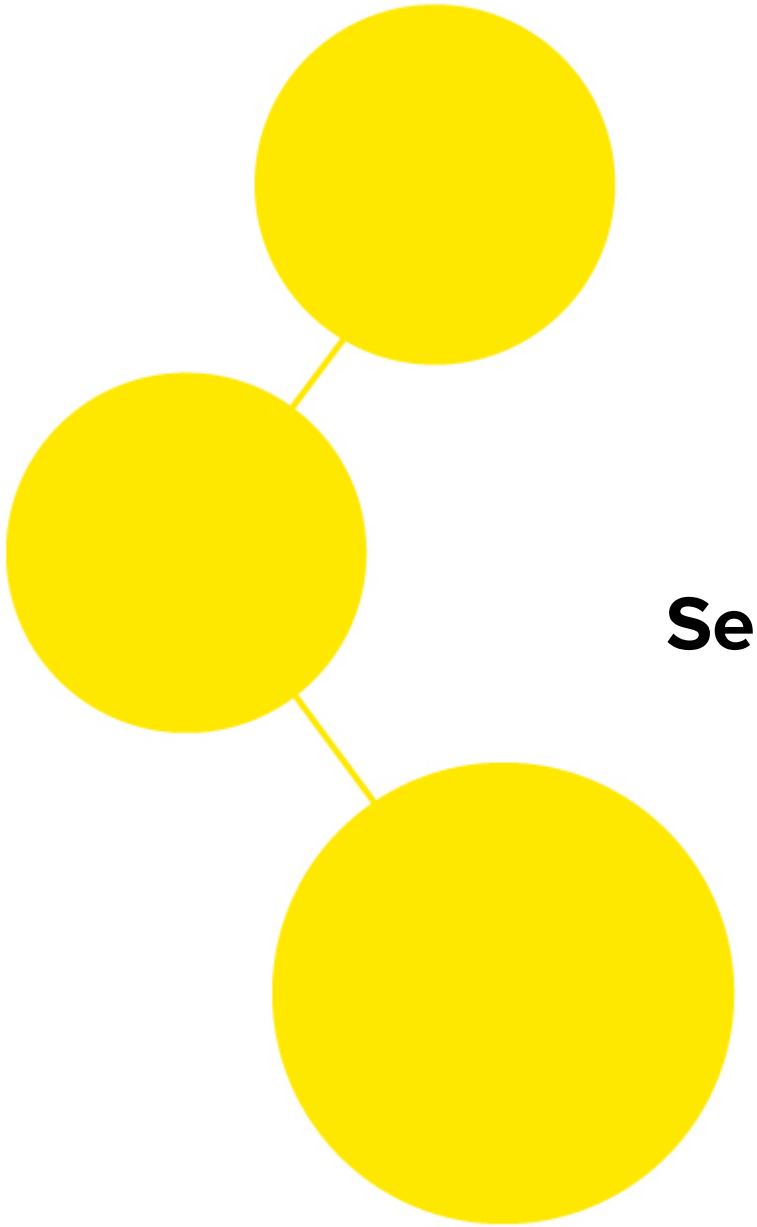


SECURENOK

Introduction to Securing Critical Infrastructure

Keith Frederick
CISSP, CAP, CRISC, Author

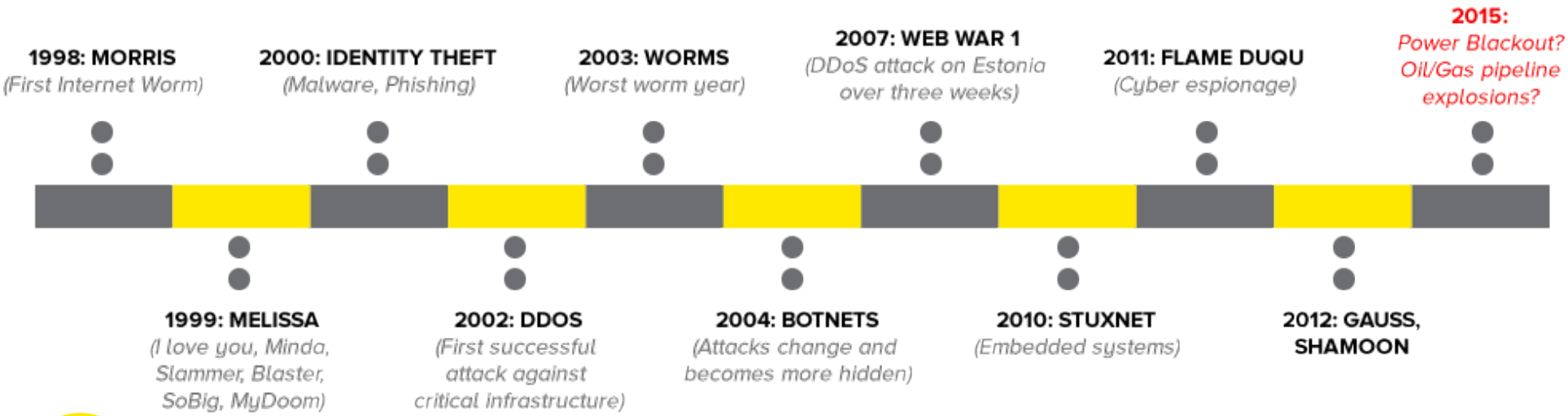
securenok.com

Topics

- Attacks on the Oil and Gas Industry.
- Executive Order 13636 (February 12, 2013).
- Presidential Directive 21 (February 12, 2013).
- Cybersecurity Framework (February 12, 2014).

SECURENOK

Evolution of Cyber Attacks



SECURENOK

Why the Focus on O&G?

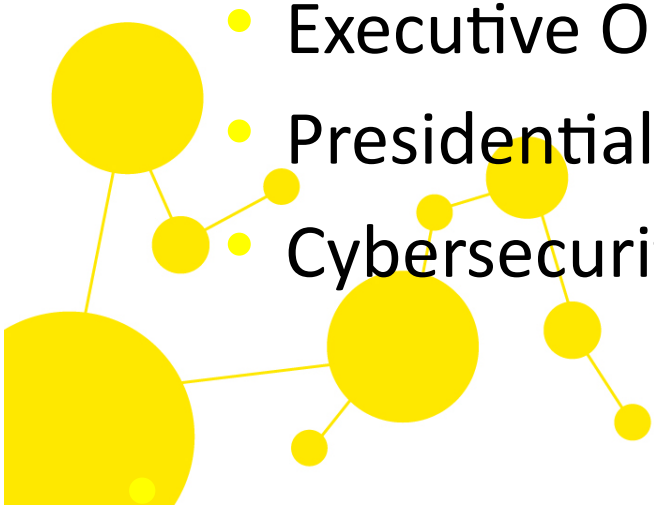
- Energy is fundamental to the nation's economy and defence and pervasive throughout critical infrastructure.
- Represents the political direction of the government and future war efforts aimed at country/corporate economics.

Hacker ability to take over "Control Systems".

SECURENOK

Threats to the Energy Industry

- In 2013, **53%** of attacks against the critical infrastructure in the United States targeted the "Energy Industry".
  - **Continues to increase annually.**
- Motivation behind:
  - Executive Order 13636,
  - Presidential Directive 21 (PD-21), and
  - Cybersecurity Framework (CSF).



SECURENOK

Executive Order 13636: Improving Critical Infrastructure Cybersecurity

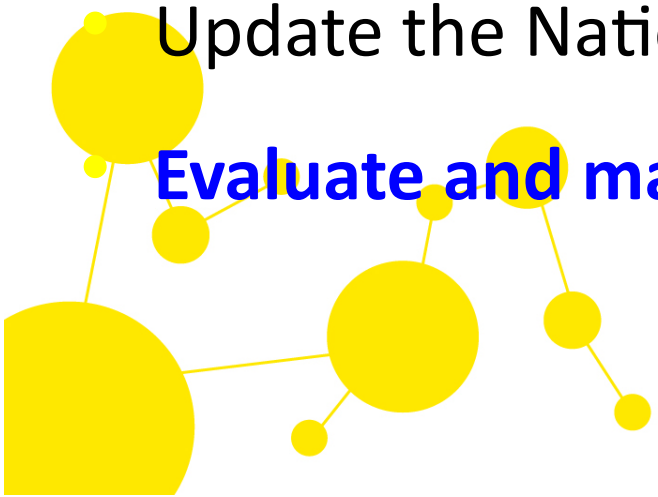
- Develop a technology-neutral voluntary cybersecurity framework.
- Promote and incentivize adoption of cybersecurity practices.
- Increase the volume, timeliness, and quality of cyber threat information sharing.

Explore the use of existing regulation to promote cyber security

SECURENOK

Presidential Policy Directive 21: Critical Infrastructure Security and Resilience

- Develop a situational awareness capability that addresses both physical and cyber aspects of how infrastructure is functioning in near-real time.
- Understand the cascading consequences of infrastructure failures.
- Update the National Infrastructure Protection Plan.
- **Evaluate and mature the public-private partnership.**



SECURENOK

Cybersecurity Framework (CSF)

- **The Cybersecurity Framework (CSF) is a living document and will continue to be updated.**
- The CSF uses risk management processes to enable organizations to inform and prioritize decisions regarding cybersecurity.
- It supports recurring risk assessments and validation of business drivers.

SECURENOK

CSF Overview

- CSF is a risk-based approach to managing cybersecurity risk, and is composed of three parts:
  - The CSF Core,
  - The CSF Implementation Tiers, and
  - The CSF Profiles.

Each CSF component reinforces the connection between business drivers and cybersecurity activities.

SECURENOK

CSF Core

- The CSF Core is a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors.
- The Core presents industry standards, guidelines, and practices in a manner that allows for communication of cybersecurity activities.

SECURENOK

CSF Core Chart

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

SECURENOK

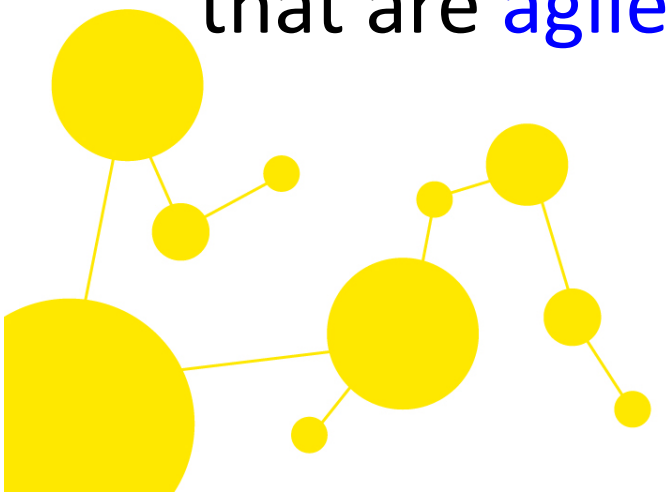
CSF Implementation Tiers

- "Tiers" provide context on how an organization views:
  - Cybersecurity risk and
  - The processes in place to manage that risk.
- Tiers describe the degree to which an organization's cybersecurity risk management practices exhibit.

SECURENOK

CSF Implementation Tiers

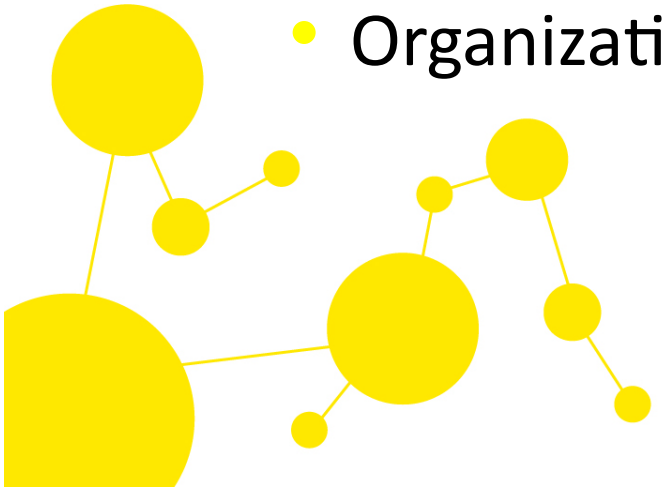
- The Tiers characterize an organization's practices over a range, from Partial (Tier 1) to Adaptive (Tier 4).
- These Tiers reflect a progression from informal, reactive responses to approaches that are agile and risk-informed.



SECURENOK

CSF Implementation Tiers (continue)

- An organization should consider its:
  - Current risk management practices,
  - Threat environment,
  - Legal and regulatory requirements,
  - Business/mission objectives, and
  - Organizational constraints.



SECURENOK

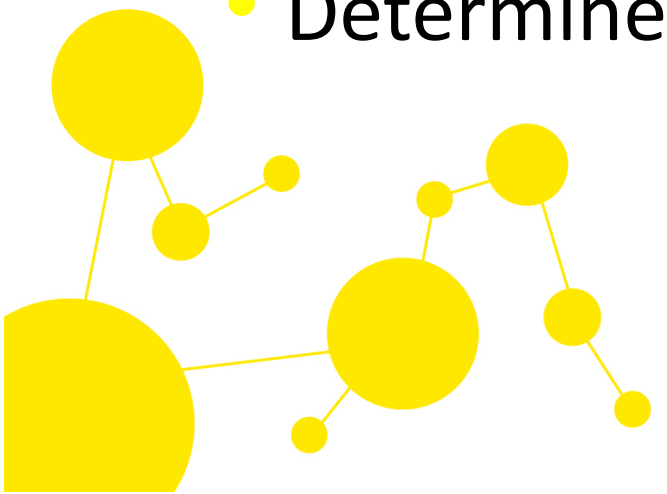
CSF Profiles

- A “Profile” represents the outcomes based on business needs that an organization has selected from the Framework:
  - Categories and
  - Subcategories.
- The Profile can be characterized as the alignment of:
  - Standards,
  - Guidelines, and
  - Practices

SECURENOK

CSF Profiles (continue)

- To develop a Profile,
  - An organization reviews all of the categories and subcategories and,
  - Based on **business drivers** and a **risk assessment**,
  - Determine which are most important.



SECURENOK

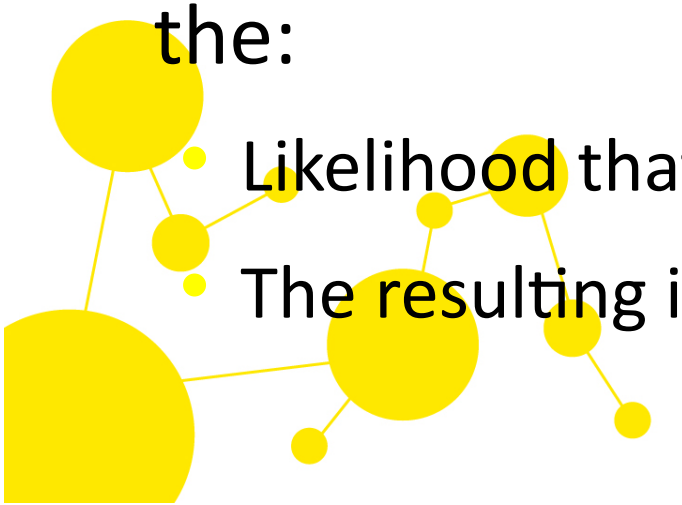
CSF Profiles (continue)

- Profiles can be used to identify opportunities for improving cybersecurity posture by comparing:
  - “Current” Profile (the “as is” state) with a
  - “Target” Profile (the “to be” state).

SECURENOK

Risk Management and the CSF

- Risk management is the ongoing process of:
  - Identifying,
  - Assessing, and
  - Responding to risk.
- To manage risk, organizations should understand the:
  - Likelihood that an event will occur and
  - The resulting impact.



SECURENOK