Brookhaven National Laboratory

U.S. DEPARTMENT OF ENERGY

Cyber Security at BNL

Ian Ballantyne, CISO

March 2024

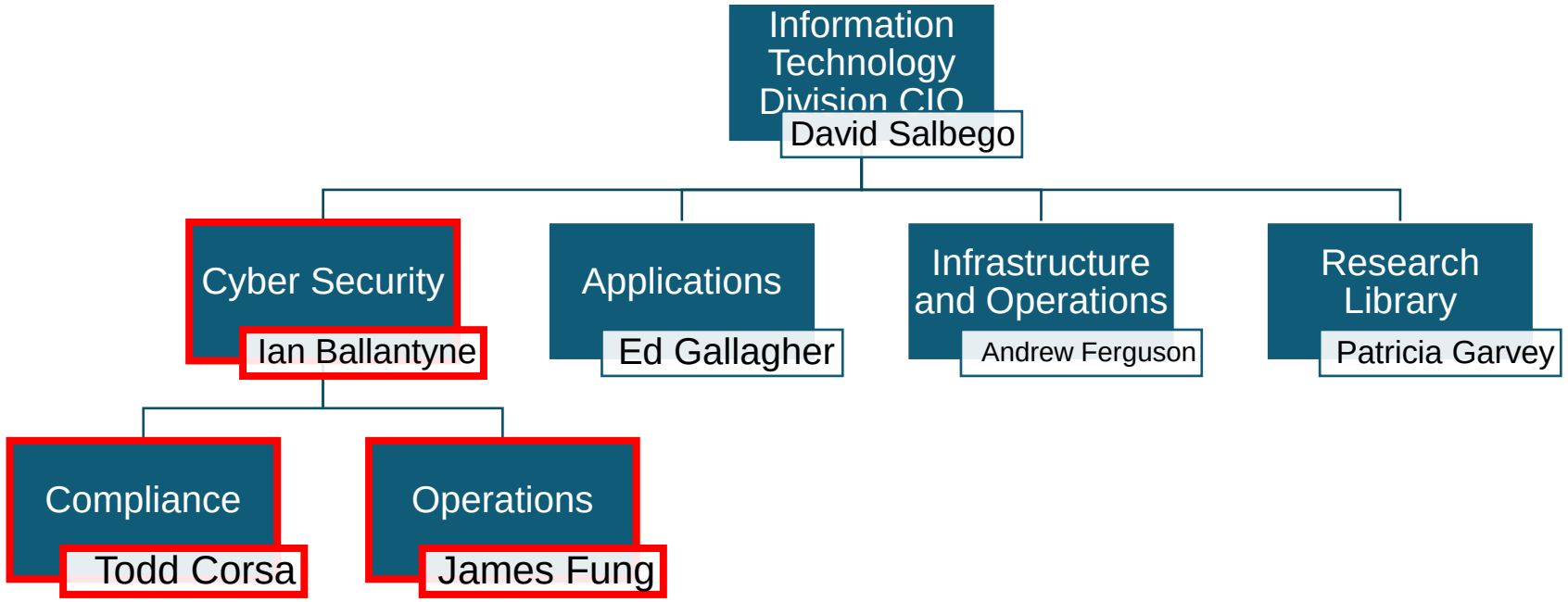
@BrookhavenLab

Agenda

- Cyber Organization
- Regulatory Environment
- Threat environment
- Operational environment
- Responsibilities
- Outcomes

Cyber Organization

Cyber Organization



Cyber Organization

- ~14 FTEs
- ~$8M annual budget (IT)
- Primarily direct funded by DOE Office of Science ~90%

Regulatory/Compliance Environment

Regulatory/Compliance Environment

Federal

- Federal Information Security Management Act
- Executive Orders/Binding Operational Directives
- National Institute of Standards and Technology (NIST) Risk Management Framework
- NIST SP 800-53
- NIST Cyber Security Framework
- Site office Authorizing Official Oversight
- Inspector General/General Accounting Office Audits

DOE

- Orders (205.1)
- Office of Science Cyber Security Program Plan
- Audits

BNL

- Institutional Risk Management Council
- Audit Committee
- BNL Internal Audit

Threat Environment

$10.5 trillion

The cost of cybercrime is projected to hit an annual $10.5 trillion by 2025.[1]

USD 4.45 million

The global average cost of a data breach in 2023 was USD 4.45 million, a 15% increase over 3 years.

Ransomware attacks increase in sophistication and speed.
$1 billion in payments collected in 2023.
Avg payout $1.54 million in 2023

Threat levels are at unprecedented heights, with the number of publicly reported ransomware attacks up by more than 50% and breached data records more than doubling in the first eight months of this year. At current rates, 2023 will be the worst year on record, far exceeding 2021 levels, when ransomware came to the forefront after a series of high-profile events

CISO Research reveals 90% of organizations suffered at least one Major Cyber Attack in the Last Year; 83% of those impacted by ransomware reported making ransomware payments

Password-based and Multifactor Authentication (MFA) fatigue attacks skyrocket

Caesars Entertainment Pays $15 Million Ransom to Cyber-Hackers after Breach

Casino giant MGM expects $100 million hit from hack that led to data breach

Johnson Controls Ransomware Attack Could Impact DHS

Hawai'i's Gemini North observatory suspends operations following cyberattack

Clorox reports production issues after August cyberattack

Mattress giant Tempur Sealy hit with cyberattack forcing system shutdown

University of Michigan shuts down network after cyberattack

Russian hackers accessed Microsoft source code

New technique leads to largest Distributed Denial of Service attacks ever, Google and Amazon say

Henry Schein ransom saga now in third month, hackers show no mercy
December 13, 2023

Henry Schein, a global leader in healthcare technology and product distribution, is still struggling to restore business operations since it announced the ransomware attack on its company website on October 15th.

School cyber incidents on Long Island: Reported cases rose sharply in 2023

Island schools reported 35 cyber incidents last year, a bump of 52% from 23 in the prior year.

Suffolk County Ransomware Attack Sept 2022

So far, the ransomware incident has cost Suffolk County $5.4 million for investigation and restoration, and $12 million for new hardware and software.

German Light Source Cyber Attack

On Thursday 15 June 2023 Helmholtz-Zentrum Berlin was victim of a cyber attack. For protection we have shut down all IT systems. The research centre cannot be reached via the website, email or telephone at the moment. We ask for your understanding.

Operational Environment

Trends and external forces

Increasing Information Technology (IT)/Operational Technology(OT) and cyber mandates

- Zero Trust
- IPv6

Hybrid and mobile workforce

- Bring your own device (BYOD)
- Convenience vs increasing security requirements

Challenges

- Steady stream of mandates some of which are not funded
- Decentralization of IT
- Difficulty in hiring and retaining staff
- Increasing pace of change across IT industry e.g. Artificial Intelligence and Quantum

Cyber Responsibilities

Cyber Program Functions (CSF)

- **Identify**
  - Data and assets that need to be protected, threats and vulnerabilities, risk threshold
- **Protect**
  - Deploy security controls and ensure effectiveness
- **Detect**
  - Monitor for control failure
- **Respond**
  - React quickly to attacks to minimize damage
- **Recover**
  - Restore operations

Cyber Responsibilities

Confidentiality
Integrity
Availability

Policy/Compliance

- Cyber Security Program Plan and cyber policy development
- Cyber Risk management
- Assessment of security controls
- Cyber security training and awareness
- Cloud approvals

Operations

- Incident Response
- Detection engineering
- Email secure gateways
- Central Logging
- Firewall rule management
- Endpoint detection and response

Cyber Outcomes

Cyber Outcomes

- Low number of reportable incidents and low impact to mission
- Cyber security is an important consideration in planning new projects and involved earlier rather than later
- Cyber security program balances mission and security outcomes and requires widespread BNL team effort
- Cyber security is an emergent property that comes from how we design, build and maintain our IT infrastructure

Thank you!

Personal Cyber Safety

https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/basics
https://www.cisa.gov/news-events/news/4-things-you-can-do-keep-yourself-cyber-safe