Cybersecurity and Research are not a Dichotomy

How to form a productive operational relationship between research computing and data support teams and information security teams

Deb McCaffrey*
Health Information & Technology Services, Michigan Medicine
debmccaf@med.umich.edu

Jessica Kelley*
Information Assurance: Michigan Medicine, Michigan Medicine
kelleyje@med.umich.edu

ABSTRACT

Cybersecurity and research do not have to be opposed to each other. With increasing cyberattacks, it is more important than ever for cybersecurity and research to corporate. The authors describe how Research Liaisons and Information Assurance: Michigan Medicine (IA:MM) collaborate at Michigan Medicine, an academic medical center subject to strict HIPAA controls and frequent risk assessments. IA:MM provides its own Liaison to work with the Research Liaisons to better understand security process and guide researchers through the process. IA:MM has developed formal risk decision processes and informal engagements with the CISO to provide risk-based cybersecurity instead of controls-based. This collaboration has helped develop mitigating procedures for researchers when standard controls are not feasible.

CCS CONCEPTS

• **Security and privacy** → Human and societal aspects of security and privacy; Usability in security and privacy.

KEYWORDS

risk management, HIPAA, research computing and data, information security, cybersecurity, workforce development, relationship building

ACM Reference Format:
Deb McCaffrey and Jessica Kelley. 2022. Cybersecurity and Research are not a Dichotomy: How to form a productive operational relationship between research computing and data support teams and information security teams. In *Practice and Experience in Advanced Research Computing (PEARC '22), July 10–14, 2022, Boston, MA, USA.* ACM, New York, NY, USA, 4 pages. https://doi.org/10.1145/3491418.3535180

1 INTRODUCTION

Cyberattacks have been increasing steadily for the past decade, but the Russian invasion of Ukraine in February 2022 led to an unprecedented increase in attacks, notably from nation-states. It is more important than ever to secure all forms of infrastructure. At many institutions, however, the relationship between research computing and data (RCD) and information security seems contentious. This is what the authors experience anecdotally, at least.

Michigan Medicine (MM), the University of Michigan's academic medical center, published a paper last year about their Research Liaison program [5]. It stresses the value of establishing relationships with service providers to help provide a better experience for researchers. Given the current cybersecurity crisis, the authors wanted to elaborate on one relationship in particular: the relationship between the Research Liaison team, represented by D. McCaffrey, and the cybersecurity unit, Information Assurance: Michigan Medicine (IA:MM), represented by J. Kelley.

RCD professionals have certainly been concerned with cybersecurity for many years. This is evident in the numerous papers for research specific cybersecurity tools [3, 4, 7–9]. However, this isn't always apparent to cybersecurity teams because it often doesn't resemble standard controls. When RCD and cybersecurity teams have a more collaborative relationship instead of an adversarial one, this leads to products that are both innovative and secure [1, 2, 10]. The purpose of this paper is to describe how this relationship works at MM in the hopes that other institutions can replicate it.

2 THE MICHIGAN MEDICINE ENVIRONMENT

Michigan Medicine is an academic medical center, meaning that it combines clinical care, education, and research. It is financially separate from the University of Michigan and is subject to HIPAA. Because of this, it has a separate network from UM, complete with firewall, and its own Chief Information Security Officer (CISO) in addition to the University of Michigan's CISO.

The IA:MM program consists of offensive and defensive teams working towards a common goal; confidentiality, integrity, and availability of systems, services, and data. They address risk management with a lifecycle consideration. This means assurances are to be considered through planning, provisioning, operation, and decommissioning of technology. For researchers, this means that the network is more strictly controlled and everything but managed services must be assessed for risk.

The art of assuring research initiatives is a continuous learning experience. While there are established frameworks applied to information security, IA:MM anticipates new technological initiatives that exist outside the parameters of a typical investment. These scenarios are often presented by academic research. The progressive impact is welcomed and appreciated as we continue to mature

*These authors contributed equally.

PEARC '22, July 10–14, 2022, Boston, MA, USA

ACM ISBN 978-1-4503-9161-0/22/07…$15.00
https://doi.org/10.1145/3491418.3535180

our security program through strategy, operations, technology, and most importantly, relationships. Alignment and partnership between teams can help expedite processes that without context and understanding may be perceived as barriers.

3 THE IA:MM LIAISON

The Research Liaison team [5], charged with guiding researchers through the MM environment, needed some guidance themselves when it came to information security procedures. A lack of understanding around security processes led to frustration and delays that set back research project timelines significantly. To smooth out the process, the Research Liaison team requested their own IA:MM Liaison.

The IA:MM Liaison is the main point of contact for the Research Liaison team. They also attend the weekly liaison Research Liaison team meetings so that both sides can stay updated on each other's work. Often, the IA:MM Liaison provides context behind the procedures and documents that researchers need to do, translating some of the "security speak." Knowing the intent of these controls allows for mitigating controls to address risk when standard controls aren't feasible. The IA:MM Liaison also serves as a point of escalation when service requests fall through the cracks or communication breaks down with other risk analysts.

Consider the transmission of data flow in a computer's network. The ultimate objective is to ensure information is received by its intended recipient while the integrity of the message is preserved. The implementation of liaisons between teams shares a similar objective. To clarify positioning, we have research teams, technology service providers, and an assurance team that works towards security best practice. Between the roles are opportunities for improved communication and partnership. IA:MM Liaisons and Research Liaisons are intended to serve as intermediary support. This works in a cyclical fashion. While the IA:MM Liaison works to bridge gaps between the Information Assurance department and Research Liaisons, the Research Liaisons return that value by working directly with study teams that rely on MM infrastructure. They help to guide the research community though IA:MM internal processes and terms while creating a common ground that we can all stand upon.

For example, consider a study in which two separate universities share and store participant's data. The Principal Investigator (PI) engages their technology department and submits the request for the creation of a web application and database that will house and process the data. One week later the Principal Investigator is contacted by a security analyst requesting technical details that seem out of scope from their normal duties. This may cause the Principal Investigator feelings of frustration and worry. Two important aspects missing from this example are alignment and context. The implementation of liaisons working between researchers and information assurance has allowed MM to eliminate a culture of internal auditing and uplift the shared responsibility of information security.

4 ACCOMODATING CONFLICTING NEEDS

Unsurprisingly, there are many MM required controls that can't always be met due to conflicting business needs. Instead of taking a binary controls-based approach, IA:MM uses a risk-based approach based off Odell [6]. This framework allows for consideration of the attacker's incentive and the impact of the investment when making risk decisions. A tangible example is the need for deprecated databases that store historical research information. The risk of an unsupported or unpatched database is real, but the scientific value of the data is also real. A proven model to help bring balance amongst teams has been attitude and understanding. When all teams understand the "why" behind what is being asked, we can help each other achieve individual interests. The Research Liaison team, as well as the rest of the RCD staff, can use the Risk Decision Request (RDR) for official risk decisions. They can also work directly with the CISO for unique solutions.

4.1 Risk Decision Request process

Historically, balancing security and innovation has been a challenge. For example, there is a continuous conflict between grant funded research study deadlines and the process of assurance. Before a new system is deployed in the MM environment it must undergo a partnered risk assessment. If the findings of the assessment are unsatisfactory, the owner of the technology is tasked with remediation and/or mitigation of the risks (opportunities for threats to exploit vulnerabilities). The research community benefits from a more streamlined process which is why risk management techniques such as Odell's "4 T's" are being leveraged. Terminate, Tolerate, Transfer, or Treat are four options to consider when a risk(s) has been identified within a system or process [6]. In the above example of the historical database, the research team can ask for a temporary Toleration so they have time to implement a new solution and migrate the data. This will keep the database from being Terminated.

Another common example of 4 T's applicability is when a system is being built to support a grant funded research study that is extremely time sensitive. The standard process of assurance has the potential to negatively impact the success of the study. In this scenario, should we move forward with the research initiative and ignore the need for a security assessment, or should we delay the study and secure the technology? There are many factors to consider: data sensitivity, data flow, transmission techniques, etc. On behalf of the study team, the assigned Research Liaison is authorized to request a provisional authorization to operate in lieu of a permanent shared responsibility agreement. Leveraging the Treat option will require a documented plan to address the portions of the assessment that were unable to be completed. This may be due to both the sensitive timeline and the unavailability of IA:MM resources.

4.2 Collaborating directly with the CISO

For more complex issues and advice, the CISO offers to work directly with teams. He has biweekly office hours open to the research computing and data support teams to work through operational issues that have come up. Most issues are about how to achieve the controls that IA:MM has instructed them to implement, which is often nontrivial. The CISO will also provide commentary in RDRs that get stuck on details. Research teams can also request to work with the CISO directly when quick turnaround is necessary.

5 EXAMPLES

These activities have led to a fruitful partnership that has minimized the amount of time to complete security requirements for research workflows. As a testament to the success, the IA:MM Liaison role transitioned to a new analyst when the first analyst took a new position. Here are a few examples of the work achieved.

5.1 Advanced Genomics Core

One example where this relationship has helped is with MM's Advanced Genomics Core (AGC) that offers sequencing services to researchers. For business continuity purposes, AGC purchases service contracts for their (often unique) equipment. These contracts forbid anyone but the vendor from modifying the equipment configuration.

This scenario has come into conflict with cybersecurity requirements twice within a few months of writing this manuscript. The first was a NextSeq 2000 that AGC wanted to connect to the wired network. In the process of assessing the device, it was discovered that the NextSeq uses privileged local accounts to run processes and joining it to Active Directory would interfere with them. The vendor has stricter password controls than MM requires though, so it went through an RDR for Toleration with the help of the CISO through office hours.

The second was a server component of a GeoMX Digital Spatial Profiler. It had multiple critical vulnerabilities that needed to be addressed, but the vendor would not be patching them before the mitigation due date. With the guidance of the IA:MM Liaison, it went through an RDR for an extension on the due date based on the vendor's timeline for patching.

5.2 Research IoT device category

AGC is not the only group with service contracts that prevent modifications. Even without service contracts, it is not always possible to add controls like encryption and joining to Active Directory. With increasing attacks from nation states, the incentive to attack these devices has increased and they are becoming more of a risk. They need more mitigating controls to remain on the network.

Because these devices can't be modified, they are practically the same as IoT devices, like internet toasters. To simplify, reframe the question as "How do I secure an internet toaster?" Segment it and apply more restrictive firewall policies. The Research Liaisons next worked on a high-level list of connections that these Research IoT devices would require, such as access to network storage and vendor monitoring services. The Research Liaisons will be working with the networking team on an appropriate implementation of these requirements.

Currently, out of date devices, such as Windows 7 devices, are not allowed on the network. It is unclear if this solution will be adequate for such devices.

5.3 Research devices without ePHI

Network Access Control is the technique that governs which devices can connect to an MM network. Similar to most enterprise environments, our network is segmented. This can be imagined as logical partitions. MM's standard process requires that before a research device can connect to our intranet, an assessment of the device must be performed. The parameters of the assessment are dependent on the data sensitivity involved and the classification of the device. One component of the research device assessment is a vulnerability scan. You may be wondering, how does one complete a scan without network access? This is a prime example of how research and security efforts combined require people in addition to processes. The onboarding method of research devices will vary, but having a segmented network specifically for unassessed technology is highly recommended. This allows us to prevent the delay of studies while isolating devices that present an elevated risk. MM currently leverages two different processes for onboarding and may continue to expand this effort as the need increases.

6 FUTURE WORK

To assist more with risk assessments, the MM RCD teams recently hired a business systems analyst whose primary responsibility is to guide researchers through all the required security processes, such as vulnerability scans and vendor questionnaires. They have already helped the Liaisons tremendously by taking over on some assessments. The Liaisons look forward to seeing this position evolve more in the future.

The Research Liaisons are also partnering with IA:MM's Education and Awareness team to create security documentation specifically for research audiences. The goals are twofold: to help researchers see themselves in institutional shared responsibility and create a central location to explain all security requirements that they could possibly encounter. This will hopefully prevent unfortunate situations, such as when researchers buy incompatible devices because they didn't consult with any RCD teams beforehand. It is also intended to create a cybersecurity safety culture long term. At the same time, service providers are reducing the financial and time burdens to move to the more secure, enterprise services. For example, we provide faculty with 80,000 CPU hours on the clusters, 10TB active storage, and 100TB archive storage at no cost. We've also decided to centrally fund primary computers for faculty and students in the medical school. That project had a successful first year of implementation and will continue to roll out over the next few years.

7 CONCLUSION

The cyberthreat landscape is changing. The relationship between RCD and information security cannot remain contentious. Researchers cannot continue gambling with insecure equipment, but neither can information security slow down research productivity. We have discovered that this apparent dichotomy of priorities is just a lack of shared context. By staying in constant communication and continuing our education, the Research and IA:MM Liaisons maintain that shared context. This has benefited our researchers tremendously: procedures run with fewer delays and mitigating procedures have been developed to account for research workflows. We look forward to continued collaboration on behalf of Michigan Medicine's research mission.

8 ACRONYMS

AGC: Advanced Genomics Core; CISO: Chief Information Security Officer; IA:MM: Information Assurance: Michigan Medicine;

MM: Michigan Medicine; PI: Principal Investigator; RCD: Research Computing and Data; RDR: Risk Decision Request

ACKNOWLEDGMENTS

The authors acknowledge the Michigan Medicine Research Liaisons for their effort in this relationship, particularly Ryan Echlin for his "internet toaster" language. We acknowledge the Michigan Medicine CISO, Jack Kufahl, for background on risk frameworks and his effort in this relationship. We acknowledge Rob ZurSchmiede for his role as the previous IA:MM Liaison.

REFERENCES

[1] Andrew Adams, Craig Jackson, Ryan Kiser, Mark Krenz, Jim Marsteller, Barton P. Miller, Sean Peisert, Scott Russell, Susan Sons, Von Welch, John Zage, Kay Avila, Jim Basney, Dana Brunson, Robert Cowles, Jeannette Dopheide, Terry Fleury, Elisa Heymann, and Florence Hudson. 2019. Trusted CI Experiences in Cybersecurity and Service to Open Science. In Proceedings of the Practice and Experience in Advanced Research Computing on Rise of the Machines (learning) - PEARC '19, ACM Press, Chicago, IL, USA, 1–8. DOI:https://doi.org/10.1145/3332186.3340601

[2] Jason Christopher, Gary Jung, and Christopher Doane. 2019. Making it More Secure: The Technical and Social Challenges of Expanding the Functionality of an Existing HPC Cluster to Meet University and Federal Data Security Requirements. In Proceedings of the Practice and Experience in Advanced Research Computing on Rise of the Machines (learning) - PEARC '19, ACM Press, Chicago, IL, USA, 1–5. DOI:https://doi.org/10.1145/3332186.3332250

[3] Erik Deumens, Thomas Samant, Eric Byrd, Samuel Porter, Axel Haenssen, Curtis W. W. Hillegas, Elizabeth Holtz, and Irene Kopaliani. 2021. Secure Research Infrastructure Using tiCrypt. In Practice and Experience in Advanced Research Computing, ACM, Boston MA USA, 1–8. DOI:https://doi.org/10.1145/3437359.3465577

[4] Kuan-Ching Li, Nitin Sukhija, Elizabeth Bautista, and Jean-Luc Gaudiot (Eds.). 2022. Cybersecurity and high-performance computing environments: integrated innovations, practices, and applications (First edition ed.). CRC Press, Boca Raton, FL.

[5] Deb McCaffrey, John Brussolo, Ryan Echlin, John Herlocher, Einor Jacobsen, Lovida Roach, Amy Yamasaki, Dan St. Pierre, and Erin Dietrich. 2021. Research Liaisons: the next layer of Facilitation: Research Liaisons. In Practice and Experience in Advanced Research Computing, ACM, Boston MA USA, 1–6. DOI:https://doi.org/10.1145/3437359.3465568

[6] Laura A. Odell. 2016. Data to Decisions—Terminate, Tolerate, Transfer, or Treat. Institute for Defense Analyses, Alexandria, VA. Retrieved from https://apps.dtic.mil/sti/pdfs/AD1106083.pdf

[7] Sean Peisert, Eli Dart, William Barnett, Edward Balas, James Cuff, Robert L Grossman, Ari Berman, Anurag Shankar, and Brian Tierney. 2018. The medical science DMZ: a network design pattern for data-intensive medical science. Journal of the American Medical Informatics Association 25, 3 (March 2018), 267–274. DOI:https://doi.org/10.1093/jamia/ocx104

[8] Wirawan Purwanto, Hongyi Wu, Masha Sosonkina, and Karina Arcaute. 2019. DeapSECURE: Empowering Students for Data- and Compute-Intensive Research in Cybersecurity through Training. In Proceedings of the Practice and Experience in Advanced Research Computing on Rise of the Machines (learning) - PEARC '19, ACM Press, Chicago, IL, USA, 1–8. DOI:https://doi.org/10.1145/3332186.3332247

[9] Isuru Ranawaka, Suresh Marru, Juleen Graham, Aarushi Bisht, Jim Basney, Terry Fleury, Jeff Gaynor, Dimuthu Wannipurage, Marcus Christie, Alexandru Mahmoud, Enis Afgan, and Marlon Pierce. 2020. Custos: Security Middleware for Science Gateways. In Practice and Experience in Advanced Research Computing, ACM, Portland OR USA, 278–284. DOI:https://doi.org/10.1145/3311790.3396635

[10] Shivam Trivedi, Lev Gorenstein, Erik Gough, Alex Younts, Xiao Zhu, Lauren Featherstun, Nathan DeMien, Callum Gunlach, Sagar Narayan, Jacob Sharp, Brian Werts, Lipu Wu, and Carolyn Ellis. 2019. PULSAR: Deploying Network Monitoring and Intrusion Detection for the Science DMZ. In Proceedings of the Practice and Experience in Advanced Research Computing on Rise of the Machines (learning) - PEARC '19, ACM Press, Chicago, IL, USA, 1–8. DOI:https://doi.org/10.1145/3332186.3333058