TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

Enhancing Cyber Hygiene in Research: Identifying Gaps and Proposing Solutions

Trusted CI Fellows Report

April 15, 2024

For public release

Author, Lori L. Sussman, Ed.D.
Trusted CI Fellow
University of Southern Maine

My path to academia was circuitous about best. I graduated from West Point in the early eighties. For the next three decades, I focused on understanding and operationalizing military and government information networks to move secure voice and data to the decision-maker in the correct format at the right time. Conceptually, cybersecurity existed long before science fiction writer Bill Gibson (1984) coined the term. My focus has always been to provide that kind of security with information. Even after retiring from service, I focused on secure information technology solutions, spending the next decade in companies like Cisco, Hewlett Packard Enterprise, and others. Realizing that my eligibility for the post-911 GI Bill was about to end, I pivoted to academia by getting a doctorate and joining the University of Southern Maine (USM). My current role allows me to use my expansive background to focus on human-centered cybersecurity research.

Thirty years of dealing with secure information technologies for federal entities gave me a deep understanding of the ins and outs of cyber safety. I have sought out roles where I could share tricks, tips, and techniques with others. This desire to learn state-of-the-art practices led me to apply for the Trusted Cyberinfrastructure (CI) Fellowship. The curriculum opened my eyes to the challenges of research cybersecurity. The program of study gave me a more expansive view of researchers' cyber hygiene challenges. This new perspective allows me to take what I have learned and fold in best practices for cyber hygiene into my everyday work and research community.

The Researchers' Cyber Hygiene Landscape

When reviewing guidance given to researchers, higher education institutions' research offices often refer faculty to the NIST Special Publication (SP) 800-171 for cyber hygiene requirements (Ross, Pillitteri, Dempsey, Riddle, & Guissanie, 2020). For researchers pursuing federal government awards, additional conditions can exist to adhere to specific control frameworks detailed in the Department of Defense's Cybersecurity Maturity Model Certification (CMMC) (CIO, U.S. DOD, 2021, December). Both frameworks have become increasingly relevant even when not contractually required. Actions for researchers, especially in remote settings, include using institution-issued hardware and software, being aware of licensing and security risks associated with third-party platforms, employing endpoint security controls, and using virtual desktop infrastructure and encryption software to protect data. However, these guidance documents can be unwieldy for researchers to administer.

Cyber hygiene is crucial in research, ensuring data integrity, confidentiality, and availability. Good cyber hygiene practices protect sensitive information from unauthorized access and cyber threats, such as data breaches, malware, and phishing attacks. Steps require education, access controls, authentication, monitoring, and updated security protections ((CIO, U.S. DOD, Implementation, n. d.). These practices are critical in higher education research, where the data often includes proprietary information, personal data, and intellectual property. Adequate cyber hygiene helps maintain the trustworthiness of research institutions, upholds data privacy standards, and complies with legal and ethical obligations, thereby preserving the reputation and the validity of the research outcomes.

The current cyber hygiene guidance, particularly in research within higher education, is not as specific as it needs to be. It often lacks tailored instructions for different research disciplines and scenarios. While frameworks like NIST SP 800-171 provide a broad control structure, they may not address the nuanced needs of various research fields, especially those handling sensitive data. There is also a lack of detailed protocols for remote research activities, using personal devices for research, and applying security measures to protect against emerging threats like supply chain hacks. Moreover, the guidelines might need to fully cover the management of third-party communications platforms, endpoint security controls, and the legal aspects of monitoring research activities. These gaps underscore the need for more granular, research-specific cybersecurity guidelines.

The Trusted Cyberinfrastructure (CI) Framework is a game-changer in enhancing researchers' cyber hygiene. It provides a structured approach to cybersecurity, designed to help research cyberinfrastructure operators establish and refine cybersecurity programs. The framework's four pillars-mission alignment, governance, resources, and controls-offer a comprehensive and universally applicable approach. It equips research organizations with roadmaps, resources, and advice to effectively address cybersecurity challenges and protect their cyber infrastructure.

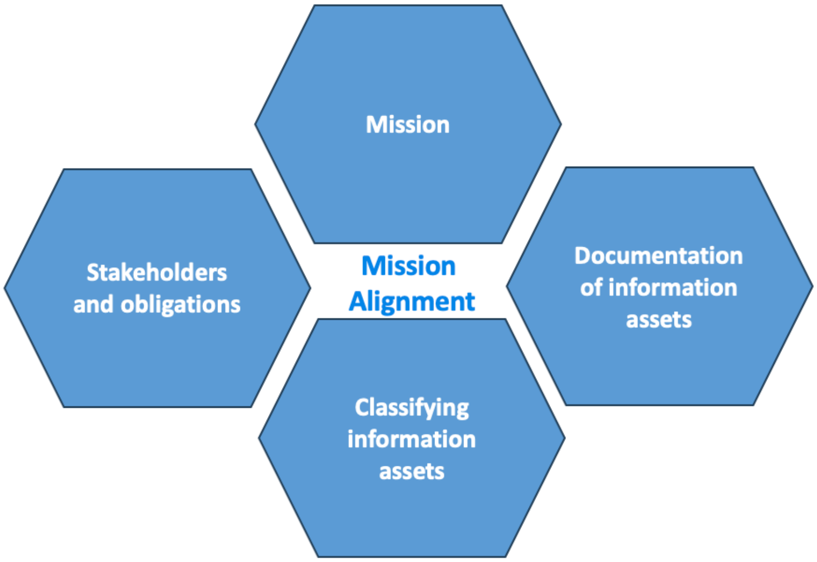
Using Mission Alignment to Create Cyber Hygiene Guidance

Cyber hygiene refers to the practices and steps used by computers and other devices to maintain system health and improve online security (Vishwanath, Neo, Goh, Lee, Khader, Ong, & Chin, 2020). These practices are often part of a routine to ensure identity safety and further details that could be stolen or corrupted. Cyber hygiene is especially critical within the research community as researchers often handle sensitive data, intellectual property, and proprietary information that cyber threats could target. Effective cyber hygiene practices help safeguard the integrity of the research, protect against data breaches, and ensure compliance with data privacy regulations.

The mission alignment pillar in the Trusted CI Framework is a crucial aspect when establishing and evaluating cyber hygiene. It specifies four 'musts' that align the cybersecurity practices with the mission and goals of the research organization (see Figure 1).

Figure 1

Trusted CI Framework Mission Alignment Pillar with "Musts"


Mission
Stakeholders and obligations
Mission Alignment
Documentation of information assets
Classifying information assets

Note. Adapted from the Trusted CI Framework Implementation Guide

Exposure to this framework established a framework to issue specific, actionable cyber hygiene practices to safeguard research integrity and data security. According to Jackson et al. (2017), there are seven reasons for researchers to put cyber safety first:

1. **Comprehensive protection against threats**: Identifying and accounting for all relevant environmental systems, actors, and risks.
2. **Maximizing opportunities**: Optimizing relationships, resources, and options available in the environment.
3. **Establishing rigor**: Creating governance for actors and systems that specifies and enforces expected outcomes, behaviors, states, and processes.
4. **Minimizing risk**: Establishing a plan to reduce the size, quantity, and complexity of what a researcher is protecting by limiting attack points.

5. **Compartmentalization to contain threats**: Isolating elements that enable and control the system so that interactions are only allowed when essential for an intended purpose.
6. **Fault tolerance for resiliency**: Anticipating and addressing potential points of compromise or failure of system elements or security controls.
7. **Proportionality to balance security with mission**: Tailoring security strategies to match risk tolerances to allow for the creation of practical constraints imposed by the research goals and environment.

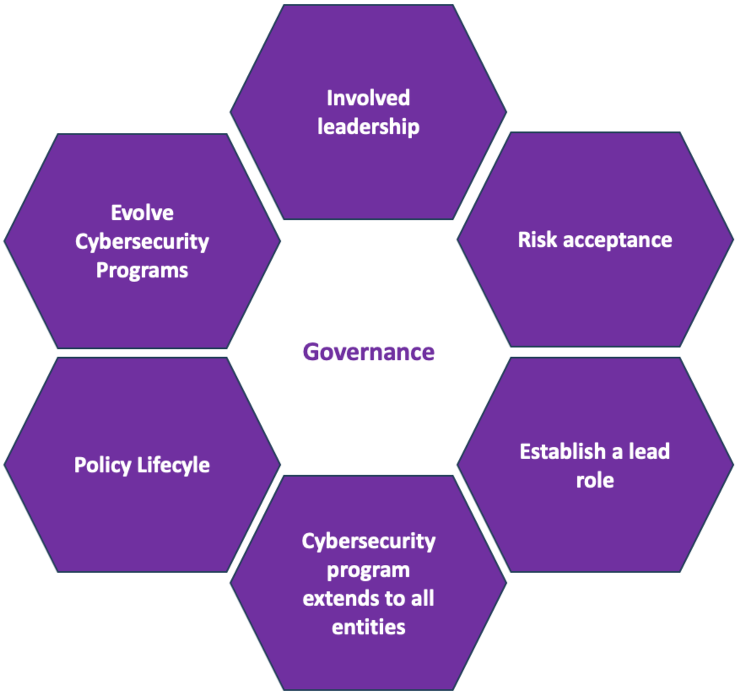
I was eager to bring this approach back to my home university. We immediately started implementing these principles with students involved in the human-centered research efforts at the USM Cybersecurity Awareness, Research, and Education Support (CARES) Center. These principles helped us enhance our safety and mission-focused culture. We used this pillar of the framework to produce well-aligned, specific, actionable cyber hygiene practices. We intend to research the value of a security culture within research organizations and demonstrate how cybersecurity is not just a policy but a vital component of routine daily operations.

Challenges in the Research Landscape

The governance pillar was extremely helpful in addressing challenges associated with involving the full extent of stakeholders, including senior academic leadership, in cybersecurity decisions. Governance is the most extensive of the four pillars involving "musts" dealing with people, policy, processes, and programs (see Figure 2).

Figure 2

Trusted CI Framework Governance Pillar with "Musts"



Note. Adapted from the Trusted CI Framework Implementation Guide

Like all who do investigative academic work, cybersecurity researchers face unique challenges that good governance can mitigate. However, now, as the lead for USM's efforts to evolve the CARES center, using the Trusted CI (Cyberinfrastructure) Governance model provided a forward-thinking approach to enhance the cybersecurity posture of the university and its students. This model is helping me emphasize critical areas such as involved leadership, risk acceptance, establishing lead roles, developing comprehensive cybersecurity programs, refreshing the policy lifecycle, and continuous evolution with students and fellow researchers within our cybersecurity programs. Integrating these principles into the university's current and future cybersecurity initiatives will significantly enhance their effectiveness and impact.

Involved Leadership

Leadership involvement is crucial for the success of cybersecurity initiatives (Jackson, Russell, & Sons, 2017). At USM, the CARES leaders and instructors are aware of and actively participate in leadership processes within our programs. This involvement can range from providing strategic direction and ensuring the allocation of adequate resources to cybersecurity efforts to championing cybersecurity awareness across the campus. Leadership's commitment is also essential in fostering a security culture among students, faculty, and staff.

Risk Acceptance

Risk acceptance is a pragmatic component of any cybersecurity strategy. The CARES leadership and departmental faculty spend time identifying and assessing cybersecurity risks and deciding which risks are acceptable and require mitigation. This process is crucial in effectively prioritizing resources and efforts. For the future Cybersecurity Operations Center classroom and the proposed cyber clinic, understanding and accepting the inherent risks will guide the development of robust measures to mitigate those risks without impeding these initiatives' innovative and educational goals.

Establishing Lead Roles

Designating lead roles for cybersecurity initiatives is critical for accountability and effectiveness. At USM CARES, this involves appointing dedicated individuals or teams responsible for programs within the Cybersecurity Awareness and Education Support Center. While faculty advise and are involved, we use student leaders for the cyber defense team and the Cybersecurity Ambassador programs, and we intend to do the same with the future cyber clinic. These student leaders would be responsible for planning, implementing, and continuously improving their areas of participation within CARES programs, thus ensuring alignment with the best practices for cybersecurity strategy.

Developing Comprehensive Cybersecurity Programs

The university's CARES Center cybersecurity programs include research using the cyber clusters, supporting a cyber defense team known as the Husky Hackers, and doing community outreach with the Cybersecurity Ambassador program. Programs such as these are foundational elements of its cybersecurity education and awareness efforts. Expanding these programs to be multidisciplinary and eventually integrating them into the Cybersecurity Operations Center classroom curriculum ensures a holistic approach to cybersecurity education. This comprehensive coverage is essential in creating a pervasive cybersecurity awareness and preparedness culture.

Refreshing the Policy Lifecycle

Cybersecurity policies must be dynamic, reflecting the evolving landscape of cyber threats and technological advancements. The development of the cyber clinic will be a mechanism where USM students can use their education regarding cybersecurity policy lifecycles and share that with state, local, and tribal governments as a starting point. Eventually, these classes that teach processes for regularly reviewing, updating, and communicating cybersecurity policies will ensure students understand those relevant and practical for clients. This experiential model will reinforce this policy lifecycle refreshment imperative while helping our communities maintain a robust cybersecurity posture. In this way, students and stakeholders will understand that policies support rather than hinder the educational and operational objectives of the university.

Evolving Cybersecurity Programs

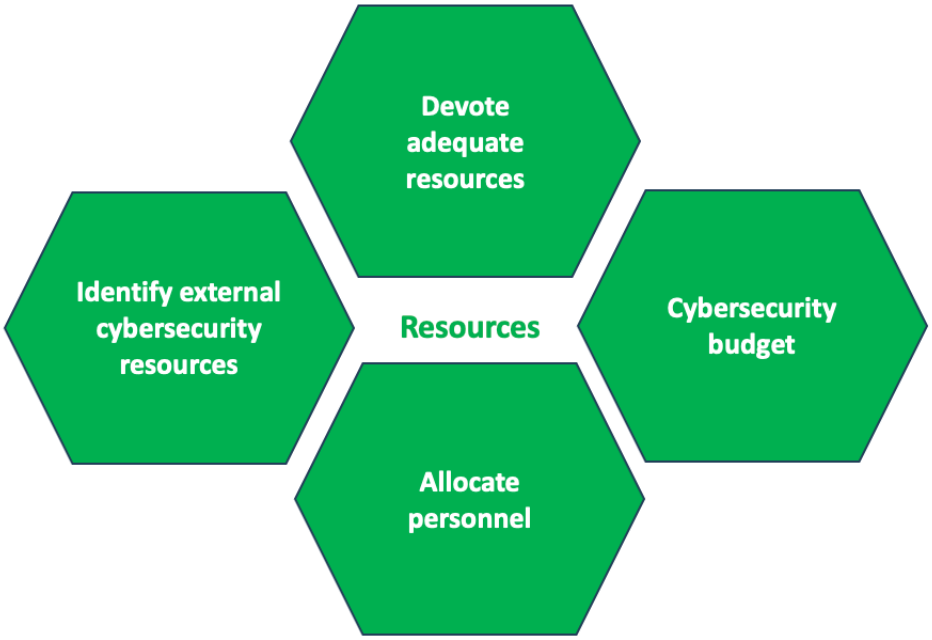
Continuous improvement is a vital principle of the Trusted CI model. The university's cybersecurity initiatives are now regularly evaluated and evolved based on new threats, technological advancements, and educational needs. The development of the Cybersecurity Operations Center classroom and the proposed cyber clinic offer opportunities to integrate the latest cybersecurity tools, practices, and learning methodologies, ensuring that students and participants gain relevant and practical experience.

Identifying the Specificity Gaps

Identifying, attaining, and allocating cybersecurity resources in a state university poses a complex challenge, given the dynamic landscape of cybersecurity threats and the unique constraints of academic environments. State universities must navigate these evolving threats, ensuring that sensitive data and infrastructure are protected while addressing the diverse cybersecurity needs across various departments. Significant university budgetary shortfalls can hamstring university administrators' spending, thus complicating proposed investments in cybersecurity needs against other priorities such as faculty salaries and educational resources. For this reason, using the Trusted CI Resource Pillar as a guide for USM CARES Center funding is imperative. The model focuses on identifying, developing, budgeting, and allocating critical resources such as people and money.

Figure 3

Trusted CI Framework Resource Pillar with "Musts"


Devote adequate resources
Identify external cybersecurity resources
Resources
Cybersecurity budget
Allocate personnel

Note. Adapted from the Trusted CI Framework Implementation Guide

The procurement process in public universities, characterized by its slow pace and bureaucracy, adds another layer of difficulty. Delaying the acquisition of essential cybersecurity tools and technology can make these Trusted CI Resource processes difficult.

Grants Must Bridge the Gap Between Resource Identification and Acquisition

One significant challenge is the imbalance between funding for personnel and equipment. While capital outlays for cybersecurity equipment might occasionally be secured, finding recurring funds for hiring skilled cybersecurity professionals proves more difficult. This personnel funding shortfall is exacerbated by a global cybersecurity talent shortage, making it challenging for universities to attract and retain the skilled personnel necessary for a robust cybersecurity posture (The White House, 2023). Universities often need help allocating resources effectively across their complex networks and myriad endpoints, further complicating their cybersecurity efforts.

Moreover, many cybersecurity initiatives in academia depend on grant funding, which is highly competitive and may require matching funds or other difficult-to-meet conditions. Grants typically support specific projects for limited durations, leaving a gap in long-term funding for ongoing cybersecurity operations. Also, a funding model that frequently prioritizes equipment purchases over the essential personnel needed to manage and operate that equipment effectively compounds the problem and reduces the implementation of cybersecurity tools and equipment.

To overcome these challenges, USM explores several strategies. Forming partnerships with government agencies, other universities, the private sector, and professional associations helps share resources and knowledge, extending the reach and effectiveness of cybersecurity efforts. Additionally, leveraging academic resources, such as engaging students in cybersecurity projects and research, can help mitigate resource constraints. Advocating for cybersecurity funding by raising awareness among stakeholders, including state legislators and university boards, is crucial for prioritizing and increasing resources dedicated to cybersecurity. However, it is difficult to get dedicated staff. As such, the USM Department of Technology researchers seek out and apply for cybersecurity grants to secure external funding. However, the inability to get stable funding often puts other efforts to secure our cybersecurity research at risk.

Balancing the complex needs of cybersecurity with the constraints of the academic environment requires strategic planning, continuous advocacy, and creative resource management. By fostering a culture of security awareness and exploring innovative solutions, we continue to navigate these challenges to enhance the CARES Center's cybersecurity posture.

Inculcating Students with an Understanding of Cyber Hygiene for Researchers

The intersection of cyber hygiene with research ethics and compliance is a critical area that demands attention in the modern digital landscape. Researchers increasingly rely on digital tools and data, so one cannot overstate the ethical implications of protecting this information. Cyber hygiene practices are not merely technical safeguards but fundamental to maintaining research data's integrity, confidentiality, and availability. These hygiene practices intertwine directly with principles of research ethics, which demand respect for privacy, consent, and the protection of sensitive information.

At the core of this intersection is the principle that ethical research practices extend to how data is managed and protected. Researchers must be adept in cyber hygiene practices to ensure that they do not expose personal and sensitive data to unauthorized access or breaches, which could have devastating consequences for research participants and the validity of the research itself. Compliance with data protection regulations, such as the Family Educational Rights and Privacy Act (FERPA), is a legal requirement but also reflects a commitment to ethical research practices. Educating researchers on cyber hygiene is essential in this context, as it empowers them to meet these obligations effectively.

Furthermore, ensuring data integrity goes beyond individual researchers to encompass institutions and funding bodies. They must support and enforce strong cyber hygiene practices through policies, training, and resources. This comprehensive approach at the CARES Center ensures that all stakeholders are aware of the risks and equipped with the knowledge and tools to mitigate them. By embedding cyber hygiene within the framework of research ethics and compliance, this academic community can uphold the highest standards of integrity and trust in their work, protecting both their subjects and the validity of their research contributions (Vishwanath et al., 2020).

Learning Baseline Controls

Inculcating core components of adequate cyber hygiene in students, especially those embarking on a research path, is essential in safeguarding the integrity and confidentiality of their work. The digital realm is fraught with vulnerabilities, and researchers, who frequently handle sensitive data, must be adept at protecting this information from cyber threats. The foundational step in this educational journey involves establishing a solid baseline of cyber hygiene practices. This baseline serves as the minimum standard for security measures. It includes practices such as using strong, unique passwords, enabling two-factor authentication, regularly updating software to patch vulnerabilities, and understanding the basics of data encryption. Educators should focus on making these practices second nature to students, ensuring they have a solid foundation to build more advanced cybersecurity skills.

Learning Additional and Alternate Controls

Once students are comfortable with these baseline practices, the curriculum can introduce additional and alternate controls tailored to the specific needs and threats in various research fields. Further controls include teaching students about advanced endpoint protection tools, secure coding practices for those involved in software development, and the importance of secure data storage and transmission methods. It is crucial to emphasize the dynamic nature of cyber threats and the corresponding need for adaptive and evolving cybersecurity measures. Educators should encourage critical thinking and problem-solving skills, allowing students to analyze and decide when additional controls are necessary and how to implement them effectively. Through hands-on exercises, simulations, and real-world case studies, students can see the practical application of these controls and understand their importance in protecting research integrity. This approach prepares students to defend their work and contributes to the research community's broader cybersecurity awareness and resilience culture.

Conclusion

Adopting the Trusted CI model has and will continue to significantly enhance the effectiveness of the University of Southern Maine's cybersecurity initiatives. The university can create a resilient cybersecurity infrastructure by fostering involved leadership, embracing risk management, establishing clear responsibilities, developing comprehensive programs, maintaining dynamic policies, and committing to continuous evolution. This approach not only enhances the educational experience but also prepares students to address the cybersecurity challenges of the future effectively.

The integration of the Trusted CI model into the development of the USM CARES Center and its future initiatives, such as the Cybersecurity Operations Center classroom and the cyber clinic, promises to create powerful platforms for experiential learning and community support. These initiatives will serve as benchmarks for how educational institutions can leverage governance models to enhance cybersecurity education and outreach, ultimately contributing to a more secure cyber environment.

References

Chief Information Officer, U.S. Department of Defense. (2021, December). Cybersecurity Maturity Model Certification (CMMC) Model Overview. Version 2.0. (Office of the Undersecretary of Defense, Acquisition and Sustainment, Washington, D.C.) https://dodcio.defense.gov/CMMC/Model/

Chief Information Officer, U.S. Department of Defense. (n.d.). Five Steps to Make Your Company More Cyber Security. (Office of the Undersecretary of Defense, Acquisition and Sustainment, Washington, D.C.) https://dodcio.defense.gov/CMMC/Implementation/

Gibson, William. (1084) *Neuromancer*. Ace.

Jackson, C., Russell, S., and Sons, S. (2017). *Security from first principles: A practical guide to the information security practice principles.* O'Reilly.

Jackson, C., Cowles, B., Russell, S., Adams, E. K., Kiser, A., Ricks, R., and Shanker, A. (2021) The Trusted CI Framework implementation guide for research cyberinfrastructure operators, Version 1.0. (National Science Foundation (NSF) Cybersecurity (Center of Excellence). https://www.trustedci.org/framework

Ross, R., Pillitteri, V., Dempsey, K., Riddle, M., and Guissanie, G. (2020). Protecting controlled unclassified information in nonfederal systems and organizations. (Department of Commerce, Washington, D.C.), NIST Special Publications (NIST SP) 800-171, Includes Updates as of January 28, 2021. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf

The White House. (2023) National Cybersecurity Strategy. https://www.easybib.com/guides/citation-guides/how-do-i-cite-a/how-to-cite-a-white-house-press-briefing/

Vishwanath, A., Neo, L. S., Goh, P., Lee, S., Khader, M., Ong, G., & Chin, J. (2020). Cyber hygiene: The concept, its measure, and its initial tests. *Decision Support Systems, 128*, 113160. https://doi.org/10.1016/j.dss.2019.113160