The Office of the National Coordinator for Health Information Technology

Cybersecurity: A Cyber Publication Study and Update

2017 HIPAA Summit

Malikah Smith, PMP, CISSP, CAP,
OCPO Security Branch Chief

Agenda

- A Review of Industry/Government Cybersecurity Reports
- Common Themes Found in the Cybersecurity Reports
- ONC Security and Cybersecurity Activities
- On the Horizon

Cybersecurity Reports

Report Name	Author	Commissioner	Release Date
Commission on Enhancing National Cybersecurity: Report on Securing and Growing the Digital Economy	National Institute for Standards and Technology (NIST)	President of the United States	December 1, 2016
Healthcare Information and Management Systems Society (HIMSS) Cybersecurity Position Statement	HIMSS	HIMSS	September 30, 2016
Joint Analysis Report (JAR)-16-20296A – Grizzly Steppe	Department of Homeland Security (DHS) and Federal Bureau of Investigation (FBI)	DHS and FBI	December 29, 2016

Cybersecurity Commission Report

- Commission established by Executive Order 13718 and charged with making detailed cybersecurity recommendations:

> "The Commission will make detailed recommendations to strengthen cybersecurity in both the public and private sectors while protecting privacy, ensuring public safety and economic and national security, fostering discovery and development of new technical solutions, and bolstering partnerships between Federal, State, and local government and the private sector in the development, promotion, and use of cybersecurity technologies, policies, and best practices."

COMMISSION ON ENHANCING NATIONAL CYBERSECURITY

DECEMBER 1, 2016

REPORT ON SECURING AND GROWING THE DIGITAL ECONOMY

Cybersecurity Commission Report, cont'd

- Expert input from:
  - National Institute for Standards and Technology (NIST)
  - Department of Homeland Security (DHS)
  - Department of Defense (DoD)
  - U.S. Department of Justice
  - General Services Administration (GSA)
  - U.S. Department of the Treasury
  - Public Contributors (1,100 comments)

Commission Recommendations – ONC Interest

- Incent the sharing of threat information, and how to act on such information, through public/private collaboration (Recommendation 1.2, starts at p. 14)
- Increase the use of strong identity authentication (Recommendation 1.3, starts at p. 16)
- Develop concrete efforts to support small- and medium-sized businesses (Recommendation 1.5, starts at p. 21)

Commission Recommendations, cont’d

- General Cybersecurity
  - » Improve consumer awareness of cybersecurity in managing their own affairs
  - » Impose cybersecurity standards by agency rulemaking when appropriate
  - » Expand qualified cybersecurity workforce
  - » Improve government management of data assets and procurement, including a more influential role for the Office of Management and Budget (OMB), using Enterprise Risk Management techniques
  - » Collaborate internationally

HIMSS Cybersecurity Position Statement

- HIMSS and cyber experts from various sectors outlined a position statement to encourage a robust cybersecurity future state
- Three key recommendations for U.S. Department of Health and Human Services (HHS):
  - » Adopt a universal information privacy and security framework for the health sector
  - » Create an HHS cyber leader role (an elevated chief information security officer)
  - » Address shortage of qualified cybersecurity professionals

HIMSS Cybersecurity Position Statement
Approved by the HNA Board of Directors
September 30, 2016

HIMSS North America

The Health Sector is the Target.

Due to persistent and pervasive cyber-attacks, the health sector's understanding, approach, and sense of urgency around cybersecurity has significantly changed. Previously, the

DHS/FBI JAR on Grizzly Steppe

- Provides technical details regarding the tools and infrastructure used by the Russian civilian and military intelligence services (RIS) to compromise and exploit networks and endpoints associated with a range of U.S. Government, political, and private sector entities
- Refers to this malicious RIS cyber activity as “Grizzly Steppe”

JAR Recommendations

- Recommended Mitigations – Cybersecurity Best Practices
  - » Data Backups
  - » Risk Analysis and Remediation
  - » Staff Training
  - » Vulnerability Scanning and Patching
  - » Application Whitelisting
  - » Incident Response
  - » Business Continuity Planning
  - » Penetration Testing

TLP:WHITE

NCCIC

Federal Bureau of Investigation

JOINT ANALYSIS REPORT

DISCLAIMER: This report is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service referenced in this advisory or otherwise. This document is distributed as ***TLP:WHITE:*** *Subject to standard copyright rules,* ***TLP:WHITE*** *information may be distributed without restriction. For more informa*

Reference Number: JAR-16

GRIZZLY STEPPE – I

Summary

This Joint Analysis Report (JAR
Homeland Security (DHS) and t
provides technical details regard
military intelligence Services (R
associated with the U.S. election
sector entities. The U.S. Govern
GRIZZLY STEPPE.

Previous JARs have not attribut
However, public attribution of th
the U.S. Intelligence Communit
determination expands upon the
of Homeland Security and the D

This activity by RIS is part of an
U.S. government and its citizens
targeting government organizati
political organizations, and corp
RIS actors conducted damaging
infrastructure networks. In some
false online personas designed t
JAR provides technical indicato
suggested actions to take in resp
report such incidents to the U.S.

1 of 13

TLP:WHITE

Description

The U.S. Government confirms that two different RIS actors participated in the intrusion into a U.S. political party. The first actor group, known as Advanced Persistent Threat (APT) 29, entered into the party's systems in summer 2015, while the second, known as APT28, entered in spring 2016.

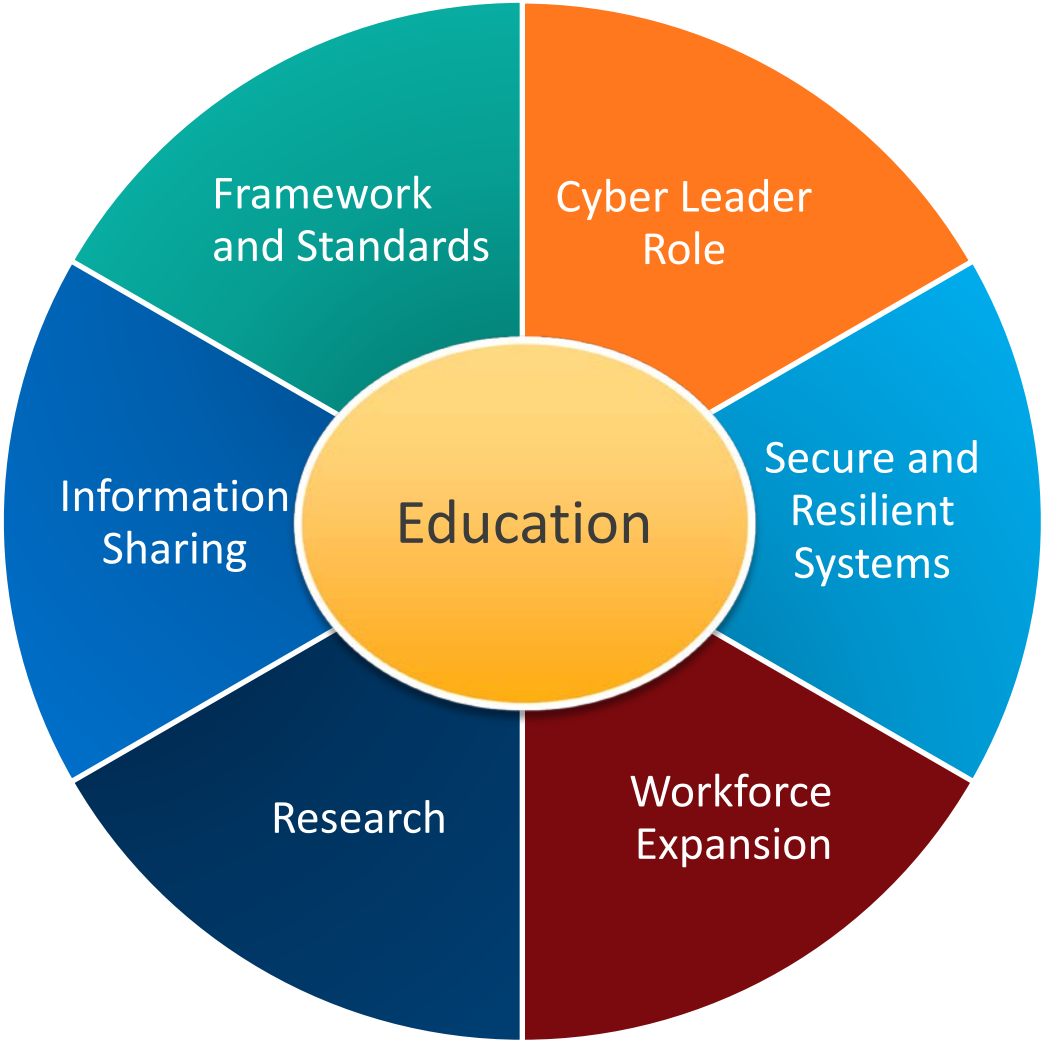
Figure 1: The tactics and techniques used by APT29 and APT 28 to conduct cyber intrusions against target systems

Both groups have historically targeted government organizations, think tanks, universities, and corporations around the world. APT29 has been observed crafting targeted spearphishing campaigns leveraging web links to a malicious dropper; once executed, the code delivers Remote Access Tools (RATs) and evades detection using a range of techniques. APT28 is known for leveraging domains that closely mimic those of targeted organizations and tricking potential victims into entering legitimate credentials. APT28 actors relied heavily on shortened URLs in their spearphishing email campaigns. Once APT28 and APT29 have access to victims, both groups exfiltrate and analyze information to gain intelligence value. These groups use this information to craft highly targeted spearphishing campaigns. These actors set up operational infrastructure to obfuscate their source infrastructure, host domains and malware for targeting organizations, establish command and control nodes, and harvest credentials and other valuable information from their targets.

In summer 2015, an APT29 spearphishing campaign directed emails containing a malicious link to over 1,000 recipients, including multiple U.S. Government victims. APT29 used legitimate

2 of 13 TLP:WHITE

Publication Common Themes



Framework and Standards

Cyber Leader Role

Information Sharing

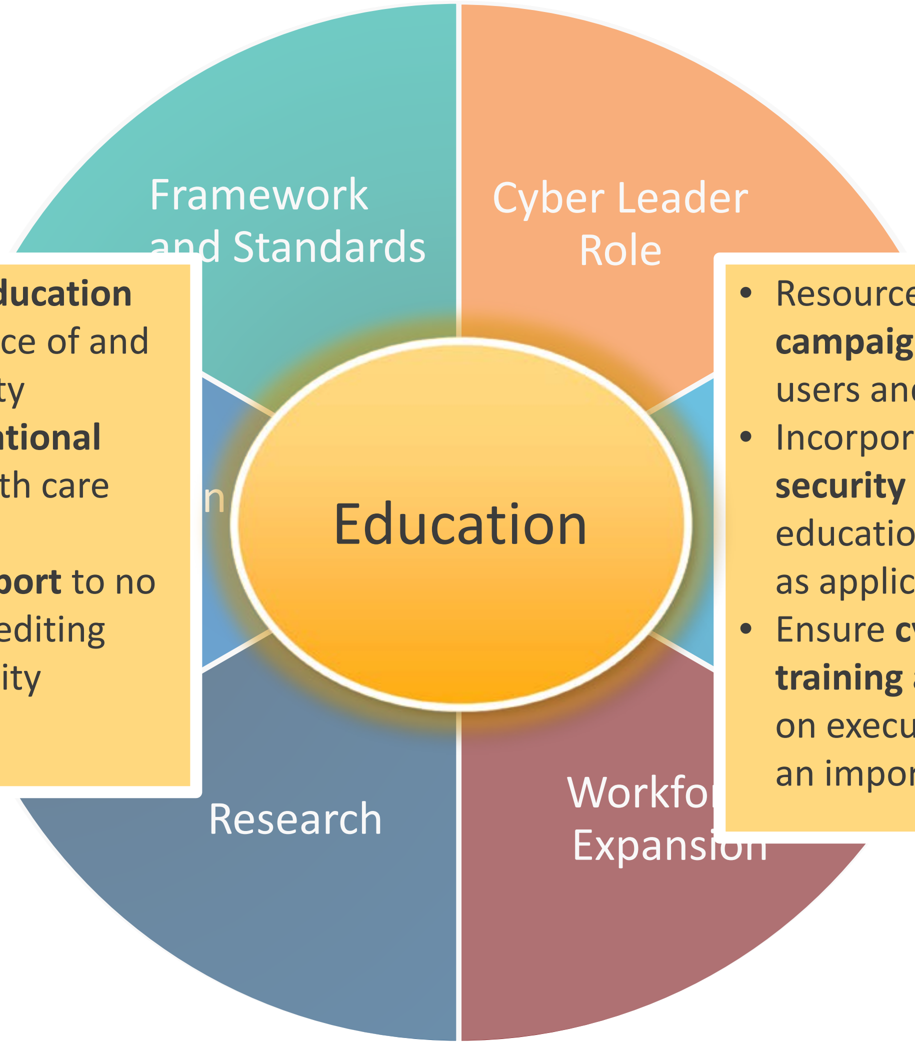
Education

Secure and Resilient Systems

Research

Workforce Expansion

Publication Common Themes, cont’d



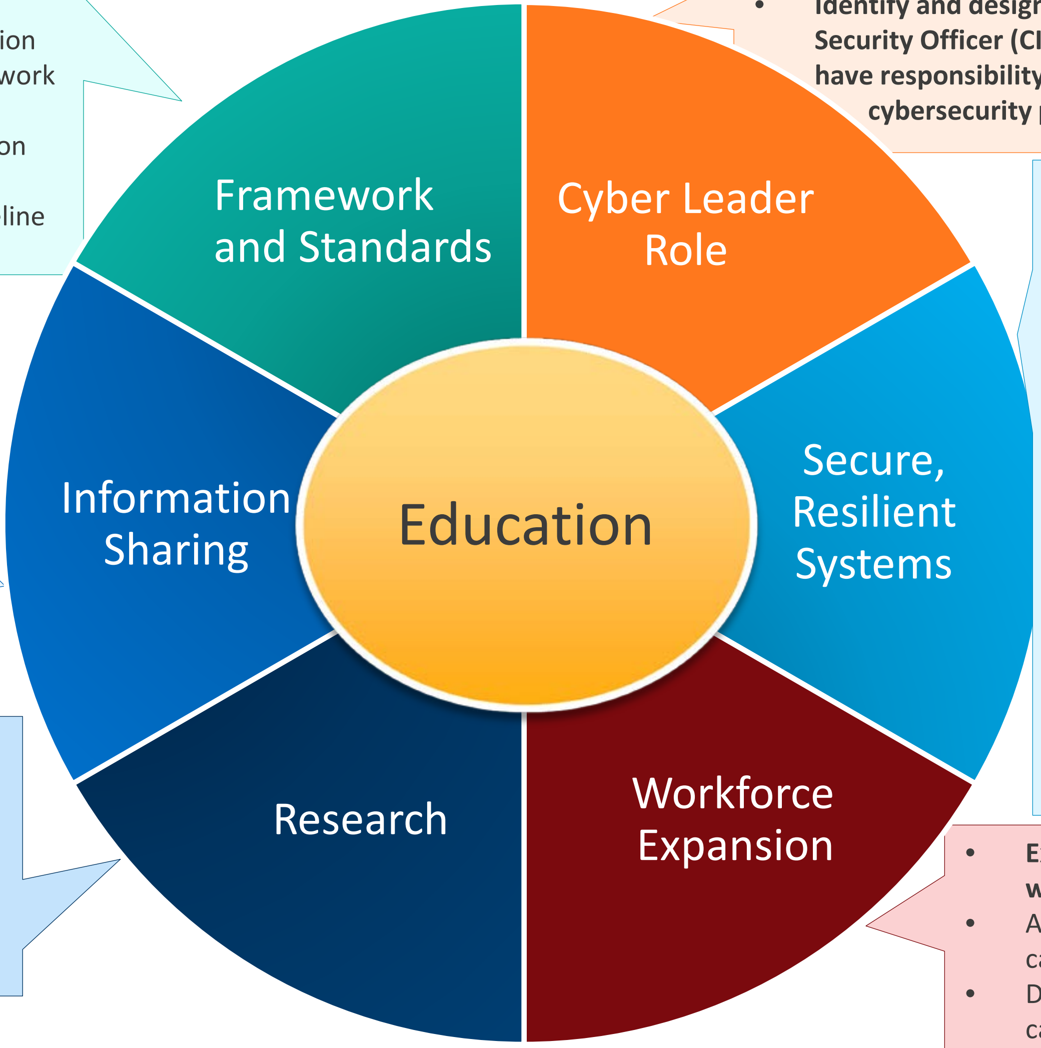
- Improve **consumer education**
- Increase the prevalence of and access to cybersecurity **awareness and educational programs** across health care sector stakeholders
- Provide **financial support** to no more than three accrediting bodies for cybersecurity education

- Resource an **ongoing education campaign** addressing both end users and the boardroom
- Incorporate **privacy and security training** into all patient education modules or courses, as applicable
- Ensure **cyber workforce training** and education focuses on executive communication as an important goal

Publication Common Themes, cont’d

- **Leverage NIST Cybersecurity Framework**
- Adopt a universal information privacy and security framework for the health sector
- Establish a new accreditation framework to support the cybersecurity hygiene baseline

- Create an HHS cyber leader role
- **Identify and designate a Chief Information Security Officer (CISO)/security leader who will have responsibility for and authority over HHS cybersecurity program**



- **Incent the sharing of threat information, and how to act on such information, through public/private collaboration**

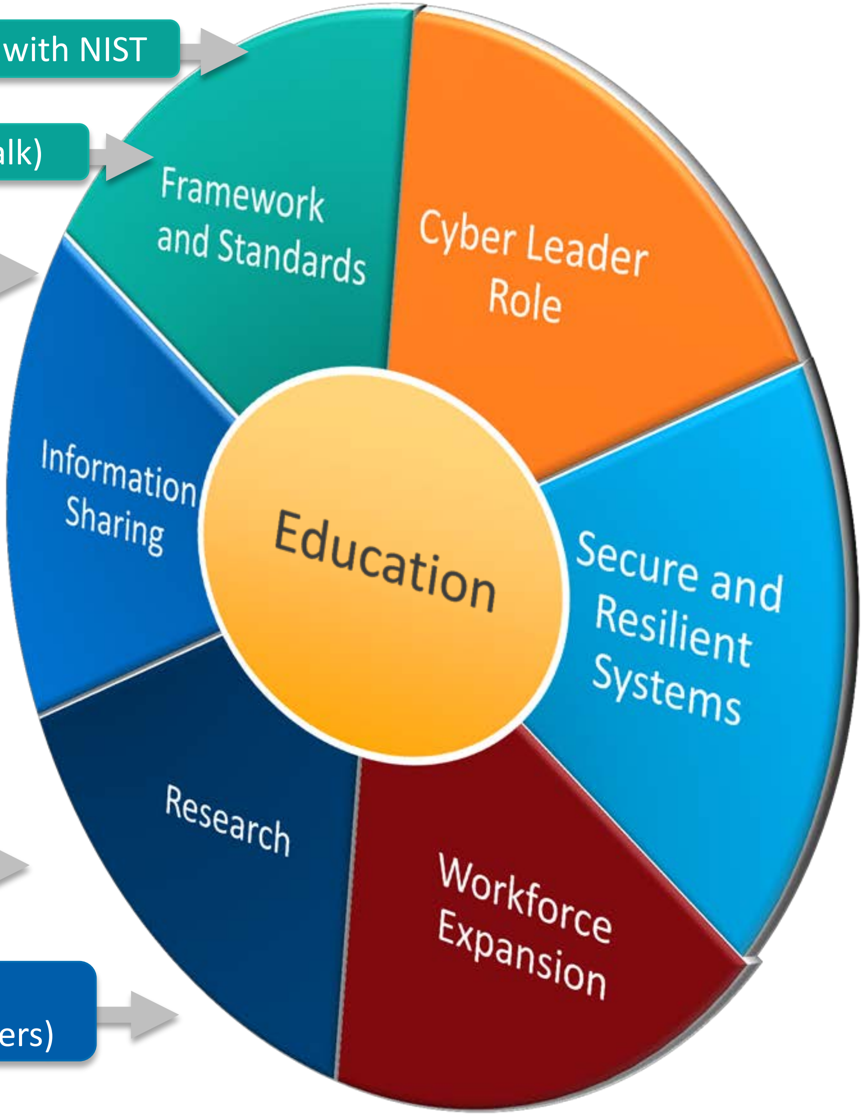
- Incentivize the development and adoption of secure operating systems for medical devices and Internet of Things (IoT)
- **Secure legacy systems and incentivize the replacement of legacy technology with newer secure alternatives**
- Use funding to remove unsecure devices from the U.S. marketplace and provide partial funding for more effective and more secure current technologies

- Establish, strengthen, and broaden investments in research programs to improve the **cybersecurity and usability of consumer products and digital technologies**

- **Expand qualified cybersecurity workforce**
- Address workforce gaps through capacity building
- Develop workforce within health care necessary to prioritize cybersecurity awareness and technical capabilities.

ONC/OCPO Security and Cybersecurity Activities – Hitting the Mark

- Identity Management – Federated Identity Framework with NIST
- Interagency Cybersecurity Efforts (e.g., NIST-HIPAA Crosswalk)
- Privacy and Security of APIs – Education and Outreach
- SRA Tool (iOS update)
- Ethical Hacking Landscape Analysis
- CISA Task Force
- Health IT Playbook
- PMI Support (e.g., PMI Security Principles Implementation Guide)
- ISAO Initiative (CHIME, HIMSS, AHA connections to disseminate general cyberthreat info with their members)



On the Horizon for ONC/OCPO

Unified Approach to Cybersecurity

Enhanced SRA Tool
(incorporating NIST Cybersecurity Framework)

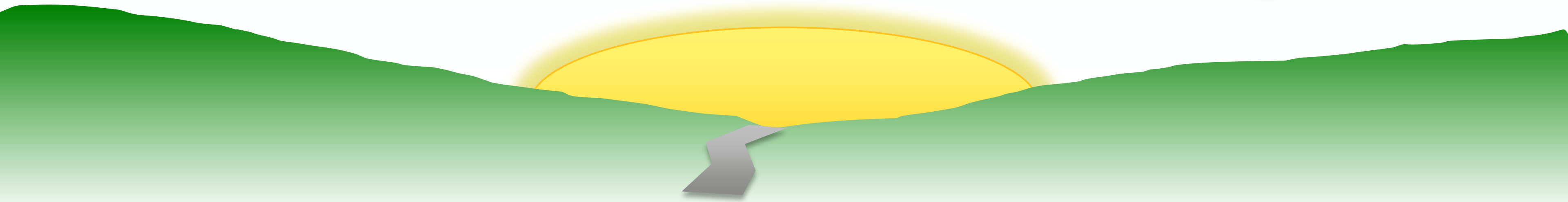
CISA Task Force Report

Best Practice Guidance on Federated Identities

Trusted Exchange Framework

API Education Tool

ISAO – Expanding Cyberthreat Information-Sharing Reach



Key ONC/OCPO Resources

- Guide to Privacy and Security of Electronic Health Information
- Mobile Health Apps Interactive Tool
- Patient Access Videos
- API Task Force Recommendations
- Report to Congress on Non-Covered Entities
- Security Risk Assessment Tool (Updated)
- National Governors Association (NGA) Interoperability Roadmap for States
- Health IT Playbook
- Privacy and Security Training Games
- Privacy and Security Technology Learning Collaborative
  - » PrivacyandSecurityTLC@hhs.gov

Identify
Assess
Manage
Safeguard
Guide to Privacy and Security of Electronic Health Information
ACCESS =
See and get copies of your health information
Introduction
Introduction to the Health IT Playbook

The Office of the National Coordinator for
Health Information Technology

Questions?

Mikki Smith, PMP, CISSP, CAP
Office of the Chief Privacy Officer (OCPO)
Office of the National Coordinator for Health Information Technology (ONC)
U.S. Department of Health and Human Services (HHS)
Malikah.Smith@hhs.gov

@ONC_HealthIT @HHSONC HealthIT.gov