Cyber Branch

Introduction Brief

23 July 2020

Presented by: Bill Larsen

Mike Del Pozzo

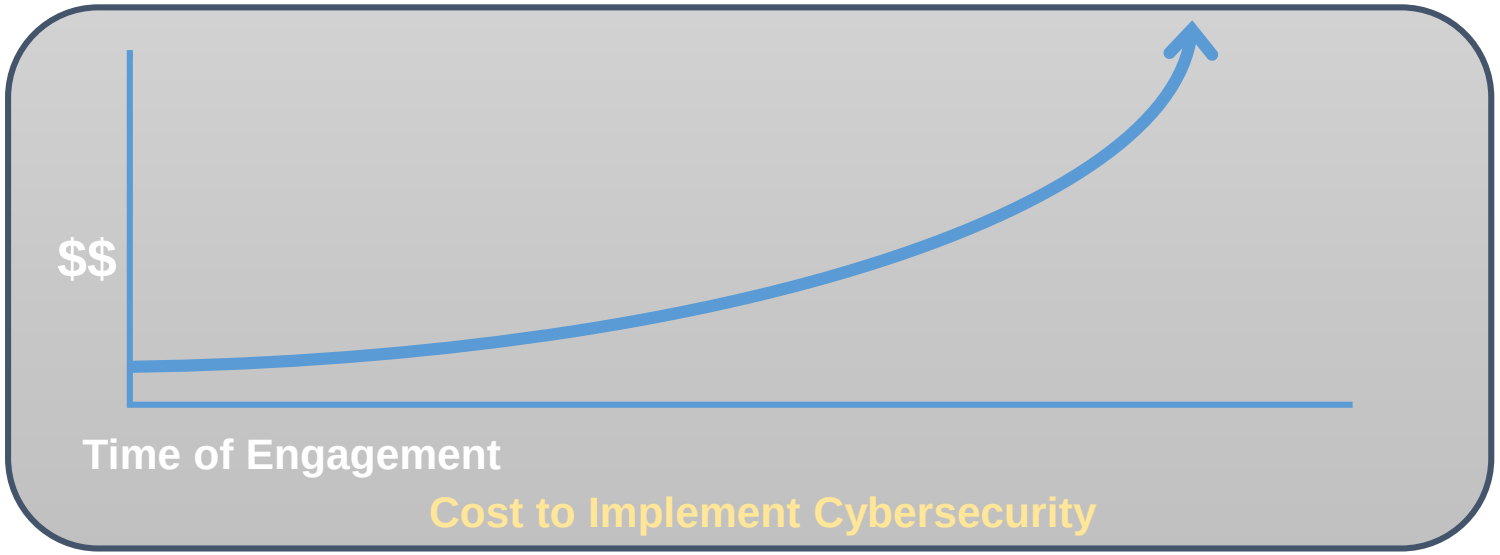
Dan Collins

V 0.1

Authorization Support

Cyber Branch Goals

- The goal of Cyber is to secure systems and reduce the Navy's overall threat exposure
  - Obtaining an authorization (ATOs and IATTs) is a validation of this process; however, ATOs are not the ultimate end-goal
- Cybersecurity engagement must occur early in development
  - Significantly reduces the lifecycle costs of producing a secure system



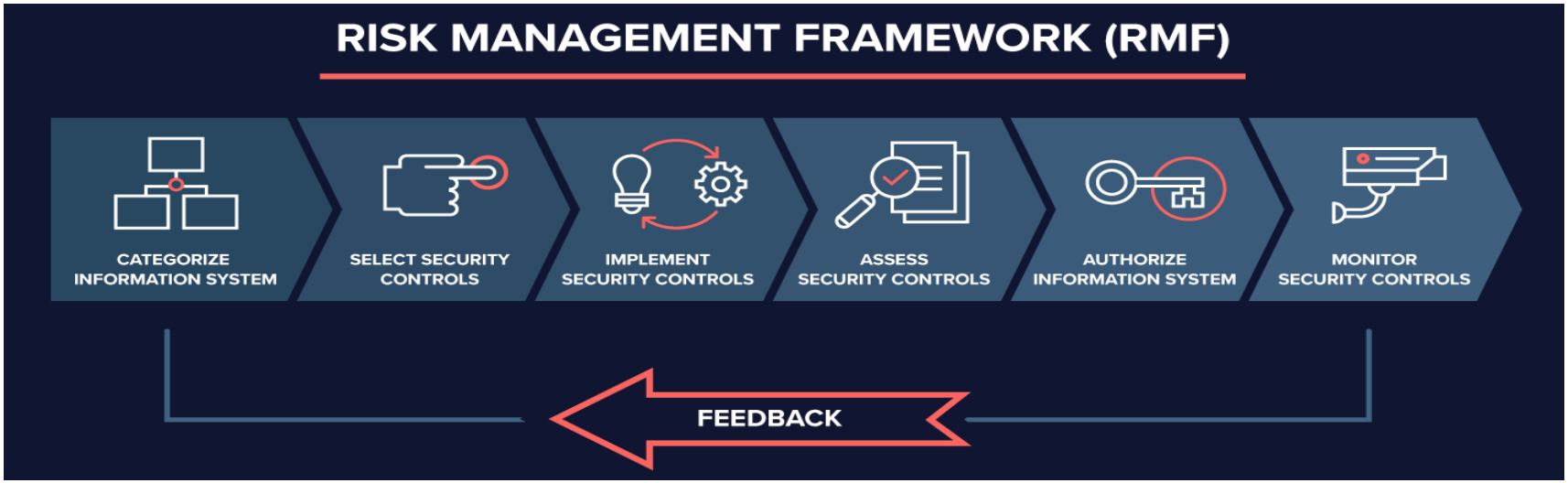
Cybersecurity is not just about being complaint with policy; it's about securing the tools and assets the NAVY relies on every day

ALRE & SE Authorization Support

Largest % of work/support within the Cyber Branch

- Provide qualified and certified cybersecurity workforce professionals to serve as Information System Security Officers (ISSO's)

- Carry out the DoD Risk Management Framework (RMF), a six-step lifecycle process, used to obtain and maintain the **Authority to Operate (ATO)** within the Enterprise Mission Assurance Support Service (eMASS) which is the tool/application where all assessment and authorization (A&A) information and documentation resides



ALRE & SE Authorization Level of Effort

ALRE Authorization Cyber Team consists of:

- 6 personnel
  (2 Government & 4 Contractors)
- Support 19 systems

SE Authorization Cyber Team consists of:

- 8 personnel
  (3 Government & 5 Contractors)
- Support 32 systems

Lakehurst ISSM Support

- **Lakehurst Information System Security Manager (ISSM) Site Lead:**
  - For enforcing Cybersecurity Policies, Cybersecurity Compliance, Assessment and Authorization, and Technical Countermeasures as a means to reduce risks in view of the exponential growth we've witnessed in the threat environment. Ensure all NAWCAD Lakehurst systems, networks, and users are in compliance with Department of Navy and Department of Defense Cybersecurity Directives.
- **NMCI Account Management (NIPR / SIPR)**
- **RDT&E Assessment and Authorization (A&A)**
- **Cybersecurity Workforce (CSWF) Management**
  - CSWF Training and Certification
  - Position Designation and Investigation Compliance
- **Computer Network Defense (CND)**
  - OPORD / EXORD / FRAGORD / TASKORD Compliance and Implementation
- **Security Incident Handling and Reporting**
  - Electronic Spillage Handling
  - IA Violations / User Counseling
  - Lost / Stolen IT

Where we need to go…

Electronic patching

- Background: The Navy continually faces a challenged network to deliver information safely and efficiently. Software security updates are needed to prevent cyberattacks on Navy systems
- Purpose: Improve the software security posture by expediting the delivery and process of applying software updates
- Current state: We currently use time consuming manual processes for security updates (takes weeks)
- End state: With an electronic process, a security update can quickly occur and deliver a report back (could take minutes)

Pentesting

Pentest Team Overview

- Penetration testing is a real-world style “attack” on a system in a controlled environment with the intention of verifying/validating security vulnerabilities
- Pentesting presents a more realistic view of a system’s risk posture by providing ‘proven out’ vulnerability assessments, as opposed to scanning-based assessments
- By viewing systems from an attacker’s point-of-view, Pentesting provides a better assessment of how systems will respond to actual attacks. This helps:
  - Assess system attack detection mechanisms, as well as resiliency mechanisms to react to attacks
  - Assess true risk from known vulnerabilities
  - Detect vulnerabilities that arise from how a system is used, which may not be detected by scanning alone

Recent Pentest Highlights

- The Lakehurst Pentest Team competed in the DAU Capture the Flag (CTF) event on 13 May 2020. CTF events consist of a series of challenges that vary in their degree of difficulty, and that require participants to exercise various pentest skillsets to solve. Lakehurst took 2nd place with 2,810 points.
- The Lakehurst Pentest Team competed in CTF Event #4 hosted by the National Cyber Range from 16-17 January 2020. Lakehurst scored first place of the session, capturing 6 of 9 primary flags and 10 of 11 bonus flags.
- Performed a penetration test against LSODS Mod 1 (ECP 345) in December 2019. Feedback and recommendations were made for inclusion in a future ECP.
- Participated in USS SECURE Serial VIII event from 19-30 August 2019, in the new ALRE Technology Integration Center (A-TIC). The test was specific to the ALRE components representing the CVN-78 shipboard systems consisting of: AAG, ADMACS, EMALS, IFLOLS, and MWS. The team's findings provided detailed explanations to offer insights, opportunities, and security recommendations to significantly improve the ALRE security posture

Cyber R&D

Cyber R&D Mission

- Perform cutting-edge research (R&D) into novel solutions to address immediate Navy cybersecurity issues
- Rapidly transition solutions to aircraft programs
- Serve as a single point of research and development for technologies applicable to multiple program offices
- Respond to rapidly-evolving requirements from across NAVAIR
- Coordinate efforts with colleagues in other Services and other parts of the Navy

Current Capabilities

- 1 Lab in Patuxent River, MD
  - Standing up Lab in Lakehurst, NJ
- 12 personnel
  - Various backgrounds
  - Computer science, electrical engineering, diagnostics
- Current project areas:
  - Blockchain
  - Data bus security
  - Cyber resiliency
  - Software Assurance
- Future project areas of interest:
  - AI and Machine Learning
  - Supply Chain Risk Management

Questions?