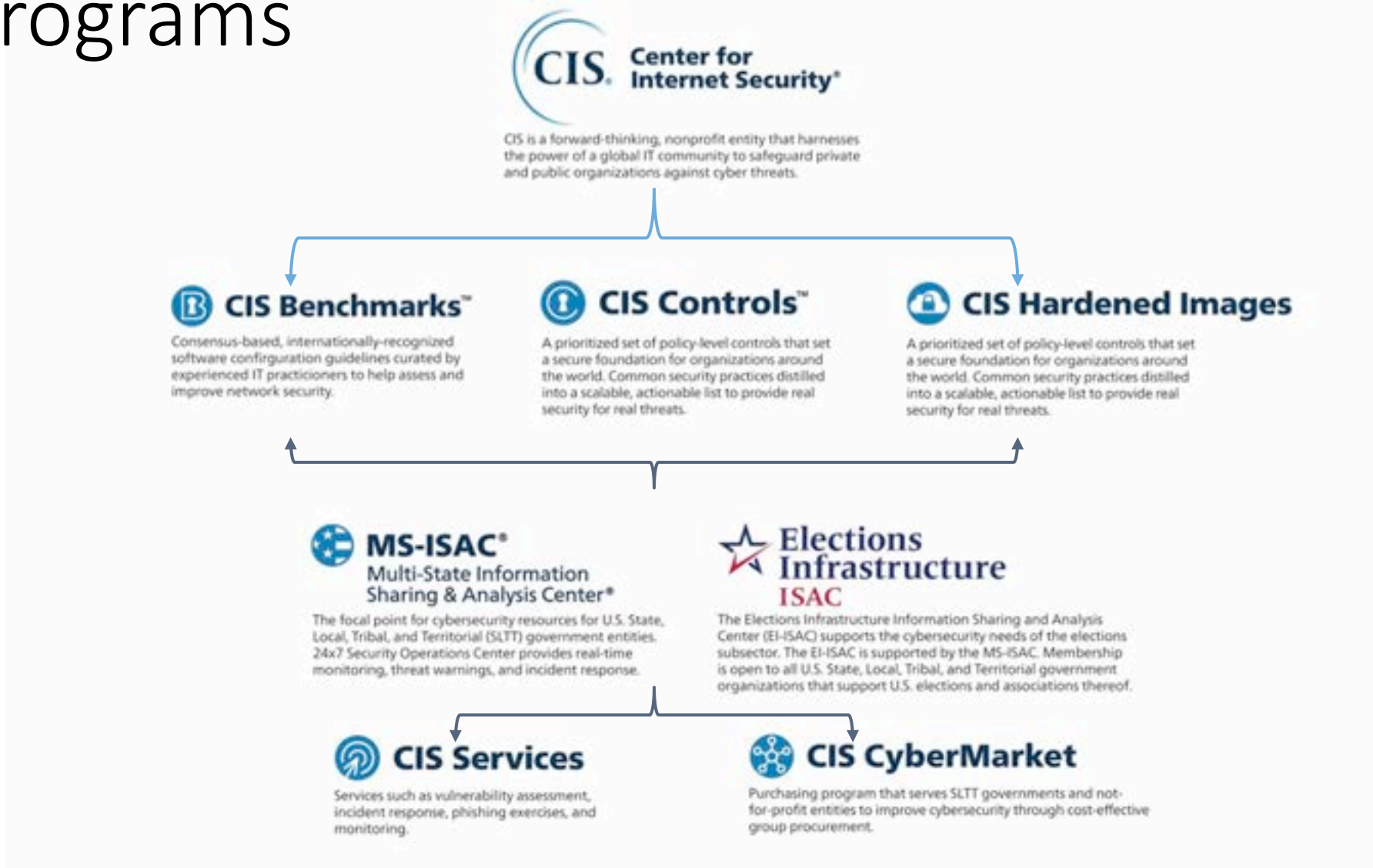
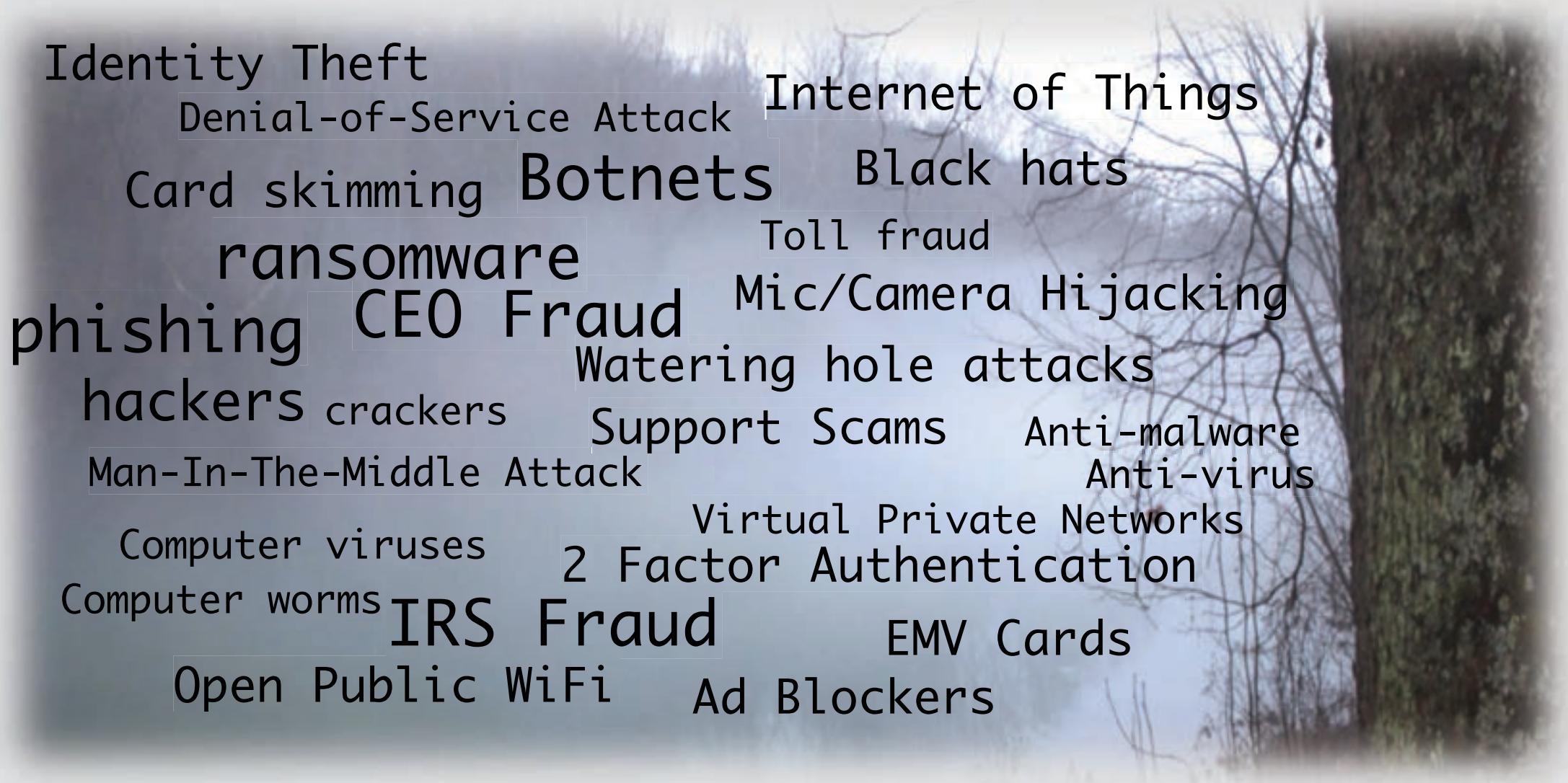
# Legislative Cyber Security Briefing Introduction

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

# CIS Programs



# "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"?

# The Cybersecurity Problem

- Every type of victim: country, sector, size, individual…
- Every motivation: financial and IP theft, extortion, social control, political statements, notoriety, influence operations, “false flags”, “prep of the battlespace”….
- Attackers are efficient: information sharing, automation, very large scaling, specialization, a marketplace… (4K ransomware attacks/day)
- threat of cyber a top 3  disruption (World Economic Forum)
- Cyber threats greater than physical threats (DHS Secretary Nielsen)
- Worldwide cybercrime costs $600B/year (McAfee, CSIS)
- Expect $100B in defensive spending in 2020 (IDC)
- *Y2K with real impact, and without the deadline*

# Small Businesses and Cyber

- 29 million small businesses - less than 500 employees (SBA)
- Over half of all attacks target them (NCSA, Symantec, DBIR, etc.)
- Over half of them report an attack or data breach in prior year
- Half have no budget allocated for risk mitigation
- Most of the data breaches are from small businesses (the Hill)
- Typical cost between $84k and $148K, 60% out-of-business 6 months later (UPS Capital)

| 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 |
| Almost all attacks are repeats of a type or class | Build a foundation before taking a “moonshot” |
| 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, non-profits, 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 |

# A DC-centric View

- Legislative
  - Sharing; “hygiene”; use of commercial standards
  - Privacy (encryption policy; commercial data gathering)
- Executive
  - Regulatory approaches
  - MS-ISAC
- Market Forces
  - Compliance, “Multi-Framework Era”
  - Supply Chain management
  - Alignment with existing risk-decision models in industry

# Some References

- Verizon Data Breach Incident Report:
  https://www.verizonenterprise.com/verizon-insights-lab/dbir/
- Center for Strategic & International Studies Cyber Incident List
  https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity
- National Academy of Sciences: At The Nexus of Cybersecurity and Public Policy
  https://www.nap.edu/catalog/18749/at-the-nexus-of-cybersecurity-and-public-policy-some-basic