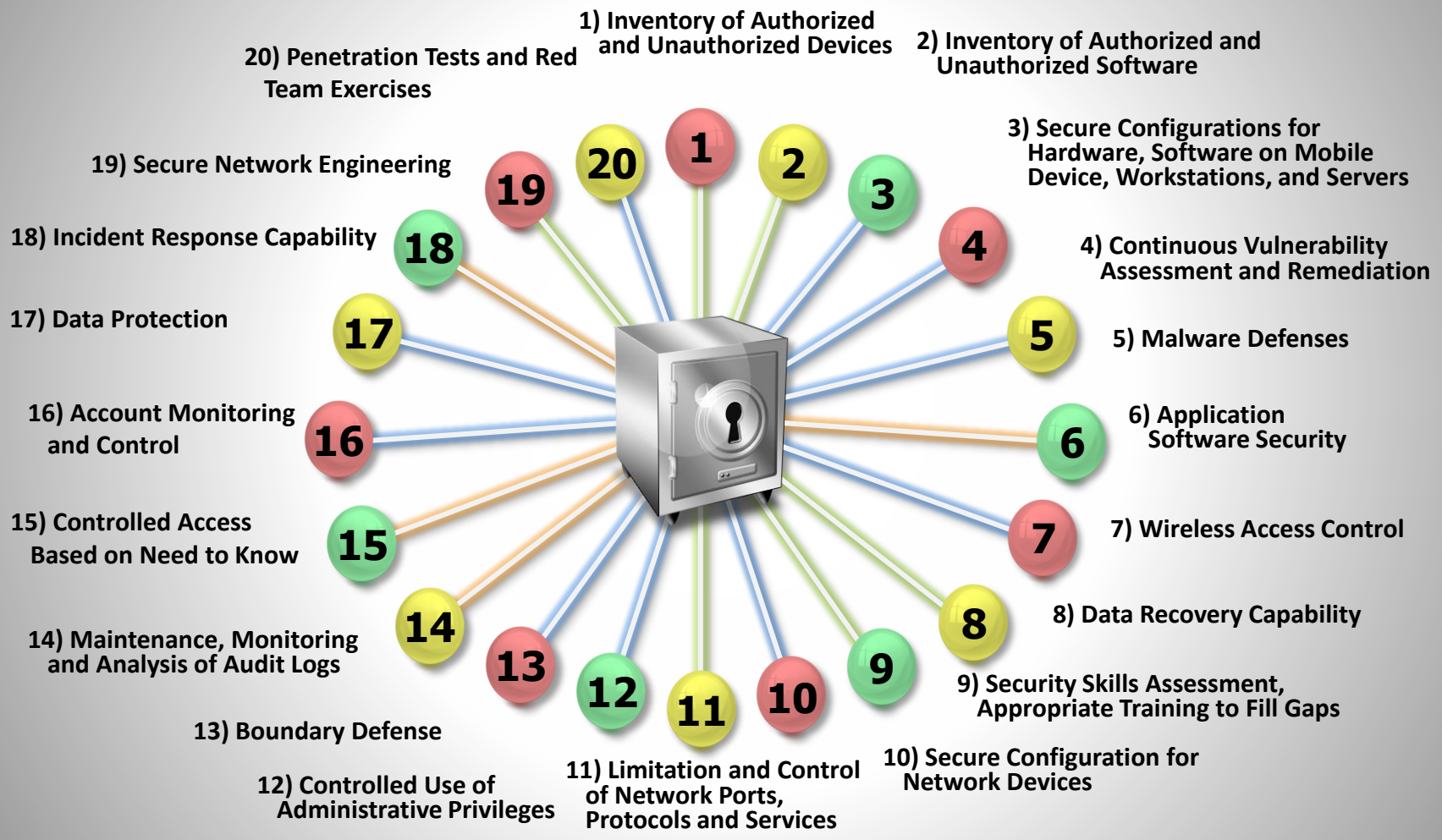
The Defender's Challenges

- *How can I extend my information 'reach' to get a more complete picture of what's going on?*
- *Who can I trust to help me cut through the fog?*
- *How can the data be translated into prioritized action?*
- *How will I know if something relevant changes?*
- *How can I do the right thing – **and then prove it?!?***

Attributes of a usable threat model

- Driven by data
- Translatable to action
  - as part of a larger Risk process, tailored
- Repeatable, dynamic
- Open
  - documented, can use multiple sources, standards-based
- Demonstrable, negotiable

The Critical Security Controls



Council on CyberSecurity
Le Conseil de la CyberSécurité

Evolving a Threat Model for the Critical Security Controls

- Gather friends that I trust
  - and guide them to consensus
- Add thousands of friends
  - and repeat
- Translate/map from an authoritative source of data
  - Verizon DBIR 2013, 2014
- Add numerous sources of data
  - Standardize language, workflow
- Align with Risk Management Frameworks, models
  - Building a “Community Threat Model”

Why a Community Threat Model?

- Extend our information reach
  - *“volume, velocity, variety”*
- Most Enterprises can’t do it on their own
  - *or cannot do it more than once*
- And even if you could, does that make sense…
  - *in a dynamic, connected world?*
  - *where trust and risk are dynamic, and must be negotiated?*

The Council on CyberSecurity

Website: www.counciloncybersecurity.org

Email: info@counciloncybersecurity.org

Twitter: @CouncilonCyber

Facebook: Council on CyberSecurity

Council on CyberSecurity
Le Conseil de la CyberSécurité