Journal of Cybersecurity and Privacy

MDPI

Article

Cybersecurity in a Large-Scale Research Facility—One Institution's Approach

David S. Butcher [1,*], Christian J. Brigham [2], James Berhalter [1], Abigail L. Centers [1], William M. Hunkapiller [2], Timothy P. Murphy [1], Eric C. Palm [1] and Julia H. Smith [1,*]

[1] National High Magnetic Field Laboratory, 1800 E. Paul Dirac Drive, Tallahassee, FL 32310, USA
[2] Information Security and Privacy Office, Florida State University, 1721 W. Paul Dirac Dr., Tallahassee, FL 32310, USA
* Correspondence: dbutcher@magnet.fsu.edu (D.S.B.); jsmith@magnet.fsu.edu (J.H.S.)

Abstract: A cybersecurity approach for a large-scale user facility is presented—utilizing the National High Magnetic Field Laboratory (NHMFL) at Florida State University (FSU) as an example. The NHMFL provides access to the highest magnetic fields for scientific research teams from a range of disciplines. The unique challenges of cybersecurity at a widely accessible user facility are showcased, and relevant cybersecurity frameworks for the complex needs of a user facility with industrial-style equipment and hazards are discussed, along with the approach for risk identification and management, which determine cybersecurity requirements and priorities. Essential differences between information technology and research technology are identified, along with unique requirements and constraints. The need to plan for the introduction of new technology and manage legacy technologies with long usage lifecycles is identified in the context of implementing cybersecurity controls rooted in pragmatic decisions to avoid hindering research activities while enabling secure practices, which includes FAIR (findable, accessible, interoperable, and reusable) and open data management principles. The NHMFL's approach to FAIR data management is presented. Critical success factors include obtaining resources to implement and maintain necessary security protocols, interdisciplinary and diverse skill sets, phased implementation, and shared allocation of NHMFL and FSU responsibilities.

Keywords: cybersecurity; user facility; FAIR data; open access; release of stored energy; cyberattack; major research facility; data theft; data breach; confidentiality; integrity; availability; data repository

Citation: Butcher, D.S.; Brigham, C.J.; Berhalter, J.; Centers, A.L.; Hunkapiller, W.M.; Murphy, T.P.; Palm, E.C.; Smith, J.H. Cybersecurity in a Large-Scale Research Facility—One Institution's Approach. *J. Cybersecur. Priv.* **2023**, *3*, 191–208. https://doi.org/10.3390/jcp3020011

Academic Editors: Leandros Maglaras, Helge Janicke and Mohamed Amine Ferrag

Received: 31 March 2023
Revised: 28 April 2023
Accepted: 7 May 2023
Published: 16 May 2023

1. Introduction

The National High Magnetic Field Laboratory (NHMFL) is a scientific user facility funded by the National Science Foundation (NSF) and the State of Florida [1,2]. The NHMFL's mission is to provide the highest magnetic fields and related services for scientific research conducted by domestic and international users from a wide range of disciplines, including physics, chemistry, materials science, engineering, biology, and geology. The NHMFL mission translates into four major areas of focus: first, the development and operation of user facilities and services for magnet-related research, which is open to all qualified scientists and engineers via competitive proposal programs. Second, the advancement of magnet technology in cooperation with industry. Third, promoting a multidisciplinary research environment, which is also reflected by in-house research programs that use and advance the user facility infrastructure and scientific setups. Fourth, the development of an educational outreach program.

In practice, the NHMFL's mission is focused on the operation and advancement of seven user facilities across three sites. Florida State University (FSU) in Tallahassee, FL, houses the DC Field Facility (strongest, quietest steady magnetic fields), the Electron Magnetic Resonance Facility, the Ion Cyclotron Resonance Facility, and the Nuclear Magnetic Resonance Facility; the University of Florida in Gainesville, FL, hosts the High B/T Facility (experiments at the extremes of high magnetic fields and low temperature) and the

Advanced Magnetic Resonance Imaging and Spectroscopy Facility; finally, Los Alamos National Laboratory (LANL) in Los Alamos, NM, hosts the Pulsed Field Facility. In 2021, the NHMFL supported the high magnetic field research of more than 1600 users from hundreds of universities, government labs, and private companies from all over the world visiting the laboratory's facilities or participating remotely [3].

The success of the NHMFL's mission in providing the highest quality magnetic field research to the (inter)national scientific community relies on the availability of world-class magnets, the input of excellent and innovative staff, as well as reliable and high-performance equipment. This level of facility performance requires a high level of operational uptime. This requirement, among other factors in the realm of reliability, availability, and maintainability, relies on a high-level yet practicable cybersecurity approach.

This article outlines one such cybersecurity approach for a large-scale user facility where major anticipated attack vectors are denial-of-service (possibly via ransomware or malware attacks), code injections, masquerades, authentication hijacking, or compromised single-board computing systems that could lead to compromised controls or monitoring capabilities of large-scale equipment, respectively. In addition, data theft represents a threat to the facility-generated FAIR data.

In Section 1, we use the NHMFL's DC Field Facility (DCFF) at FSU as an example to showcase the unique challenges of cybersecurity for academic science at a widely accessible user facility. The background and cybersecurity architecture are outlined in Section 2, along with the significance of the support that a host institution, such as FSU, can provide to a facility such as the NHMFL. Section 3 provides on-the-floor examples of this approach. Section 4 gives an overview of the intersection of cybersecurity with FAIR (findable, accessible, interoperable, and reusable) data practices and open science at the NHMFL, as well as the security challenges these guiding principles can entail.

Cybersecurity Challenges to Protection with Access—Using the Example of the NHMFL DC Field Facility

In recent years, the operation of a number of large-scale industrial, public, and academic facilities has been disrupted by cyberattacks, resulting in significant operational downtime, facility damage, compromise to the safety of personnel and the environment, as well as significant monetary losses due to downtime, equipment, and reputational damage [4–6]. High-profile institutions and facilities with unique, world-leading, or critical capabilities are particularly vulnerable to cybersecurity threats and cyberattacks. Hence, the development of a strong yet practicable cybersecurity strategy is needed to enable scientific exchange, adequate access for remote participation, and reliable instrument control.

The DCFF is a large-scale, scientific user facility featuring industrial-grade equipment. The DCFF is a 24/7 site comprised of a magnet cooling water plant, a 60-megawatt power infrastructure, and a cryogenics plant, which are monitored and controlled via a Distributed Control System (DCS, Figure 1). Specifically, the 60 MW power system features an onsite substation, several subsidiary switchgear line-ups, four dedicated 14.5 MW DC power supplies for magnet operation, and power quality conditioning equipment. The magnet cooling water plant features primary magnet cooling loops that utilize four 500 HP and one 800 HP pumps, each equipped with a variable speed drive, as well as a water treatment system that ensures high-resistivity deionized magnet cooling water. The primary cooling loops are linked to a secondary cooling system that features four 2000-ton chillers, four cooling towers, and 4,000,000 gallons of stored chilled water and various pumps. The cryogenics plant purifies, compresses, and liquefies helium from the NHFML's closed helium recovery system and directly connects to the superconducting magnet cryostats of two of the NHMFL's flagship magnets, the 45T hybrid magnet [7] and the Series Connected Hybrid magnet [8].

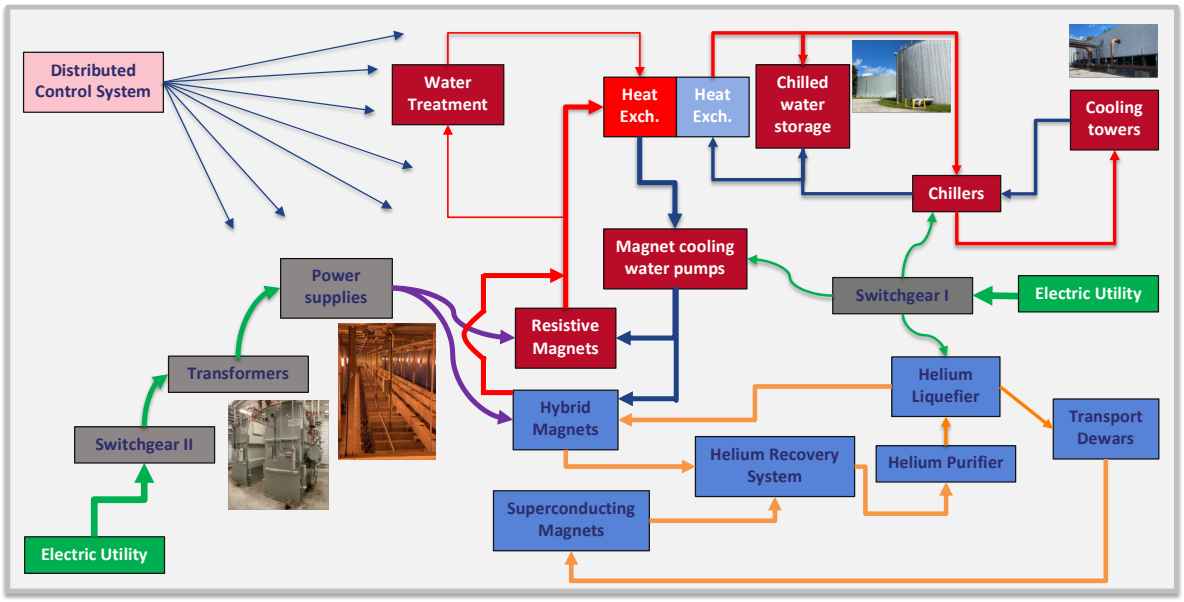

Figure 1. Overview of the DCFF industrial infrastructure.

Importantly, the operation of all three plants is required to serve the user facility at its full capacity. The DCFF welcomes several hundred scientific users per year, both in person and via remote participation [3].

A major goal of a cybersecurity program at a large-scale user facility, such as the NHMFL's DCFF, is the protection of personnel and equipment from the potentially disastrous release of stored energy via compromised controls, protection systems, or the external take-over of the large-scale infrastructure. Inherent challenges include maintaining the integrity of the industrial equipment and control systems. For example, security updates or upgrades of the operating system (OS) versions routinely disable or adversely impact previously working software and systems. As a result, (proprietary) software, vintage equipment, and operating systems are not always straightforward to update or replace, which results in system vulnerability until necessary security enhancements or compensating controls are in place. This is particularly problematic in the context of the user facility's need for high-level accessibility (Figure 2).

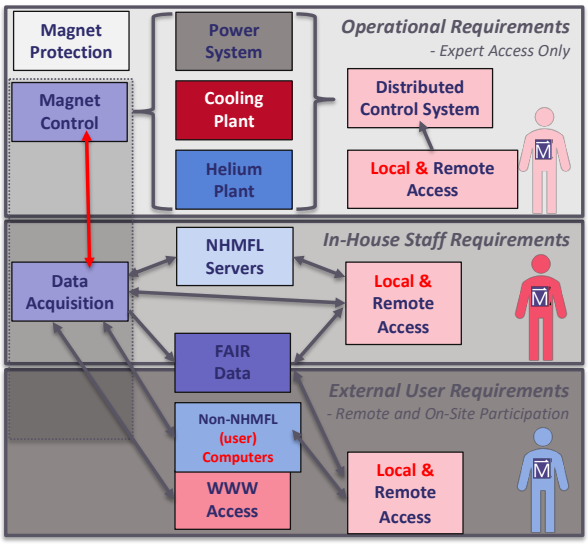

Figure 2. Overview of the accessibility needs for scientific research in a large-scale user facility, exemplified by the NHMFL's user magnet systems.

Therefore, the presented approach is highly focused on ensuring necessary cybersecurity and data privacy controls are in place while also recognizing the need to balance and reduce the inherent friction between cybersecurity and research where possible—given the complex research and technology environment that NHMFL researchers, information technology (IT), and professional cybersecurity staff are required to manage. Without an effective strategy for addressing such challenges and implementing effective controls, it is possible that increased levels of risk may result, or new risks could be created. This undesirable outcome is often related to suboptimal or ineffective "(...) cybersecurity controls that get in the way of research" [9]. Such challenges necessitate a durable lifecycle approach for managing facility needs.

In addition to the need to maintain the integrity of industrial equipment, control systems, and IT at the lab, access to industrial equipment control is needed for instrumentation and control staff. These operational requirements, for expert access (limited to a few staff members) only, include local and remote access to the Distributed Control System, which, in turn, serves as a gateway to control the magnet system via the DCFF power system, the magnet cooling water plant, and the helium cryogenics plant. In addition, a separate magnet protection system needs to be accessible for experts to review magnet performance. Scientific user support staff needs remote access for experimental setup control. Hence, in-house staff requires both local and remote access to the NHMFL servers, data storage volumes, and data acquisition systems, which are directly related to magnet control. Magnets and other experimental setups require on-site control by external users, and the remote participation of external scientists is crucial. Further, remote access to experimental data needs to be enabled to facilitate FAIR and open data management practices (Section 4). External users who participate in experiments either on-site at the DCFF or remotely from their home institutions need direct access to the data acquisition systems that also control the magnet systems—either via the standard systems provided by the NHMFL or via their own acquisition systems and experimental setups. External users also require access to the Internet. Typically, external users utilize their own computer hardware to connect to the NHMFL network.

2. Method—Establishing a Cybersecurity Architecture and Framework at a Large-Scale User Facility

2.1. Background and Cybersecurity Architecture at the NHMFL

The cybersecurity approach adopted by the NHMFL aims to balance risk and reward in a diverse research environment. Hence, this facility's approach to cybersecurity includes the review of the lab technology landscape and the development of a common understanding of the IT, industrial or operational technology (OT), and research technology (RT) domains implemented at the NHMFL because each technology domain is often accompanied by dissimilar investment, implementation, and support lifecycles. This establishes baseline knowledge and decision-making requirements among interdisciplinary team members, which include faculty and student researchers, managers, IT and cybersecurity professional staff, and executive leadership from the NHMFL and FSU.

Importantly, a major objective is developing and sustaining cybersecurity capabilities that can be managed and adjusted over time with the participation of lab and university stakeholders to meet the unique operational, scientific research, technology, and access requirements inherent to the NHMFL's mission (Section 1, Figure 2). Moreover, cybersecurity control implementations need to be manageable and maintainable over technology domain usage lifecycles to reduce the need for future investment.

2.2. Establishing a Cybersecurity Architecture and Framework at a Large-Scale User Facility

In view of these goals, established cybersecurity control implementations based on standards-based cybersecurity and architectural frameworks available through sources, such as the National Institute of Standards and Technology (NIST) [10,11], National Electric Reliability Corporation (NERC) [12], International Electrotechnical Commission (IEC), and

International Society of Automation (ISA) [13] were considered as possible cybersecurity and architectural frameworks for the NHMFL DCFF. However, based on a readiness and gap assessment, a practical, short-term result-focused strategy was chosen that prioritizes major risks and minimizes the resource investment typically associated with traditional audit-driven approaches.

The readiness and gap assessment was jointly performed by a team of NHMFL and FSU experts and conducted its evaluation against aspects of the NIST and NERC cyber security standards relevant to a large-scale user facility [10–12]. The assessment included the identification of the NHMFL and FSU personnel responsible for managing the NHMFL IT, RT, and OT infrastructure. Enterprise FSU tools and services were leveraged in the readiness and gap assessment and included a risk assessment, vulnerability scanning (and remediation), use of the public key infrastructure certificate system, and FSU enterprise security assessment and reporting tools. Utilizing a readiness and gap assessment rather than a detailed audit enabled the NHMFL to develop approaches for addressing the major risks it has identified and serve as the basis for the needed cybersecurity controls. Importantly, this involves a balancing act between accessibility, risk management, and security that cannot be successfully accomplished in a single implementation, but depends on a durable lifecycle approach that can be used to revisit, adjust when necessary, and manage NHMFL requirements over time.

More specifically, the chosen cybersecurity approach also makes use of the ISA-99 industrial automation and control systems and IEC 62443 security standards [13] to provide an architectural template for identifying and integrating the necessary IT, OT, and RT central to our efforts (Figure 3, which depicts the segmentation architecture for the NHMFL based on ISA-99). ISA-99 directly provides a framework for organizing the various technology (domain) types at the lab—aligning systems and infrastructure with well-defined architectural zones and levels based on system, communication interface, access, and cybersecurity requirements. It is noteworthy that these ISA and IEC standards continue to be developed based on predecessor standards and collaboratively between working groups across organizations [14,15]. The NHMFL/FSU approach adapts ISA-99 to incorporate large facility research technology for this application. In our approach, ISA-99 provides a network segmentation architecture organizing the requirements associated with the technology at each level (Figure 3.). The use of ISA-99 and related standards also emphasizes the need to consider the implications of new technology acquisitions on cybersecurity controls and requirements and vice versa, which provides an inherent feedback loop between technology selection/implementation and concordant implementation of cybersecurity controls. One of the foundations for ISA-99 was the Purdue Enterprise Reference Architecture (PERA, or previously, the Purdue Reference Model) [16]. ISA-99 offers guidance for industrial control system network segmentation using security zones, levels, and conduits (facilitating required connectivity between zones) that align functional and technology requirements with the services provided or processes conducted within a particular zone or level (Figure 3) [13,14] and as such, could be adapted to represent the NHMFL's high-level cybersecurity architecture. Since the Purdue Model was initially developed, its concepts have been enhanced through ISA and other standards bodies to support industrial systems process management and related technology and security requirements that have evolved, adapted, and been applied over time [17].

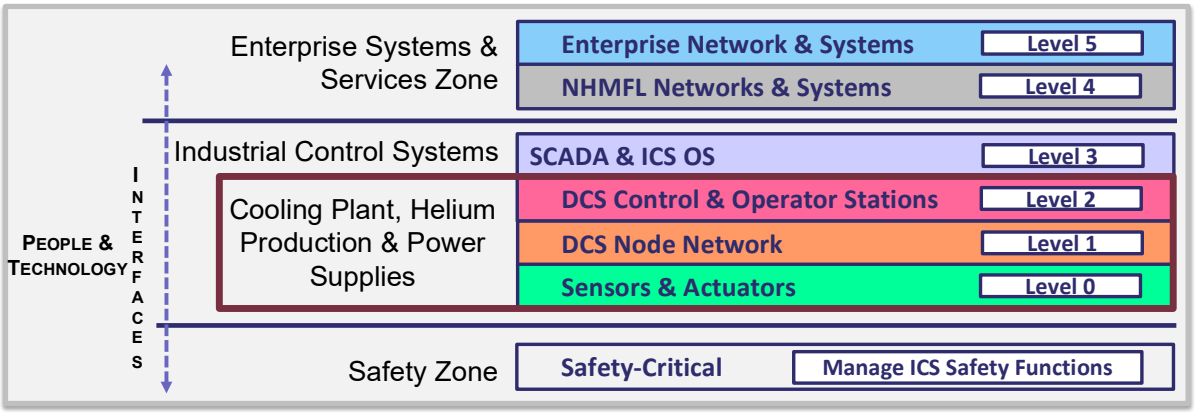

Figure 3. High-level overview of the presented cybersecurity architecture based on ISA-99 [13,14] (figure adapted to NHMFL needs from [18]). Zone summary (conduits and Science Demilitarized Zone (DMZ) not shown).

2.3. Role of a Host Institution

The NHMFL's cybersecurity program also benefits from a robust and maturing FSU cybersecurity program. FSU cybersecurity tools and processes are available to all university departments and intended to support a broad range of applications and protection needs, which include teaching and academics, research, and administrative systems. The FSU cybersecurity program provides access to enterprise tools, which include cybersecurity support and consulting, implementation services focused on risk assessment/management, vulnerability management, encryption, cybersecurity posture assessment and reporting, third-party cybersecurity services, and security awareness training. The centrally provided services also include business continuity, disaster recovery, and incident response planning services, as well as plan and procedure templates, which are designed to be adapted by university entities to meet the wide range of operational and technical preparedness requirements facing the university. The majority of FSU's enterprise tools and services are centrally funded and available at no additional cost to FSU entities. However, certain tools and services also require department-level resources and investments to meet the entities' specialized needs. In some cases, department-level resource requirements can be substantial.

2.4. Stakeholders and Technology and Cybersecurity Domains

Finally, the NHMFL's approach addresses the need to manage the various required decisions related to cybersecurity and interrelated infrastructure, architecture, application, and research systems. Such "decision domains" include cybersecurity policies, procedures, and guidelines that need to be established and maintained, as well as disseminated and implemented, to ensure a functional and effective cybersecurity solution. A lab governance approach was chosen that emphasizes the need to accurately understand the types of decisions that need to be made in an organization based on input from stakeholders of each decision domain as well as from all levels of the organization. This approach makes the best use of complimentary skill sets, expertise and experience, and interdisciplinary responsibilities [13,16,19].

Table 1 displays a high-level representation of the five decision-making domains that were identified as components of effective technology governance in high-performing organizations [19,20]. In the NHMFL/FSU model, cybersecurity, information security, and privacy management are viewed as a set of interdependent requirements that must be effectively integrated with stakeholders responsible for each domain. This approach to governance is designed to help ensure that necessary cybersecurity requirements are considered as critical parts of the research, operational, technology, and investment decision-making continuum.

Table 1. Representation of NHMFL stakeholders and technology and cybersecurity domains. Abbreviations in the table: Scientific (SCI); Engineering (ENG); Business Systems (BUS); NHMFL Executive Committee (EXEC); NHMFL (Lab). Adapted from figure 6 of Weill, Peter and Ross, Jeanne W., "IT Governance on One Page", Center for Information Systems Research, Sloan School of Management, Massachusetts Institute of Technology, Working Paper No. 349 (November 2004): 12 [20]. Used with permission.

Style	Technology and Cybersecurity Domains									
	IT-RT Security Principles and Policies		IT-RT Infrastructure		IT-RT Architecture		Business Applications and Research Systems		IT-RT Investment and Prioritization	
	Input	Decision	Input	Decision	Input	Decision	Input	Decision	Input	Decision
Multi-Disciplinary	SCI, IT, ENG Staff	Lab and IT Managers	SCI, IT, ENG Staff	SCI, IT, ENG Staff	SCI, IT, ENG Staff	SCI, IT, ENG Staff	BUS, Lab and IT Managers	EXEC, CIO, CISO	SCI, IT, ENG Staff	EXEC, CFO, COO
Information Technology	IT Staff	Lab and IT Managers	SCI, IT, ENG Staff	Lab and IT Managers	SCI, IT, ENG Staff	SCI, IT, ENG Staff	BUS, Lab and IT managers	IT Managers	FSU and Lab IT Managers	EXEC, CFO, COO
Research and Operational Technology	SCI, IT, ENG Staff	Lab and IT Managers	SCI, IT, ENG Staff	SCI, IT, ENG Staff	SCI, IT, ENG Staff	SCI, IT, ENG Staff	SCI, IT, ENG Staff	Lab and IT Managers	SCI, IT, ENG Staff	EXEC, CIO, CISO

3. Cybersecurity Approach at the NHFML's DCFF in Practice

A typical DCFF embedded system is chosen as a representative example of how the NHMFL's DCFF implements the presented cybersecurity approach. Such systems interface with large-scale infrastructure, require remote accessibility and are used for data acquisition and equipment protection. The purpose of each embedded system must be individually assessed when identifying appropriate security measures so that the desired level of security can be determined by weighing the level of risk and impact on the facility. The assessment involves determining accessibility needs, understanding technology risks, capabilities, and constraints, and (ease of) use requirements.

Specifically, the NHMFL's DCFF uses a device with a high-speed Field Programmable Gate Array (FPGA), a Linux-based real-time operating system, and hot-swappable input/output (I/O) modules for equipment monitoring and control. This setup requires a host PC (Personal Computer) on which software is developed and from which software is deployed to the FPGA or real-time operating system over the network. It also requires the development of custom-built applications that can run on a remote PC and enable user access to the device after deployment. As a result, security measures need to be applied at the physical, OS, application, and network levels. Each layer is related, and failure to protect one layer of the architecture can lead to vulnerabilities in another [21]. Importantly and in addition to the outlined measures, essential parameters monitored by this real-time system are redundantly recorded by the facility's main Distributed Control System to aid in fault or attack recovery.

An example of such an embedded system at the DCFF is the magnet power supply monitor, which logs and displays power-system-related instrumentation data. The power supply monitor program runs on an integrated controller, which consists of a real-time embedded processor, FPGA, three analog input modules, and one digital input module. Users can remotely connect to the controller via a custom-built TCP (Transmission Control Protocol) client application to monitor down-sampled power system data in real time and can download data log files through an encrypted web server hosted on the device.

The device is secured using a variety of physical and electronic methods. The device is isolated within a wall-mounted box enclosure in a restricted area for physical protection. The device can only be accessed through the DCFF's staff network (Figure 2; Figure 3, Level 4) or, if offsite the FSU campus, the NHMFL's virtual private network (VPN), which requires multifactor authentication and limits access only to staff members who require it. Remote accessibility is limited to a transport layer security/secure socket layer (TLS/SSL)

encrypted client application and a TLS/SSL encrypted web server—an approach that is enabled by FSU offering enterprise public key certificates as a service to all FSU departments and organizations with a web presence [22]. Access to the web server is limited via username and password that give permission to download data files. Importantly, the client application can only be used to view the status of the power supplies and cannot be used for malicious purposes that could potentially be co-opted and cause (un)intentional equipment damage or power system configuration changes. The client app is distributed as an executable to ensure that the source code cannot be modified and is available for download on the NHMFL's password-protected intranet. Any editable parameters available to the user on the client application require password authentication (e.g., signal scaling factors and threshold values that can trigger an event file). Online training resources are provided to mitigate unintentional application misuse. As new OS and device driver updates are released, they are downloaded on a development system, and the power supply monitor program is tested for correct functionality. If functionality remains unchanged, updates are installed and configured on the production system.

Network access restrictions in the DCFF's magnet cells present another important example of the NHMFL's cybersecurity approach and its impact on the user experience. Crucially, no wireless network access is available in the magnet cells since the 2.4 and 5 gigahertz radio frequencies used by Wi-Fi represent a source of experimental noise for the low-level measurements being performed. Therefore, network access is hardwired only and is divided into three virtual local area networks (VLANs). Each experimental space has network jacks labeled for use in one of the three VLANs (corresponding to the domains displayed in Figure 2). First, there is the Visitor Network, which is for external users and visitors (Figure 2, external user requirements; Figure 3, Level 5). This VLAN gives access to the Internet, specific facility printers, and specific data acquisition computers. Second, there is the DC Magnet Building (DCMB) Network, which is intended for internal staff (Figure 2, in-house staff requirements; Figure 3, Level 4). It is the gateway to file servers and printers and enables remote monitoring via NHMFL-authorized remote access methods so that in-house personnel can monitor experimental setups remotely using desktops or laptops. Last, there is the Protected Network, which is limited to a subset of qualified internal staff (Figure 2, operational requirements; Figure 3, Level 2 and Level 3). This most sheltered network includes access to the DCS and, hence, handles control and monitoring of the large-scale industrial equipment (water-cooling and cryogenics plants) and magnet power supply control. Moreover, magnet protection systems are housed on this network. There is no Internet access to and from the Protected Network, and only static IP and reserved DHCP (Dynamic Host Configuration Protocol) addresses managed and allocated by NHMFL IT personnel are used. Access to this network is limited to expert lab and IT personnel only.

3.1. Practical Challenges

A comprehensive cybersecurity approach has wide implications for the organization and scientists utilizing the user facility, as well as for the facility's funding agencies. For instance, mature user facilities, which have served their respective scientific user communities for more than a decade, may rely on industrial control or network infrastructure that dates to their inception. Inevitable replacements of the infrastructure are disruptive to operations, time-consuming, and costly. This emphasizes the need for effective implementation planning and decision-making. Similarly, RT is routinely kept current or expanded with present-day equipment, while critical parts of the large facility OT are often based on outdated standards and architecture.

Facilities are hardly in a position to discard or replace equipment with new technology without adequate assessment and prioritization of the risks that must be managed, along with understanding the inherent capabilities and constraints associated with vintage systems and technology. As a result, many facilities utilize various mitigation techniques

and compensating controls that make do with less-than-optimal setups and architectures until proper solutions and updates can be implemented.

3.2. Why Is a Robust Cybersecurity Framework Critical?

In pursuit of their mission, large-scale user facilities strive to provide the best possible experimental capabilities to their scientific users who expect seamless functionality during their stay at the facility. Hence, the implementation of a robust cybersecurity framework in a user environment has significant effects throughout the user experience. Importantly, merging a cybersecurity framework and related requirements with the research needs of the facility users involves an increasingly greater level of facility and institutional resources (personnel, time, and money) than is historically allocated. Specifically, departmental investments include resources needed to provide and sustain information security and information privacy management roles, funds needed for necessary cybersecurity tools and system acquisition (including maintenance, upgrades, and enhancements), and funds to support preparedness for and response to major disasters, disruptions, or cybersecurity incidents.

4. FAIR and Open Science at the NHMFL

4.1. A Brief Introduction to FAIR Data and Open Science

In recent years, a consensus has emerged among stakeholders in scientific research that there is great value in the broad sharing and reuse of the products of scientific research and that facilitating reuse should be a fundamental part of the scientific process. This includes raw and processed data, associated metadata, and research workflows. In the United States, this perspective is reflected in policy guidance from the White House Office of Science and Technology Policy (OSTP) [23] and funding agencies such as the NSF [24], Department of Energy [25], and the National Institutes of Health (NIH) [26]. These agencies agree that the practical realization of the goal of broader reuse necessitates the application of the principles of FAIR and open science, which is showcased by OSTP declaring 2023 as the "Year of Open Science" in recognition of government actions to advance national open science policy.

Originally developed in 2016, the FAIR principles [27] provide guidance (and a memorable acronym) for ensuring data, metadata, and workflows are findable, accessible, interoperable, and reusable for both humans and machines. The FAIR principles specify that to be considered FAIR, research products should be associated with relevant data and metadata, be findable using tools, such as search engines and repositories, utilize standardized formats and vocabularies, and be associated with unique and persistent identifiers, among other aspects [28]. The FAIR guiding principles are closely related to, but distinct from, the principles of open science. While openness has long been a key value in science with a long history and evolution of its implementation [29], the modern open science movement began to take its current form at the beginning of the 20th century with statements, such as the Budapest Open Access Initiative in 2001 [30] and the Berlin Declaration on Open Access to Knowledge in the Sciences and Humanities in 2003 [31]. According to the United Nations Educational, Scientific, and Cultural Organization (UNESCO), the open and unrestricted availability of data, publications, and software is critical to the goals of the open science [32].

The NHMFL is committed to applying the principles of FAIR data and open science to ensure that the products of research generated using its unique and specialized instrumentation, especially the research data, are shared as widely and openly as possible to generate the greatest scientific and social benefits [33]. In pursuit of this goal, the NHMFL has been working to review and improve its policies related to research data management and dissemination and has become aware of a variety of risks and challenges that lie at the intersection of research, cybersecurity, and FAIR and open data.

4.2. Risks of Compromised Cybersecurity

Sections 1–3 illustrate many ways in which cyberattacks could disrupt operations at a scientific user facility, such as the NHMFL, by targeting the building's physical infrastructure, including IT, OT, and RT. The potential for disruption extends to cyberinfrastructure (CI) involved in user research data management. Since the NHMFL is an NSF major research facility that is closely associated with and shares CI with its three host institutions (two of which are R1 research universities), it is appropriate to include an analysis of cyberattacks on comparable major facilities or institutions of higher education as a part of NHMFL's risk assessment.

For example, a potential ransomware attack on the NHMFL analogous to the May 2020 attack on the Physics and Astronomy department at Michigan State University documented in a case study by Trusted CI, the NSF cybersecurity center of excellence [11], could result in encryption or theft of months or years' worth of user research data stored on NHMFL servers and data acquisition systems. In the case of research data encryption, it may be unlikely that user access to research data would be lost, as it is routine for users to make private copies and facility data management plans [34] to ensure backups are made for disaster recovery purposes. While possible, restoration of the affected data would be a complex and time-consuming process. The theft of original research data as part of a ransomware (or any other kind) cyberattack is a far greater risk to the NHMFL.

Data theft is viewed as one of the greatest risks to research data management at the NHMFL for a variety of reasons. First, user program policy is strongly deferential to the preferences of user proposal principal investigators (PIs) in deciding how data is stored, transmitted, accessed, and disseminated. The NHMFL's general data management plan states that "(. . .) the PI will select the vehicle(s) for publication or presentation of products of research, and [have] ultimate authority in their initial use" [35]. For this policy to be upheld, data stored by the NHMFL must remain secure until the PI of the user proposal is prepared to disseminate them. The only limitation of the PI's discretion is that all NHMFL user facilities require that research data be utilized in a publication and/or made openly available within three years of the last assignment of magnet time. Extensions to this deadline can be provided at the discretion of the facility.

The three-year minimum embargo period is necessary to allow users to make full use of their research data, which is granted after a competitive and meritocratic review process. Research data collected at one or more of the NHMFL's user facilities and elsewhere may represent the culmination of multiple runs of magnet time, utilizing systems of increasing magnetic field strength over several years. PIs may have invested hundreds or thousands of person-hours in research, development, sample generation, and data acquisition related to their user proposal. The theft of user data could, therefore, represent the loss of exclusive access to proprietary knowledge obtained through a massive investment of user and science funding resources. If this information is acquired by competitors, there is a risk of damage to the careers of the researchers involved.

Compromised cybersecurity controls leading to data theft also present a risk of violating the legal or ethical obligations of the NHMFL and/or its users. For example, some datasets contain protected health information, proprietary intellectual property, or constitute a national security concern for a user's nation of origin and cannot be made openly available or must be modified prior to release to remove or censor sensitive information. Theft of the original, unmodified data at any time after acquisition could be damaging to a user facility, the host institution, the facility's user community, research subjects, and other stakeholders. Data theft could also result in harm to the NHMFL's and the host institution's reputation and hinder the ability of the NHMFL to fulfill its mission due to a lack of trust from its potential user base. Due to its global reach and the large impact the NHMFL has on the body of the literature in a variety of fields, a large-scale breach (e.g., theft, tampering, or unauthorized exposure of data related to a large number of user projects) could also call into question the integrity of a wide array of published research articles if the provenance of the underlying research data cannot be determined [36]. Hence, the NHMFL must be

able to ensure the security of research data for at least three years and potentially much longer. This is in direct contrast to the findings of the 2021 Report of the JASON group on Facilities Cybersecurity, whose executive summary stated that "NSF major facility data are to be openly shared; confidentiality is not a primary goal" [12]. The JASON report lacks an understanding that for institutions, such as the NHMFL, a data breach in the time between acquisition and open availability of data could result in the leaking of confidential or misleading data, which is an acknowledged fact by NSF's Trusted CI [36].

4.3. Evaluating the Probability and Prevalence of Research Data Theft

While cyberattacks leading to the theft of user research data pose the greatest threat to the NHMFL, it is difficult to assess the risk associated with various cyberattack scenarios. Cyberattacks of all kinds are on the rise [37,38]. Higher education institutions [39] and NSF major research facilities tend to have significant cyber security risks [40]. Additionally, information on cyberattacks and research-related risks in general, particularly in higher education, is severely lacking [39,41]. Information on the specific threat of data theft is even more scarce. Reports on data breaches at higher education institutions, whether in the form of research articles or news reports, tend to focus on the amount and types of personal information that are stolen or are vague about the nature of the stolen data and the implications of its theft.

For example, in June 2020, three institutions were subject to ransomware attacks by the Netwalker criminal organization: the University of California San Francisco (UCSF, San Francisco, CA); Columbia College Chicago (CC, Chicago, IL); and Michigan State University (MSU, East Lansing, MI). Each institution had a different degree of openness about the nature of the stolen data. UCSF released a public statement stating that malware affected "a limited number of servers within the School of Medicine" and that the stolen data were "important to some of the academic work we pursue as a university serving the public good", without describing the precise nature of the data [42]. A series of reports in the CC student-run newspaper, Columbia Chronicle, stated that the college was not providing information on the nature or severity of the attack. However, ransomware victims were to be notified and offered a free online credit monitoring service, implying that personal information was stolen [43–45]. Importantly, CC is a private art college and presumably generates limited scientific research. MSU was the most open about the ransomware attack, which was documented in a Trusted CI case study [46] outlining that research data from the Department of Physics and Astronomy were stolen, in addition to other types of data.

In the absence of more information, one can speculate on the reasons for institutions generally not being open about the nature of stolen data. They may reason that they could open themselves up to future attacks by revealing their weaknesses or attempting to avoid legal consequences related to violation of the Family Educational Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), or General Data Protection Regulation (GDPR).

The lack of concrete information on the prevalence of research data being stolen from major research facilities and institutions of higher education is a major hindrance in assessing the possible nature and probability of its theft. The NHMFL and its host institutions would greatly benefit from additional research in this area as it would allow for better determination of the most at-risk assets. While the authors understand the need to protect impacted institutions and affected data and research subjects, making vital attack vector information available to lab managers, cybersecurity, and IT professionals would enhance the ability to prepare for and defend against future cyberattacks. The authors believe that such information is crucial to support the research community. In the meantime, due to the potential damages to the NHMFL described in Sections 1–3, a significant threat of data theft is assumed, and needed mitigations are viewed as elements that must be continually reviewed and updated where needed.

4.4. Challenges of Data Security for FAIR and Open Data

The risks of data breach and theft are inherent to scientific research when using a combination of vintage and modern RT and CI and not unique to an environment where FAIR and open-science principles are emphasized. However, the application of these principles creates novel challenges for data security and integrity for researchers, data stewards, cybersecurity practitioners, and IT professionals. For example, visions for the future of FAIR data within many scientific disciplines universally require interconnected, interoperable, global CI and data ecosystems to facilitate the desired functionality [47,48]. This includes the ability for researchers to use high-performance computing to carry out complex analyses on large volumes of data from federated data repositories around the globe with controlled access to sensitive data, such as protected health information or other regulated data. If not properly managed, the complexity of the CI needed to facilitate this functionality can create additional information privacy and cybersecurity risk by opening more avenues of attack, as a single insecure node in a larger system could potentially compromise the security of the entire network.

Although not new, the concept of a Science DMZ network [49] has been proposed to address some of the concerns related to maintaining network security while facilitating high-speed access to data. The Science DMZ offers one viable path forward for institutions to enhance the cybersecurity of their FAIR-related CI. However, network security is only one aspect of successful implementation. Other aspects of the solution must address data access and integrity (data management/stewardship) requirements. Furthermore, FAIR data ecosystems need to be broadly utilized, be inclusive, and have global reach to ensure their long-term sustainability. There is no guarantee that all institutions contributing to a particular FAIR data ecosystem will have the resources or expertise needed to manage or implement all necessary parts of the required cybersecurity and data management solutions; i.e., the Science DMZ, data repositories, and related access and data management workflows.

Another major challenge to making data from scientific research FAIR is that the availability of metadata, workflows, and other components of the overall data product enables them to be reused more effectively for both legitimate and malicious reasons. The rich metadata and interoperable nature of FAIR data could allow malicious actors to more easily recognize the value of stolen data and utilize it, potentially increasing the motivation for cyberattackers to attempt a data breach. To illustrate this point, we can utilize the FAIR data maturity model developed by a Research Data Alliance working group [50,51] to show scenarios where research data are not FAIR and others that are very FAIR.

The FAIR data maturity model provides indicators that can be used to judge the "FAIRness" of research data. Among these indicators are that data and metadata are expressed in standardized formats (RDA-I1-01), that rich metadata are provided to allow discovery (RDA-F2-01M), that metadata can be accessed manually (RDA-A1-02M), and that a plurality of relevant and accurate attributes are provided to allow reuse (RDA-R1-01M). Using these indicators, we can predict that, in practice, "not FAIR" data might be stored in proprietary file formats which require specific, expensive software or non-standard hardware or research processes to utilize. Data could also be stored in file formats that are trivial to open but without necessary metadata that make it possible to understand, such as a columnar text file with generic column names such as "Col1", "Col2", etc. There would also be no human-readable text, such as a "README" file, to provide context or meaning to any of the associated data files. Conditions, such as these, do not facilitate data reuse [52].

Using the same indicators, we can predict that in the "very FAIR" case, data would be in open, standard file formats richly annotated with human- and machine-readable metadata. Metadata would include a variety of useful attributes, including the identity and provenance of the sample(s), instrumental configurations and parameters, data analysis workflows and algorithms, research protocols, and a thorough description of the nature of the raw data. This kind of data could be very easy to reuse for both legitimate and malicious purposes.

Malicious reuse could involve a cyberattacker or their accomplice presenting the stolen data (or conclusions drawn from it) as their own after obfuscating its source or tampering with it so that it appears to be unique and original. Attempts to do so could be hampered by the uniqueness of some of the NHMFL's instrumentation; i.e., it would be difficult for a malicious actor to explain how they obtained data that can only be generated by a single instrument in the world located at the NHMFL without having conducted experiments there. A cyberattacker or accomplice could also utilize stolen data to inform their own independent research, providing a competitive advantage without showing any obvious signs of misconduct.

There is no simple way to make data more FAIR and enable legitimate reuse without also increasing the risk of malicious reuse. A practicable approach is to secure FAIR data through a combination of good cybersecurity hygiene and data management practices among researchers and fastidious application of cybersecurity standards by institutional and facility IT professionals.

4.5. Operational Cybersecurity Challenges

Due to the NHMFL being comprised of seven user facilities serving a broad diversity of research disciplines, it faces several unique data management and cybersecurity challenges not faced by other large-scale research facilities. The scale and number of user projects is a major factor. In 2021, the NHMFL had 1615 users from 279 different universities, government labs, and private companies worldwide [3]. The number of users was lower than average due to continuing recovery from the COVID-19 pandemic. About half of those users acquired data at the lab's largest user facility, the DCFF. Due to these numbers, it is practically impossible to develop a risk profile (guided by the Trusted CI Open Science Cyber Risk Profile [36] or a comparable risk assessment framework) for each individual user proposal to ensure that research data is shared and transferred securely.

Furthermore, due to the scale and diversity of user projects, the NHMFL does not have the resources to assume all user data stewardship and cybersecurity responsibilities for data generated there. As stated in the lab-wide data management plan, "(. . .) the ultimate responsibility for data stewardship lies with the PIs of user proposals (. . .)" [35]. In other words, PIs are responsible for ensuring the appropriate management of user research data that leaves the lab. This includes managing the confidentiality, integrity, and availability requirements associated with lab-generated data and the compliance of all collaborators with access to such data. Due to this policy, PIs are free to utilize any local or remote storage, data repositories, or other CI available to them, including CI that may be inherently insecure (although this is not recommended by NHMFL). The NHMFL cannot vet all potential CI solutions to ensure their security or prevent users from utilizing insecure CI. Any attempts to do so would likely be considered an intrusive overreach of the lab's role.

Another NHMFL-specific challenge is related to the different types, sizes, associated disciplines, and data acquisition methods for research data generated at its user facilities. There is no universally applicable solution for research data management nor a universal solution for securing, managing, and providing access to lab research data. As a result, user facilities have developed their own specialized data management strategies to address their scientific communities' unique needs. The NHMFL has begun mapping the data lifecycle—data beginning and end points within the lab—by constructing data management maps (Figure 4). These maps are radically different for the various user facilities. The internal file server that serves the Tallahassee site of the NHMFL is a common method used for data storage, but several facilities also use their own separate storage solutions, which may or may not be accessible by users. Access to the Tallahassee internal file server is controlled by the NHMFL's computer support group (CSG) and is only granted to NHMFL staff. Access to facility storage solutions may be controlled by CSG and/or facility staff, but CSG is ultimately responsible for managing the cybersecurity of all data storage solutions. The requirement for different data management strategies across facilities creates a significant

burden for the facility staff who develop and refine them and the IT professionals who are responsible for ensuring required cybersecurity controls are in place.

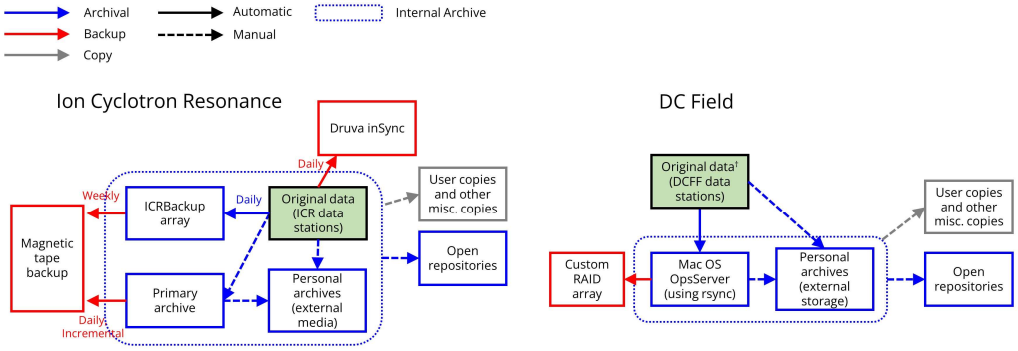

Figure 4. Data management maps showing the origin and endpoints of research data within two NHMFL user facilities. Backup refers to the process of copying data for disaster recovery purposes, and archival refers to copying data for use as a source of "working copies" and to ensure long-term availability.

4.6. Mitigating the Cybersecurity Risks of Data Sharing

The NHMFL faces numerous risks and challenges associated with the cybersecurity of FAIR and open data and has a responsibility to its user base and its funding organizations to work proactively to address them. Examples of such risks include, among others, ransomware attacks and data theft, while challenges mainly concern the lack of uniform data management practices and the difficulty of unifying them across disciplines. Fortunately, one of the major mitigations to cybersecurity risk is inherent to the nature of scientific research and requires no additional effort. Specifically, developing the expertise needed to understand and make use of research data for purposes more complex than extracting a ransom is a lengthy and often expensive process that creates a major hurdle for cyberattackers. In the Trusted CI case study of the ransomware attack at MSU, it was noted that " . . . There's no evidence [the attacker] knew they had research data. They either didn't care if they had research data or were simply unaware . . . " [46]. It is likely that the research data obtained through the breach had scientific value. Therefore, it is probable that the attackers did not have the expertise to exploit the data. In general, cyberattacks on institutions of higher education tend to focus on ransoming confidential personal information of students, faculty, staff, and research study participants [39], possibly due to a lack of expertise and because it represents a quicker route to financial gain.

Another mitigating factor is that NHMFL users are drawn from a broad variety of research disciplines, including disparate fields, such as biochemistry and condensed matter physics. Even if a cyberattacker did have expertise in a particular discipline, they would find it difficult to make use of most research data obtained in a lab-wide data breach due to the expertise required to utilize such data. However, there is the possibility that an attacker could target a specific facility to steal data of a desired discipline and/or work with an accomplice with the appropriate expertise to make use of it, so it is unreasonable to rely on a lack of expertise of cyberattackers to protect research data from malicious reuse. Efforts to mitigate data access and sharing risks must therefore focus on actions that can be taken by the NHMFL and its host institutions to comprehensively identify risks and make the necessary knowledge and tools available to facilitate good cybersecurity hygiene and information privacy practices.

For a user facility of the NHMFL's size and scope, the development of a risk profile for each user and their specific situation is highly resource-intensive and, hence, not feasible. However, risk profiles for specific facilities, experiment types, and research infrastructure are actively developed in collaboration with users, facility staff, and institutional representatives. This process includes ensuring the security of the specialized data management strategies in NHMFL user facilities by periodically reviewing them, enhancing capabil-

ities with new tools and adjustments to workflows, identifying risks, and preemptively mitigating them.

One of the most impactful risk management measures is use-education on FAIR data. While user-related risks cannot be fully mitigated by the NHMFL due to the PIs' prominent responsibility in data management, the NHMFL and similar facilities can provide access to educational resources, which may be particularly impactful when early career researcher support needs are addressed and may improve awareness and ultimately data security of users. The NHMFL is also committed to directing users to third-party platforms, such as data repositories that have been examined by independent cybersecurity assessments or are supported by NSF or NIH, for the express purpose of providing FAIR and secure access to research data. For example, the NHMFL recently obtained a subscription to Open Science Framework (OSF, Center for Open Science, Charlottesville, VA), a platform for collaboration, data sharing, and dissemination. Among its many cybersecurity and data management features, the OSF includes secure login capabilities and encrypts stored data, provides data attribution and citation tools, and includes support for data licensing. The NHMFL has designated OSF as a recommended generalist repository, but Dataverses [53], Dryad [54], Vivli [55], and other generalist or specialist repositories [56] have similar provisions and are also recommended for use.

Future NHMFL goals include partnering with cybersecurity professionals at FSU and other institutions to vet third-party discipline-specific data repositories that are relevant to facility users. These evaluations will rely on documents, such as "Desirable Characteristics of Data Repositories for Federally Funded Research", released by the National Science and Technology Council's Subcommittee on Open Science [57]. Currently, the NHMFL continues to work on the active application of cybersecurity standards and frameworks, which along with the protection of personnel and equipment, helps to ensure the protection of privileged data. This requires proactive engagement with all three host institutions (FSU, UF, and LANL) in addressing cybersecurity concerns. The NHMFL continues to monitor and adapt to the evolving landscape of cybersecurity as it relates to FAIR and open data.

5. Conclusions

Using the example of the NHMFL DCFF, the unique challenges of cybersecurity for academic science at a widely accessible user facility are showcased, along with an overview of the support that a host institution, such as FSU, can provide in the development of a robust cybersecurity strategy. Relevant cybersecurity frameworks and architectural standards available to support the complex needs of a scientific user facility with industrial-style equipment and hazards are briefly discussed, though a detailed analysis of such frameworks, an evaluation of their related strengths, and implementation challenges and requirements may present opportunities for additional research to be conducted.

Cybersecurity frameworks, such as those the authors have identified, provide robust libraries of controls designed to meet specific objectives. Their selection and implementations in practice naturally need to be adapted to an institution's needs. Because the frameworks overlap to cover similar but not identical requirements, their application requires careful analysis and tailoring when applied to cutting-edge science and engineering research environments. This requires significant personnel and/or financial resources. Therefore, the advantages associated with the adoption of a single robust framework that can cover most organization-wide needs should not be overlooked. Compounding this situation are the challenges associated with a lack of automated and affordable tools (commercial and open-source) that can be used to facilitate their implementation in a large user facility with complex research, technology, and operational and cybersecurity requirements. Though in recent years, we also observe that funding agencies such as the NSF have devoted significant resources to developing expertise, tools, and frameworks designed to address such challenges. Examples include the NSF's Trusted CI and CI Compass centers of excellence.

The NHMFL's approach to internal and external risk identification and management is presented at a high level. When effectively implemented, its output directly translates

into cybersecurity requirements and priorities. The risk assessment process is a particularly vital aspect of the lab's approach to understanding the level of tolerance for certain risks (user facility and host institution) so that priorities and effective management and mitigations can be determined, resourced, implemented, and sustained. This lifecycle activity depends on an adequate understanding of the essential differences between IT, RT, and OT and emphasizes the importance of recognizing the unique requirements and constraints associated with the technology domains, as illustrated in this article.

It also is imperative to realize that implementation of a robust cybersecurity and/or FAIR data framework in a user environment has significant effects throughout the user experience, and the needs and concerns of these stakeholders need to be considered in any implementation. Further, merging a cybersecurity framework and related requirements with the research needs of the facility users involves a tremendous amount of institutional and (user) facility resources, i.e., personnel, time, and money, which historically have not been allocated to those facilities in sufficient amounts. It is important to acknowledge that such resources are also vital to the development of sustainable cybersecurity and FAIR data capabilities, which necessitate the parallel development of organizational and funding structures that enable the professional and durable operation of these efforts. The allocation of such resources could enable the development and establishment of dedicated data protection standards (similar to existing standards focused on compliance with HIPAA, FERPA, etc.), which would be tailored to the needs of large-scale user facilities and their research.

Implementation of FAIR principles presents unique challenges that must be planned for and managed when data dissemination, accessibility, and reuse requirements are integral to the scientific process. Moreover, maintaining the confidentiality, integrity, and availability of scientific data produced in the lab while ensuring necessary access requires new tools, workflow processes, and resources that have not historically been available.

Further, the NHMFL is committed to applying the principles of FAIR data and open science as a means of ensuring that the products of publicly funded research generated using the unique and specialized instrumentation at its user facilities, especially the research data, are shared as widely and openly as possible to ensure the greatest scientific and social benefits. The NHMFL's future work includes further development of its in-house FAIR data strategy and infrastructure tailored to the needs of its facilities' users as well as their education on FAIR data.

Author Contributions: Conceptualization, D.S.B. and C.J.B.; methodology, J.B., D.S.B., T.P.M., J.H.S. and C.J.B.; software, J.B. and A.L.C.; validation, J.B. and C.J.B.; writing—original draft preparation, J.H.S., D.S.B. and C.J.B.; writing—review and editing, A.L.C., T.P.M. and W.M.H.; visualization, J.H.S. and D.S.B.; supervision, E.C.P. All authors have read and agreed to the published version of the manuscript.

Funding: The National High Magnetic Field Laboratory is supported by the National Science Foundation through NSF/DMR-1644779 and NSF/DMR-2128556 and the State of Florida.

Data Availability Statement: No new data was created for this work.

Conflicts of Interest: The authors declare no conflict of interest. Part of this work was presented at the 2022 National Science Foundation Cybersecurity Summit in Bloomington, IN.

References

1. Hannahs, S.T.; Palm, E.C. The National High Magnetic Field Laboratory. *J. Low Temp. Phys.* **2010**, *159*, 366–369. [CrossRef]
2. National MagLab Website. Available online: https://nationalmaglab.org/ (accessed on 21 February 2023).
3. Annual Report—MagLab. Available online: https://nationalmaglab.org/research/publications-all/annual-reports (accessed on 10 March 2022).
4. Kovacevic, A.; Nikolic, D. Cyber Attacks on Critical Infrastructure: Review and Challenges. Available online: https://www.igi-global.com/chapter/cyber-attacks-on-critical-infrastructure/www.igi-global.com/chapter/cyber-attacks-on-critical-infrastructure/115745 (accessed on 21 February 2023).
5. Thakur, K.; Ali, M.L.; Jiang, N.; Qiu, M. Impact of Cyber-Attacks on Critical Infrastructure. In Proceedings of the 2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS), New York, NY, USA, 9–10 April 2016; pp. 183–186.

6. Lis, P.; Mendel, J. Cyberattacks on Critical Infrastructure: An Economic Perspective. *Econ. Bus. Rev.* **2019**, *5*, 2. [CrossRef]
7. Miller, J.R.; Bird, M.D.; Bole, S.; Bonito-Oliva, A.; Eyssa, Y.; Kenney, W.J.; Painter, T.A.; Schneider-Muntau, H.-J.; Summers, L.T.; van Sciver, S.W.; et al. An Overview of the 45-T Hybrid Magnet System for the New National High Magnetic Field Laboratory. *IEEE Trans. Magn.* **1994**, *30*, 1563–1571. [CrossRef]
8. Dixon, I.R.; Bole, S.T.; Cantrell, K.R.; Hannahs, S.T.; Kynoch, J.G.; Marshall, W.S.; Powell, A.A.; Toth, J.; Bird, M.D. The 36-T Series-Connected Hybrid Magnet System Design and Integration. *IEEE Trans. Appl. Supercond.* **2017**, *27*, 1–5. [CrossRef]
9. Shankar, A.; Drake, W. Effective Cybersecurity for Research. Available online: https://scholarworks.iu.edu/dspace/handle/2022/27733 (accessed on 21 February 2023).
10. Cybersecurity Framework. Available online: https://www.nist.gov/cyberframework (accessed on 21 February 2023).
11. Joint Task Force. *Security and Privacy Controls for Information Systems and Organizations*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2020.
12. Marron, J.; Gopstein, A.; Bogle, D. *Benefits of an Updated Mapping between the NIST Cybersecurity Framework and the NERC Critical Infrastructure Protection Standards*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2021; p. 9.
13. ISA/IEC 62443 Series of Standards. Available online: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards (accessed on 21 February 2023).
14. IEC 62443. Available online: https://en.wikipedia.org/w/index.php?title=IEC_62443&oldid=1144136166 (accessed on 26 April 2023).
15. Understanding IEC 62443. Available online: https://www.iec.ch/blog/understanding-iec-62443 (accessed on 26 April 2023).
16. Williams, T.J. The Purdue Enterprise Reference Architecture. *Comput. Ind.* **1994**, *24*, 141–158. [CrossRef]
17. Ackerman, P. *Industrial Cybersecurity: Efficiently Secure Critical Infrastructure Systems*; Packt Publishing: Birmingham, UK, 2017; ISBN 978-1-78839-515-1.
18. Boyes, H.; Hallaq, B.; Cunningham, J.; Watson, T. The Industrial Internet of Things (IIoT): An Analysis Framework. *Comput. Ind.* **2018**, *101*, 1–12. [CrossRef]
19. Weill, P.; Ross, J. *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*; Harvard Business School Press: Boston, MA, USA, 2004; ISBN 978-1-59139-253-8.
20. Weill, P.; Ross, J.W. IT Governance on One Page. *SSRN Electron. J.* **2004**, *349*. [CrossRef]
21. Overview of Best Practices for Security on RIO Systems. Available online: https://www.ni.com/en-us/support/documentation/supplemental/11/overview-of-best-practices-for-security-on-rio-systems.html (accessed on 21 February 2023).
22. Enterprise SSL. Available online: https://its.fsu.edu/service-catalog/security-and-safety/secure-computing/enterprise-ssl (accessed on 21 February 2023).
23. OSTP Issues Guidance to Make Federally Funded Research Freely Available Without Delay | OSTP. Available online: https://www.whitehouse.gov/ostp/news-updates/2022/08/25/ostp-issues-guidance-to-make-federally-funded-research-freely-available-without-delay/ (accessed on 2 February 2023).
24. Public Access Plan: Today's Data, Tomorrow's Discoveries: Increasing Access to the Results of Research Funded by the National Science Foundation | NSF—National Science Foundation. Available online: https://www.nsf.gov/publications/pub_summ.jsp?ods_key=nsf15052 (accessed on 10 March 2022).
25. U.S. Department of Energy Office of Scientific and Technical Information DOE Public Access Policy. Available online: https://www.osti.gov/public-access (accessed on 6 February 2023).
26. Data Management and Sharing Policy | Data Sharing. Available online: https://sharing.nih.gov/data-management-and-sharing-policy (accessed on 1 September 2022).
27. Wilkinson, M.D.; Dumontier, M.; Aalbersberg, I.J.; Appleton, G.; Axton, M.; Baak, A.; Blomberg, N.; Boiten, J.-W.; da Silva Santos, L.B.; Bourne, P.E.; et al. The FAIR Guiding Principles for Scientific Data Management and Stewardship. *Sci. Data* **2016**, *3*, 160018. [CrossRef] [PubMed]
28. Jacobsen, A.; de Miranda Azevedo, R.; Juty, N.; Batista, D.; Coles, S.; Cornet, R.; Courtot, M.; Crosas, M.; Dumontier, M.; Evelo, C.T.; et al. FAIR Principles: Interpretations and Implementation Considerations. *Data Intell.* **2020**, *2*, 10–29. [CrossRef]
29. David, P.A. The Historical Origins of "Open Science": An Essay on Patronage, Reputation and Common Agency Contracting in the Scientific Revolution. *Capital. Soc.* **2008**, *3*, 1040. [CrossRef]
30. Budapest Open Access Initiative. Available online: https://www.budapestopenaccessinitiative.org/read/ (accessed on 7 February 2023).
31. Berlin Declaration on Open Access to Knowledge in the Sciences and Humanities. Available online: https://openaccess.mpg.de/Berlin-Declaration (accessed on 7 February 2023).
32. United Nations Educational, Scientific and Cultural Organization. *UNESCO Recommendation on Open Science*; United Nations Educational, Scientific and Cultural Organization: Paris, France, 2021; Available online: https://unesdoc.unesco.org/ark:/48223/pf0000379949.locale=en (accessed on 1 February 2023).
33. Balakireva, L.; Balakirev, F. Making FAIR Practices Accessible and Attractive | SpringerLink. Available online: https://link-springer-com.proxy.lib.fsu.edu/chapter/10.1007/978-3-031-16802-4_41 (accessed on 10 October 2022).
34. Laboratory, N.H.M.F. FAIR Data Management Plans—MagLab. Available online: https://nationalmaglab.org/research/research-groups/center-for-fair-open-science/products/data-management-plans/ (accessed on 21 April 2023).
35. National High Magnetic Field Laboratory Policies & Procedures. Available online: https://nationalmaglab.org/about-the-maglab/organization/policies-procedures/ (accessed on 21 February 2023).

36. Peisert, S.; Welch, V. The Open Science Cyber Risk Profile: The Rosetta Stone for Open Science and Cybersecurity. *IEEE Secur. Priv.* **2017**, *15*, 94–95. [CrossRef]
37. Internet Crime Complaint Center FBI Internet Crime Report. 2021. Available online: https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf (accessed on 1 February 2023).
38. Sharif, M.H.U.; Mohammed, M.A.; Sharif, M.H.U.; Mohammed, M.A. A Literature Review of Financial Losses Statistics for Cyber Security and Future Trend. *World J. Adv. Res. Rev.* **2022**, *15*, 138–156. [CrossRef]
39. Ulven, J.B.; Wangen, G. A Systematic Review of Cybersecurity Risks in Higher Education. *Future Internet* **2021**, *13*, 39. [CrossRef]
40. Adams, E.K.; Gunter, D.; Kiser, R.; Krenz, M.; Peisert, S.; Sons, S.; Zage, J. Findings of the 2022 Trusted CI Study on the Security of Operational Technology in NSF Scientific Research. *Trusted CI* **2022**. [CrossRef]
41. Cremer, F.; Sheehan, B.; Fortmann, M.; Kia, A.N.; Mullins, M.; Murphy, F.; Materne, S. Cyber Risk and Cybersecurity: A Systematic Review of Data Availability. *Geneva Pap. Risk Insur. Issues Pract.* **2022**, *47*, 698–736. [CrossRef] [PubMed]
42. Update on IT Security Incident at UCSF | UC San Francisco. Available online: https://www.ucsf.edu/news/2020/06/417911/update-it-security-incident-ucsf (accessed on 1 February 2023).
43. Polidori, K. BREAKING: Columbia Student Information at Risk in Ransomware Attack. *Columbia Chron.* 2020. Available online: https://columbiachronicle.com/breaking-columbia-student-information-at-risk-in-ransomware-attack (accessed on 1 February 2023).
44. Polidori, K. State of College Ransomware Attack Remains Unclear. *Columbia Chron.* 2020. Available online: https://columbiachronicle.com/state-of-college-ransomware-attack-remains-unclear (accessed on 1 February 2023).
45. Polidori, K. BREAKING: College to Notify Ransomware Victims; Offers Credit Monitoring to College Community. *Columbia Chron.* 2020. Available online: https://columbiachronicle.com/breaking-college-to-notify-ransomware-victims-offers-credit-monitoring-to-employees (accessed on 1 February 2023).
46. Adams, A.; Siu, T.; Songer, J.; Welch, V. *Research at Risk: Ransomware Attack on Physics and Astronomy Case Study*; Indiana University Bloomington: Bloomington, Indiana, 2021.
47. *Directorate-General for Research and Innovation (European Commission) Realising the European Open Science Cloud: First Report and Recommendations of the Commission High Level Expert Group on the European Open Science Cloud*; Publications Office of the European Union: Luxembourg, 2016; ISBN 978-92-79-61762-1.
48. Wittenburg, P.; Strawn, G. Common Patterns in Revolutionary Infrastructures and Data. Available online: https://doi.org/10.23728/b2share.4e8ac36c0dd343da81fd9e83e72805a0 (accessed on 7 February 2023).
49. Abhinit, I.; Addleman, H.; Benninger, K.; DuRousseau, D.; Krenz, M.; Meade, B. Science DMZ: Secure High Performance Data Transfer. *Trusted CI* **2022**. [CrossRef]
50. Bahim, C.; Casorrán-Amilburu, C.; Dekkers, M.; Herczog, E.; Loozen, N.; Repanas, K.; Russell, K.; Stall, S. The FAIR Data Maturity Model: An Approach to Harmonise FAIR Assessments. *Data Sci. J.* **2020**, *19*, 41. [CrossRef]
51. FAIR Data Maturity Model Working Group FAIR Data Maturity Model. *Specification and Guidelines; Research Data Allowance*; European Commission: Brussels, Belgium, 2020. [CrossRef]
52. Pasquetto, I.V.; Borgman, C.L.; Wofford, M.F. Uses and Reuses of Scientific Data: The Data Creators' Advantage. *Harv. Data Sci. Rev.* **2019**, *1*. [CrossRef]
53. The Dataverse Project—Dataverse.Org. Available online: https://dataverse.org/home (accessed on 22 February 2023).
54. Dryad | Home—Publish and Preserve Your Data. Available online: https://datadryad.org/stash (accessed on 1 February 2023).
55. Vivli—Center for Global Clinical Research Data. Available online: https://vivli.org/ (accessed on 22 February 2023).
56. Stall, S.; Martone, M.E.; Chandramouliswaran, I.; Federer, L.; Gautier, J.; Gibson, J.; Hahnel, M.; Larkin, J.; Pfeiffer, N.; Sedora, B.; et al. Generalist Repository Comparison Chart. *Zenodo* **2022**. [CrossRef]
57. White House Office of Science and Technology Policy. *Desirable Characteristics of Data Repositories for Federally Funded Research*; White House Office of Science and Technology Policy: Washington, DC, USA, 2022. [CrossRef]