

The Future of Cybersecurity Policy

Prof. David Hoffman



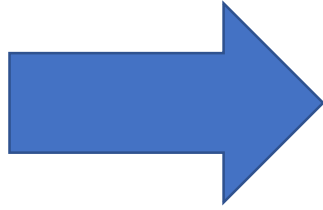


CYBER RISK MANAGEMENT FOR PORTS

Guidelines for
Cybersecurity
in the Maritime
Sector



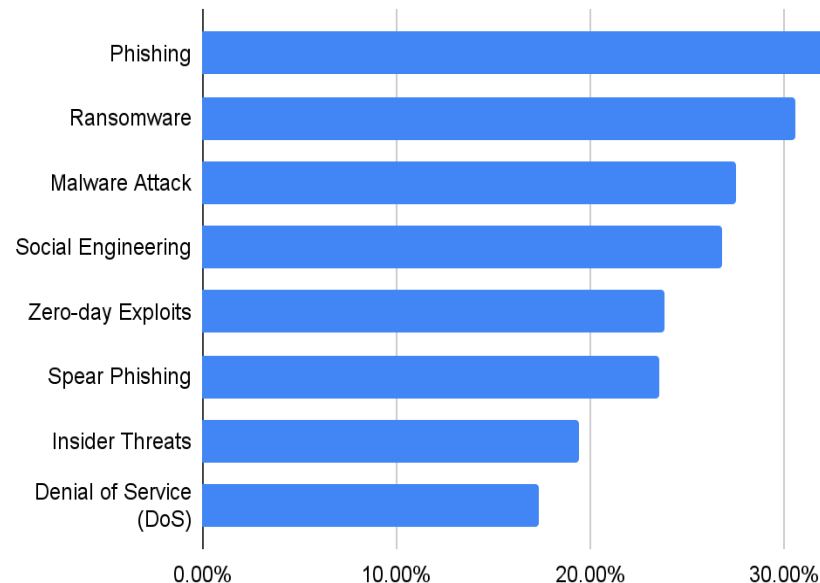




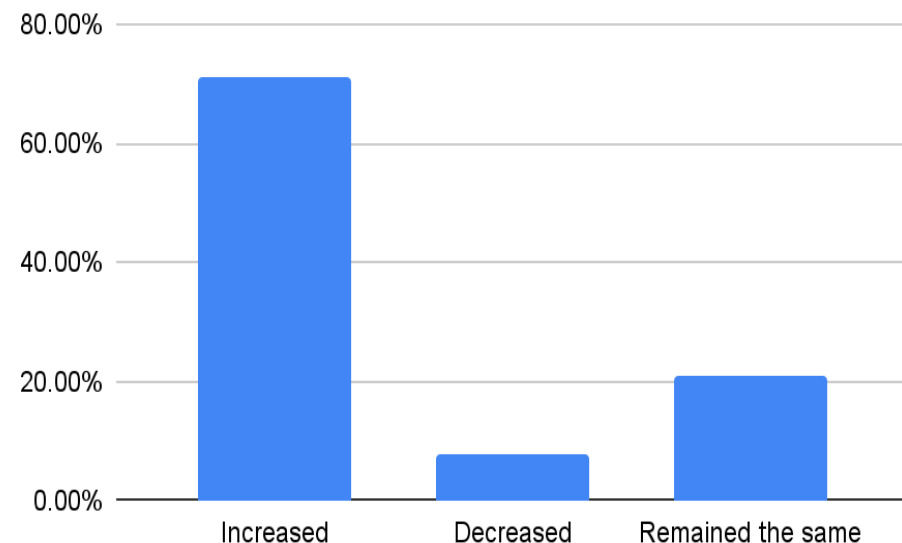
LATAM CISO Survey

- 195 organizations of different sectors and sizes
 - 21% (1-100 employees)
 - 24% (100-999 employees),
 - 56% (over 1,000 employees).
- The most heavily represented industries are Financial Services (24%), Government (23%), Professional Services (10%).

Q7. Most Common Types of Cyber Attacks



Q8. Change in Attacks Since Previous Year



The Costa Rica Experience

Attacks in early 2022 focused on the finance ministry, then Conti and Hive attacked over 27 government bodies including:

- The Administrative Board of the Electrical Service of the province of Cartago (Jasec)
- The Ministry of Science, Innovation, Technology and Telecommunications (MICITT)
- The Ministry of Labor and Social Security (MTSS)
- The National Meteorological Institute (IMN)
- Radiographic Costarricense (Rasca)
- The Interuniversity Headquarters of Alajuela
- The Social Development and Family Allowances Fund (FODESAF)
- Costa Rican Social Security Fund (CCSS)



Immediate effects

- The unprecedented scope and severity of the attacks caused the first 2-3 weeks to be filled with confusion on how to respond.
- On May 8th, 2022 Rodrigo Chaves Robles started his four year term as president and immediately **declared a “national emergency”**
 - Stated that 9 of the 27 targeted bodies were “very affected”
 - The President said that the country was **“at war, and that is not an overstatement”** (in a country with no army since 1949)
- Private sector losses (customs) of up to \$38 million per day
- International trade effectively stopped
- Thousands of medical appointments and surgeries rescheduled
- Disruption of tax payments

Lessons Learned

Plan in advance for impact to critical infrastructure

Coordinate between civilian and military agencies

Have in place disaster recovery plans

Have a coordination structure between government and the private sector

CIA

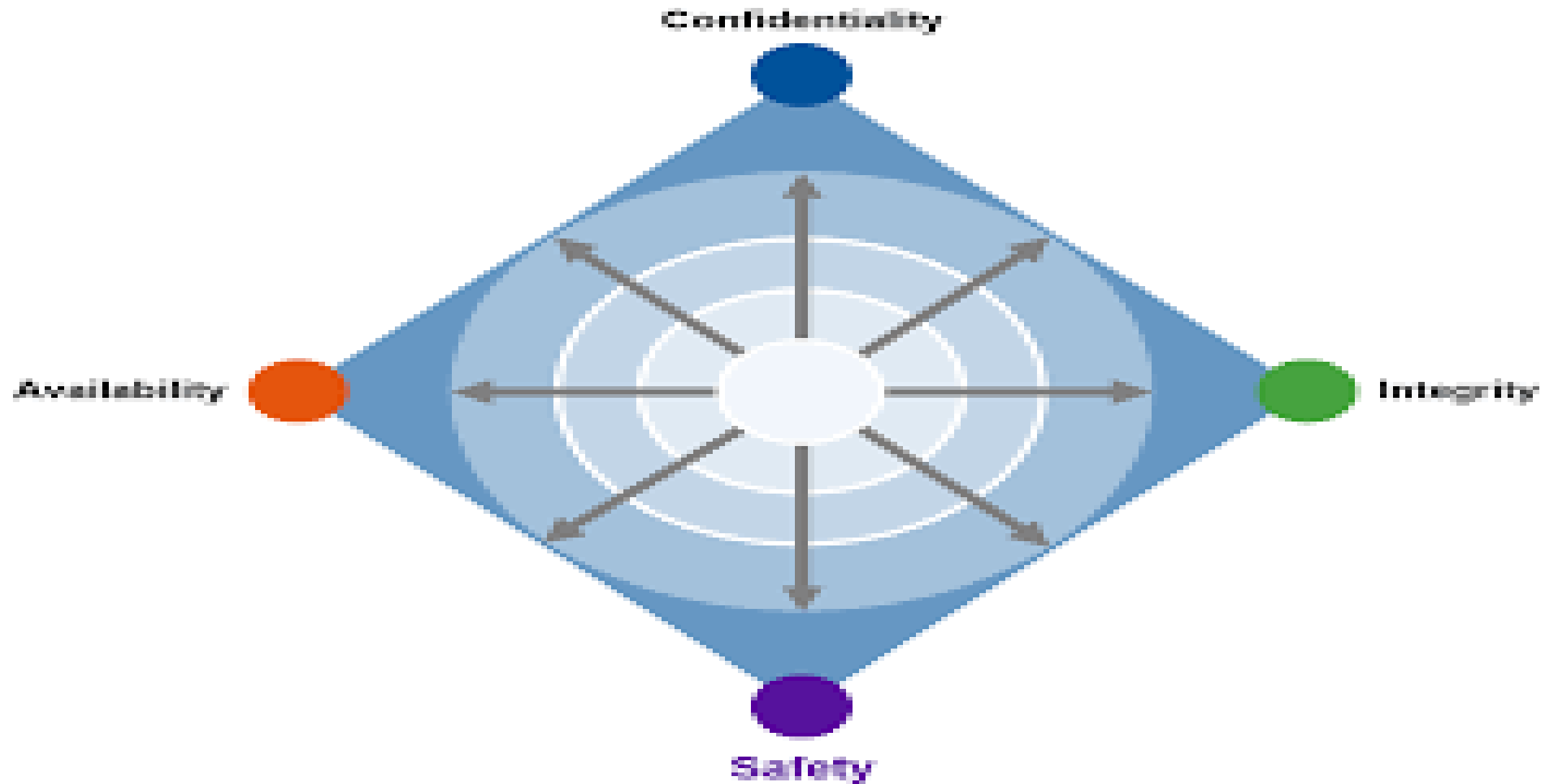


The Old Policy Approach

Blame the Victim



CIAS



Supply Chain



Zeroday for Internet

Apache

LOG4J



Ransomware



The New Policy Approach

Better Coordination Between Government Agencies

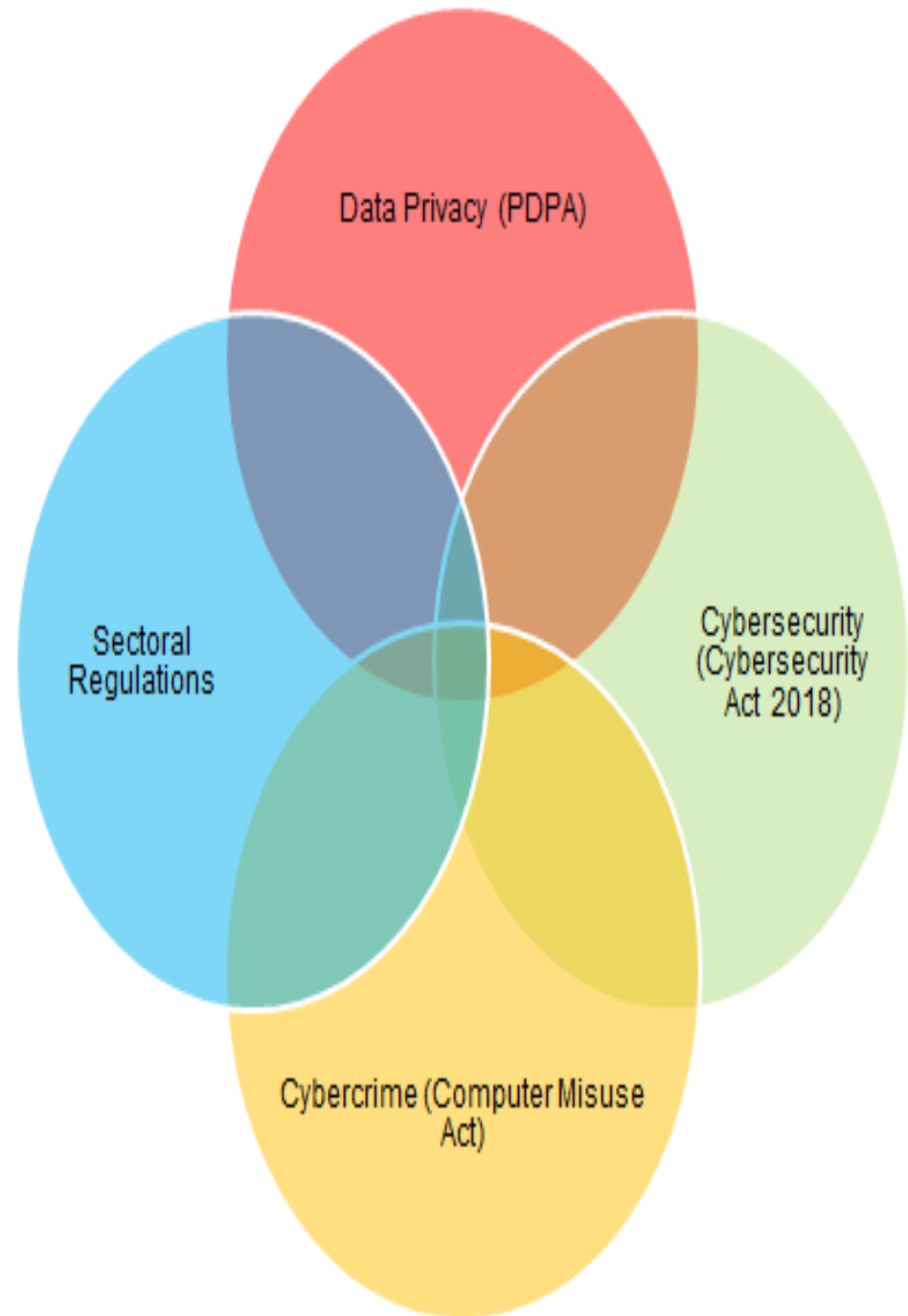
Collaboration Between Government and Industry

Focus on Critical Infrastructure

Evaluate Trustworthiness of Hardware and Software

Risk Management Regulation and Enforcement





Cybersecurity Act of 2018

1. **Appoint a Cybersecurity Commissioner**

- Power of investigation
- Power to require remediation
- Power to appoint Assistant Commissioner “sector leads”

2. **Secure Critical Infrastructure (CI)**

- Obligations on private and public owners of CI
- Focus on the technology used in 11 Sectors (Energy, Info-communications, Water, Healthcare, Finance, Public Security, Aviation, Land Transport, Maritime, Government, Media).

3. **License Cybersecurity Service Providers**





Created in 2021

NCSA focused on critical infrastructure and use of a framework for **assessment of hardware and software used in critical infrastructure systems.**

2021 – 60 CI organizations

2022 – 120 CI organizations





National Cyber Security Centre

a part of GCHQ

- distils cybersecurity knowledge into practical guidance that we make available to all
- responds to cyber security incidents to reduce harm
- uses industry and academic expertise to nurture the UK's cyber security capability
- reduces risks to the UK by securing public and private sector networks

The Three Rs – Relationships, Resources, Responses

Relationships

- Cyber-security Information Sharing Partnership (CiSP)
- UK's Industry 100
- Critical National Infrastructure (CNI)
- Bridge between government agencies and corporations

Resources

- Educational training and information for individuals, small businesses, and large organizations
- Financial support for organizations that cannot invest in cybersecurity

Advice & guidance

All topics

All articles

All topics

Find a list of the broad range of cyber security related topics that our advice and guidance covers.

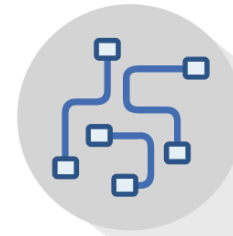
46 topics



Access control



Active Cyber Defence



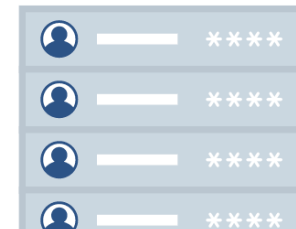
Artificial intelligence



Asset management



Authentication



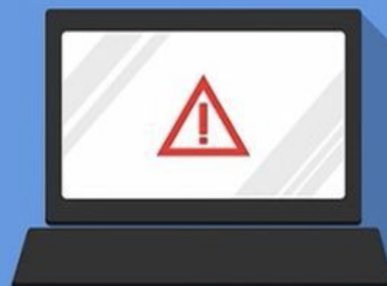
Bulk data



NEWS

NCSC advises organisations to act following Russia's attack on Ukraine

Organisations should follow NCSC advice and take action to improve their resilience with the cyber threat heightened.



 [Download / Print Article PDF](#)

 [Share](#)

PUBLISHED

3 March 2022

NEWS TYPE

General news

WRITTEN FOR

[Small & medium sized organisations](#)



Education & skills

[Schools](#)[Higher
education](#)[Professional
skills & training](#)[Working with the
NCSC](#)[CyBOK](#)[Research &
academia](#)

Cyber Security for Schools

Practical resources to help schools improve their cyber security.



ON THIS PAGE



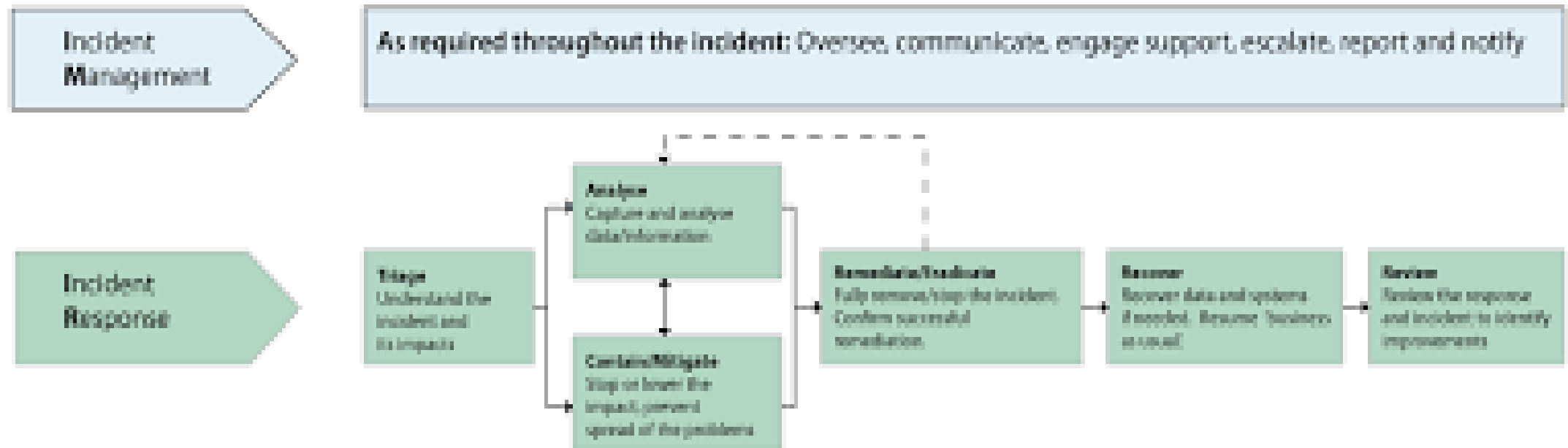
Cyber security training for school staff

The NCSC has produced a training package for school staff to help improve cyber security.

[Find out more](#)

Responses

- Incident Management
- Technological Support



Policy Formulation

NCSC Coordination and Advice

- Bringing together
 - relationships,
 - resources,
 - and responses
 - To help lawmakers inform policy
-





UNITED STATES OF AMERICA
**CYBERSPACE
SOLARIUM
COMMISSION**

CO-CHAIRMEN

Senator Angus King (I-Maine)

Representative Mike Gallagher (R-Wisconsin)


MARCH 2020

**RANSOMWARE
TASK FORCE** 

Combating Ransomware

*A Comprehensive Framework for Action:
Key Recommendations from the
Ransomware Task Force*

Presented by the Institute for Security and Technology

 **IST** INSTITUTE FOR SECURITY & TECHNOLOGY



Office of the National Cyber Director

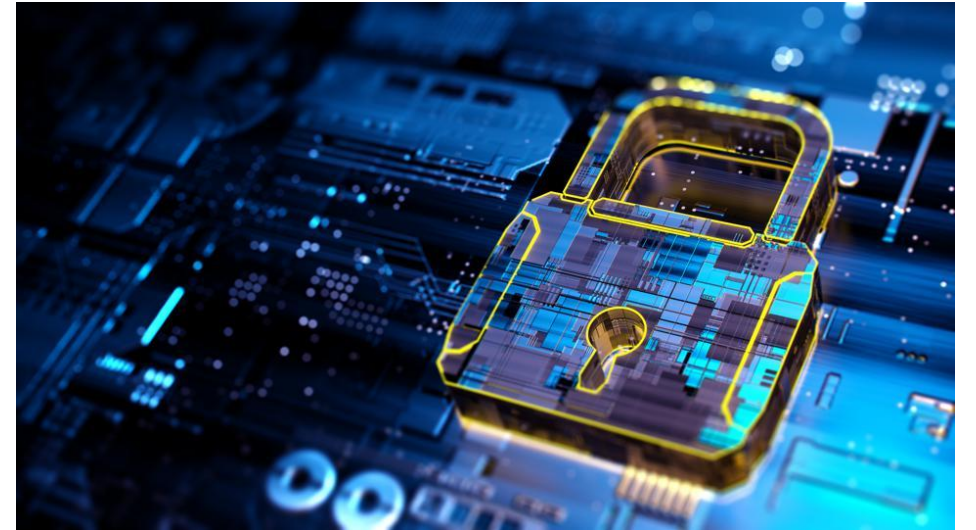


- Special Advisor to the President
- Informal communication (Walden, Easterly, Neuberger)



Protecting Critical Infrastructure

- Risk-informed, all-hazards approach
- Coordination with agencies and private sector partners to share information on cyber threats and vulnerabilities
- Cyber and physical security are core aspects of risk management strategies



Protecting Critical Infrastructure: DHS CISA and the NSA



- CISA Central 24/7 situational awareness, analysis, and incident response center
- NSA opens the Cybersecurity Collaboration Center to work with the private sector
- CISA does not want to be a regulator but companies should be incentivized to report cyber attacks
 - Potential legislation could be a fine for companies that fail to disclose attacks
- CISA relies on public private partnership for information



Information Sharing and Awareness

- Development and implementation of information sharing programs
- The private sector owns and operates a majority of the nation's critical infrastructure
- Goal: fostering strong partnerships with substantial information sharing with no regulation



Risk Management

- What is risk management?
- How do leaders manage risk outside of their area of expertise?
- Where do risk management best practices come from?
- Is risk management in cybersecurity unique?

Risk Management in Cybersecurity and Privacy

- NIST describes risk management as...
 - “The program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and includes: (i) establishing the context for risk-related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time”

Policy Approach of the Future

Less emphasis on:

- Vague technical requirements
- Blaming the victim
- Fines

More emphasis on:

- Protection of government systems
- Collaboration with critical infrastructure operators and suppliers
- Government assistance to organizations that need to invest
- Multinational threat and vulnerability information sharing
- Focus on risk management and preparation for recovery