Cybersecurity
How Much Is Enough?

Tony Sager
Center for Internet Security (CIS)
Minnesota Cyber Summit, October 2018

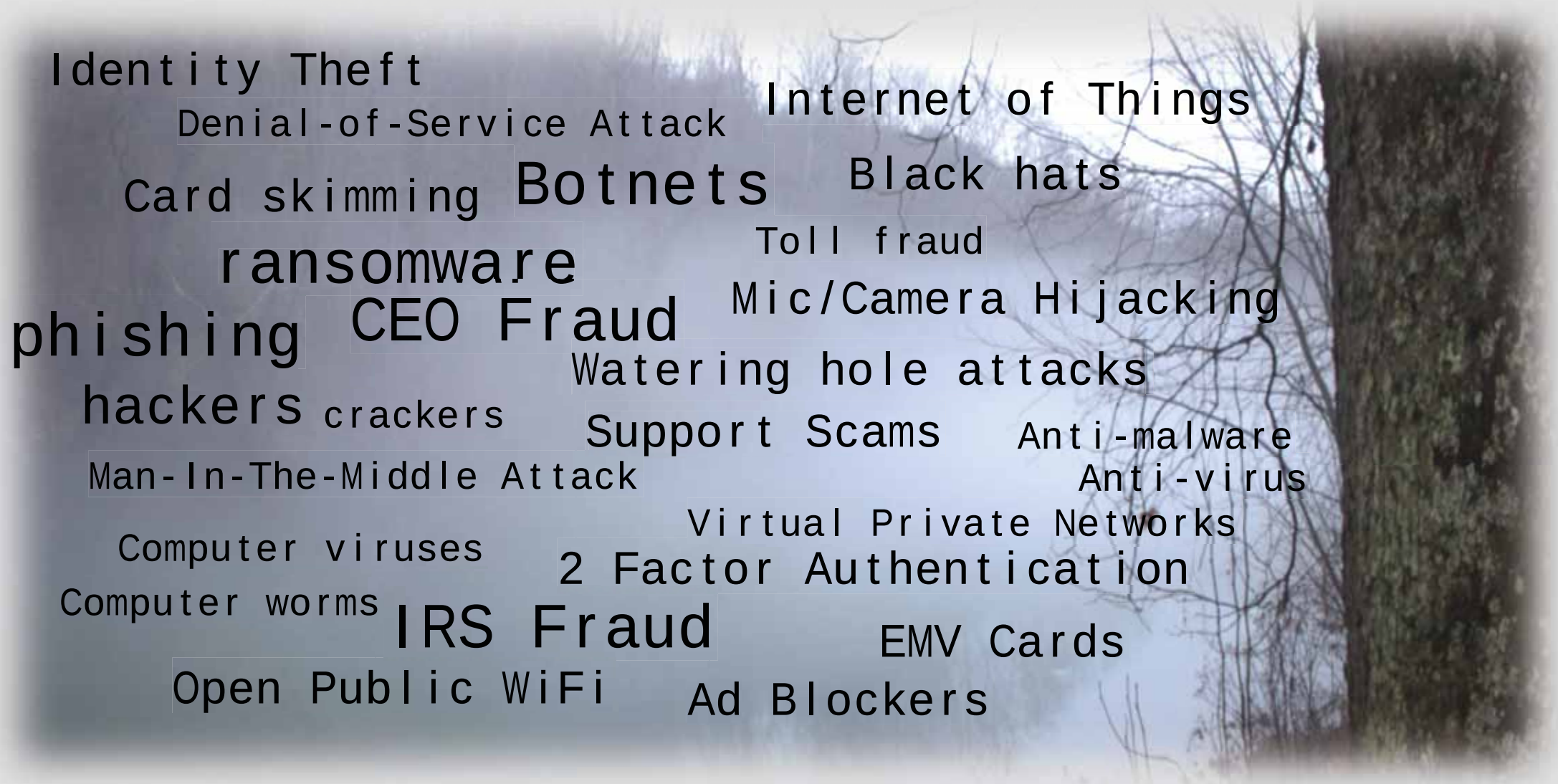
Classic Risk Equation

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

A Lifetime of Cybersecurity Lessons

- We are not Special Snowflakes, and the Bad Guy doesn't perform Magic
- Knowing about vulnerabilities doesn't get them fixed
- There's a large but limited number of defensive choices
  - the 80/20 rule applies (The Pareto Principle)
- People/enterprises don't make security decisions
  - they make economic and social decisions
- Cybersecurity == Information Management *(not Threat Sharing)*
  - when you hear "share", think "translate" and "execute"
- Cybersecurity is more like **Groundhog Day** than **Independence Day**

"The Fog of More"



The Defender's Dilemma

1. What's the "right thing" to do?
    - *and how much do I need to do?*
2. How do I actually do it?
3. ***And how can I demonstrate to others that I have done the "right thing"?***

Evolution of the CIS Controls

NSA/DoD Project

The Consensus Audit Guidelines (CSIS)

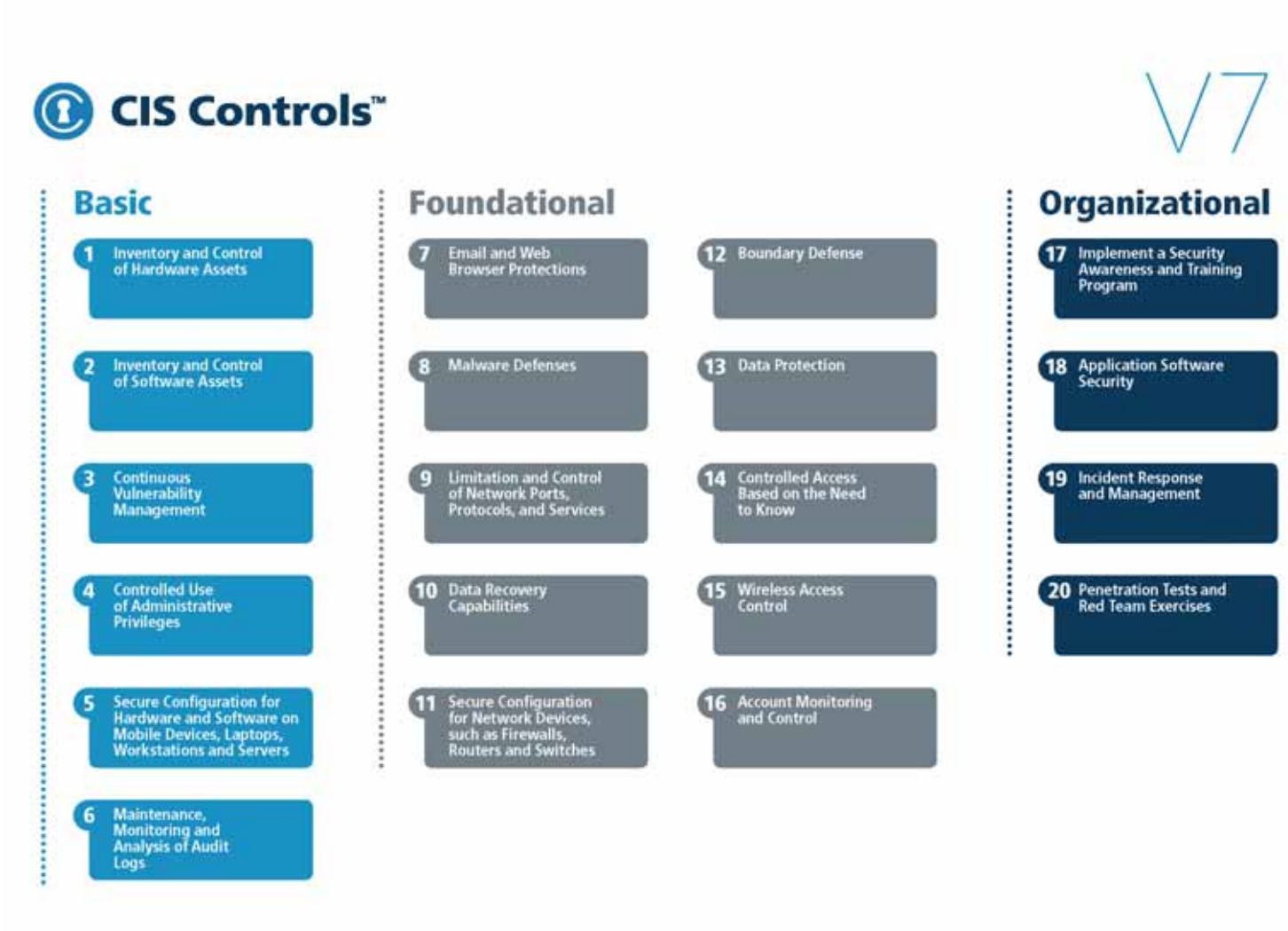
"The SANS Top 20" (the SANS Institute)

The Critical Security Controls (CCS/CIS)

CIS. Center for Internet Security®

The CIS Controls™

CIS Controls Version 7



WHAT *Real People* SHOULD KNOW	WHAT DOES IT MEAN?
Anyone in organized crime (or espionage) who is not in this (cyber) ought to be sued for malpractice	The Bad Guys are highly motivated
Just pointing out problems doesn't get them fixed	Solutions are part of a complex system of feedback, incentives, and verification
It's hard to have a unique problem or an original thought	Point to existing standards, ideas, frameworks
No security snapshot will work, trust is dynamic	Encourage machinery, not reports; measurement, not a state (of security); good IT and Ops management
Threat Sharing is over-rated	Focus on translation, action, efficiency
Not every problem can be solved in the cyber domain	Diplomacy, economics, policy, social norms
Everybody's role is changing (industry, government, academia, standards)	Less control, more about behavior; less central and top-down, more cooperative
We need better parts	Software quality, architectures, ***services***
We've hit Peak Geek in cybersecurity	Cyber as foundation for economic and social decision-making. Demand what you'd demand elsewhere

"It's Not About The List"

- **The CIS Controls Version 7**
- Mappings to other Frameworks
  - Special focus on NIST CSF [updated!]
- CIS Community Attack Model
- CIS Controls Measures and Metrics [updated]
- SME Implementation Guide
- Companion Guides to the Controls [in development]
  - IOT, Cloud, Privacy, Outsourcing for Small/Medium Enterprises
- **CIS Risk Assessment Method (CIS-RAM)** [new]

CIS Center for Internet Security®

- Website: www.cisecurity.org
- Email: Controlsinfo@cisecurity.org
- Twitter: @CISecurity
- Facebook: Center for Internet Security
- LinkedIn Groups:
  - Center for Internet Security
  - 20 Critical Security Controls