Effective Cybersecurity for Research

June 20, 2022

Anurag Shankar and Will Drake[1]
Center for Applied Cybersecurity Research
Indiana University

[1] Email: ashankar@iu.edu, wildrake@iu.edu

Abstract

The tension between cybersecurity and researchers has long hampered attempts to secure research. It is also why institutional cybersecurity efforts in academia have been confined to the most sensitive research. The status quo has persisted for other reasons as well, for instance the complexity of the research environment, but latest developments in the regulatory and cyber threat landscape are quickly changing the status quo. Funding requirements scoped beyond individual awards and newly evolving threats are pointing to a future where securing research *holistically* is no longer optional. This paper describes an approach to cybersecurity for research that is showing great promise in breaking the security versus research impasse. A product of years of effort at Indiana University, it focuses *exclusively* on the researcher and the research mission, reduces the cybersecurity and compliance burden on the researcher, and aims to secure *all* research. It has been stress tested on campus, with success evidenced by researchers embracing it *voluntarily* and research being accelerated *measurably*.

Introduction

In 2021, the White House issued presidential memorandum NSPM-33[2] directing all federal agencies to mandate institutions receiving $50 million or more annually in federally funded research to establish a "research security" program. In January 2022, further guidance[3] was provided by the National Science and Technology Council (NSTC) on elements of the program that agencies should require, including a set of cybersecurity controls[4]. NSPM-33 applies to *all* research on campus, not just individual awards with cybersecurity terms and conditions.

In 2015, former U.S. Director of National Intelligence James Clapper predicted that, *"While most of the public discussion regarding cyber threats today is focused on the confidentiality and availability of information, in the future, however, we might also see more cyber operations that will change or manipulate electronic information in order to compromise its integrity (i.e., accuracy and reliability) instead of deleting it or disrupting access to it."* It became a reality recently when a malware attack against a podiatric practice not only encrypted patient data but also altered it[5]. While no *known* incidents of malicious modification of research data have been reported, conventional cyberattacks on researchers engaged in controversial fields are already common. Only by securing research at large will it be possible to mitigate threats against research data integrity and to protect not only researchers but also the credibility of the research enterprise *itself*.

While the need to secure all research is growing, securing *any* research is a challenge in academia. The top-down approach to cybersecurity is simply not effective for research. It often creates risk instead, especially when controls that get in the way of research are bypassed or subverted. Any solution to the cybersecurity for research impasse must begin first by addressing the friction between cybersecurity and research. It must reverse the perception many researchers have, namely that cybersecurity is an obstacle that slows research down.

As cybersecurity requirements increasingly find their way into terms and conditions for grants, contracts, and data use agreements, sponsored research and information security offices in academia are realizing the need for a viable strategy to secure research. Indiana University (IU) began facing this challenge nearly two decades ago with HIPAA which was then a brand new regulation. The resulting struggle has been long and painful but also fruitful, culminating in an approach to protect *all* research that is showing great promise on campus. The purpose of this paper is to share IU's journey and lessons learned with the broader community in the

[2] "National Security Presidential Memorandum on United States Government-Supported Research and Development National Security Policy", https://trumpwhitehouse.archives.gov/presidential-actions/presidential-memorandum-united-states-government-supported-research-development-national-security-policy/

[3] "GUIDANCE FOR IMPLEMENTING NATIONAL SECURITY PRESIDENTIAL MEMORANDUM 33 (NSPM-33) ON NATIONAL SECURITY STRATEGY FOR UNITED STATES GOVERNMENT-SUPPORTED RESEARCH AND DEVELOPMENT", https://www.whitehouse.gov/wp-content/uploads/2022/01/010422-NSPM-33-Implementation-Guidance.pdf

[4] A majority of the controls (12 out of 14) are from NIST Special Publication 800-171

[5] https://www.inforisktoday.com/ransomware-attacks-data-integrity-issues-a-11917

hope that they will be of benefit to others looking to establish a cybersecurity program for research on their campus.

History

IU's secure research effort dates to the early 2000s when the IU School of Medicine received a large award to accelerate genomics research. A key component of the proposed work was the use of IU's central research cyberinfrastructure for large scale genomic data analysis. The presence of patient data and the new HIPAA Security Rule requirements in 2005 created for the first time the need to not only secure systems but also the researchers. After implementing HIPAA safeguards in 2009, we launched a campaign to advertise our HIPAA-compliant "supercomputers", "high performance storage", etc., to the clinical researchers. The beginning of our education in cybersecurity for research is marked by the utter and complete failure of the campaign to produce clients. We had expected clinical researchers to respond to our offerings like the "usual suspects" (physical scientists and engineers) who were always eager to consume anything we threw at them. Instead, we found that the doctors simply did not "speak HPC." The language barrier prevented them from recognizing how the offerings were even relevant to their research. The lesson taught us to ask, "What is it that you are trying to achieve?" instead of bragging, "Look what great toys we have for you." In time, our hopes to teach them cybersecurity and compliance also became a casualty of our ignorance as we gained insight into the pressures that researchers face.

Over the years, these and other lessons transformed the secure research service from merely offering compliant systems to injecting cybersecurity and compliance into research projects *by default*. The support workflow evolved into collaborating one-on-one with researchers, understanding the research context, gathering requirements, designing compliant solutions, and combining them to develop secure workflows to solve the problem. This baking in of cybersecurity and compliance by the experts not only made researchers happy, it also *greatly* accelerated their research.

In 2020, we decided to pilot the clinical research model for all research on campus by launching a service called *SecureMyResearch*[6]. Its purpose was to test the feasibility and scalability of the approach with no expectations of success. Metrics and researcher feedback collected within a *year* of operation showed however that the service had exceeded all our expectations. It was adopted rapidly[7] and the number and variety of researchers that began using it *voluntarily* was beyond anything we had anticipated. Two years of service provision later, any fears we had initially of a lack of scalability have also disappeared. The evidence indicates clearly that *SecureMyResearch* has been successful at the institutional scale. It also

[6] https://securemyresearch.iu.edu
[7] despite the pandemic

shows that our approach is both feasible and scalable and vindicates the basic premise, namely that the institution must *supply* cybersecurity to its researchers[8], not expect it from them[9].

Research cybersecurity

While the approach we describe in this paper is not specific to research (the ideas apply universally), we decide to call it *Research Cybersecurity*[10] to limit discussion to our work, namely cybersecurity in the research context. We also give it a formal definition: *Research cybersecurity is the application of cybersecurity to research in a manner that accelerates research while limiting risk to the research mission*. The language was carefully chosen to be researcher- and mission-centric so as to deliver a message that is both appealing and immediately understood by researchers.

Research fundamentals

Securing research requires an insight into the research enterprise. The following fundamentals are the bare minimum to begin this process and to understand the role research cybersecurity can play.

1. *Research as a mission*. A research university features research prominently in its mission statement. Keeping this front and center at all times, research cybersecurity aims to enable, sustain, and accelerate the research mission. It accomplishes this by eliminating or reducing the cybersecurity and compliance burden on the researcher.
2. *Nature of research* A quest into the unknown rarely follows a straight path. It is often disorganized, unpredictable, and chaotic. Undesirable in other professions, these very characteristics are key to innovation in research. Other important ingredients include openness, collaboration, and innovative technologies. Research cybersecurity leverages the nature of research itself to develop innovative and flexible approaches to securing those technologies.
3. *Research lifecycle*. Research begins with a new idea, followed by the researcher engaging in a preliminary, unfunded effort to test its soundness and viability. If it is found to be promising, a research proposal with a budget is prepared and submitted to a suitable sponsor. The proposal goes through a peer review where the researcher addresses questions or issues raised by the reviewers. Based on their recommendations, the sponsor either funds or rejects the proposal. Even when the proposal is successful, the sponsor may trim the budget in case there are multiple deserving proposals. Once the funds arrive at the institution, students are hired, equipment acquired, and proposed research initiated. Data is collected, analyzed, shared, and results published. Finally, annual progress reports are submitted to satisfy award terms and conditions. The research may also lead to technology transfer, which is a tedious, time-consuming exercise. Compliance may add further complexity if the research is subject to rules and

[8] This is not to say that institutions do not provide *any* cybersecurity to researchers, only that it is not at a level and in a manner required for research.
[9] This is no different from technology. The institution provides IT to researchers to make them successful, not expect them to supply their own.
[10] not to be confused with cybersecurity research

regulations. At each and every point in the process, research cybersecurity strives to find ways to shorten the research lifecycle.

4. *Pace of research* The typical research funding cycle is 1-5 years depending on a specific request for proposal (RFP) and funds available. Institutional policies and procedures, hiring, acquisitions (software/hardware, etc.), and other prerequisites such as Institutional Review Board (IRB) approval for human subjects research further squeeze the researchers forcing them to rush to get their research done. Potentially negative consequences of the inability to complete the proposed research in time adds further pressure. Being scooped by competitors is also a possibility. All this conspires to make speed *essential* for success. Any obstacles that cybersecurity and compliance present only make researchers less competitive. Research cybersecurity actively seeks out ways to match the pace of research by facilitating the minimization of time from ideation to experimentation to results.

Research cybersecurity principles

Developing research cybersecurity over two decades and implementing it at scale as *SecureMyResearch* gave rise to what we consider the ten guiding principles of research cybersecurity.

1. *Focus*. Research cybersecurity is laser focused on accelerating research and reducing the cybersecurity and compliance burden on the researcher. It leverages controls to achieve its goals but recognizes that they are merely tools. It maintains a healthy balance between and means and ends and understands that an undue focus on controls[11] is inconsistent with a positive perception of cybersecurity.
2. *Success*. Research cybersecurity is successful when it is *invisible* to the researcher. It must be baked into solutions and support.
3. *Empathy*. Empathy for researchers is a *fundamental* prerequisite of research cybersecurity. Researchers are rarely able to only do research. Commitments like teaching, fulfilling administrative duties, writing proposals, competing for limited funds, guiding graduate students, and producing quality publications place relentless burdens on researchers, robbing them of the luxury of time. The pace of research further exacerbates this burden. Research cybersecurity uses these insights to develop empathy and human connection with researchers, making it easier to accelerate their work.
4. *Attitude*. Research cybersecurity maintains a positive attitude toward researchers. Instead of a "researcher is the weak link in the chain" mentality, it takes *upon itself* the responsibility of building in cybersecurity to enable researchers and the mission to be successful.
5. *Relationships*. Research cybersecurity uses interactions with researchers to establish long-term relationships and embeds itself into their ongoing research. It also cultivates strong

[11] The malady (which we facetiously call OCD - Obsession with Controls Disorder) makes cybersecurity myopic, neglecting what is most important, namely the customer and the mission.

connections with stakeholders that support research to facilitate better service and ombudsmanship for researchers.

6. *Perception*. Research cybersecurity creates a positive perception of cybersecurity[12]. It strives to be seen as a mechanism that removes obstacles and accelerates research and actively works to reverse the perception of being a hindrance.
7. *Messaging*. Research cybersecurity uses *only* positive messaging with researchers. It ties cybersecurity to research success and improved funding prospects–a message researchers relate to immediately. It portrays itself as a vehicle for giving researchers a "sense of security" by enhancing the efficiency, trustworthiness, and reproducibility of research[13].
8. *Efficiency*. To help researchers maintain the pace of research, research cybersecurity makes speed its single most important characteristic. To accomplish this, it maximizes the efficiency of every process and tool it uses.
9. *Comprehensivity*. Research cybersecurity takes a holistic approach to cybersecurity. It strives to secure entire research workflows, not just risk components such as systems and networks. It also anticipates future needs and actively prepares for them.
10. *Risk Acceptance*. Research cybersecurity is concerned with reducing risk to research. It appreciates that researchers subverting overly strict security measures only introduces additional risk and negatively impacts the mission. It recognizes that the highest risk is obstacles to research that threaten the mission. Research cybersecurity uses risk acceptance as a tactic to balance security and the mission, but always in favor of the mission.

Implementing research cybersecurity

The success of our clinical research cybersecurity model can be attributed to making cybersecurity (largely) invisible to researchers. This was achieved not by explicit design but trial and error. It is only in hindsight that we can articulate the process and nuances that led to IU's research cybersecurity program. The subsections below describe the details[14] as guidance to make them actionable for a potential implementer.

1. Determine resource needs

A successful program needs resources. The amount depends on factors such as the number of researchers on campus, types of research, rules and regulations in scope, and the presence or absence of solutions. To provide an estimate of human resources, implementing and delivering *SecureMyResearch* at IU[15] required 2 FTEs. This translates into roughly $250K annually in fully loaded salaries. Economies can obviously be achieved by leveraging or repurposing existing personnel. Other key resources include secure institutional IT solutions (including research computing

[12] Adversarial language such as "there will be breaches if you don't do X" is counterproductive to research cybersecurity (and likely to all cybersecurity).
[13] Research cybersecurity increases research efficiency by preventing data loss and instrument unavailability due to security incidents. This also accelerates research. By protecting against integrity attacks that undercut the public's confidence in research, research cybersecurity enhances trustworthiness and repeatability.
[14] They would have been extremely helpful twenty years ago
[15] an R1 campus with 6,000 full-time faculty and $700 million in annual sponsored funding.

solutions), many of which are typically already in place. We estimate that the total annual cost of a research cybersecurity program for a large, R1 campus is likely to be in the $250–$500K range. Such a (large) sum is challenging for smaller campuses, but the combination of smaller needs and strategies such as leveraging existing resources may still make a research cybersecurity program feasible.

Arguing for resources

Getting resources is always a challenge, especially in academia. A number of arguments for having a research cybersecurity program exist already, for example regulated data, NSPM-33 requirements, and integrity threats, but they are difficult to turn into hard numbers. To make a quantitative argument[16], one can try the following exercise.

- Determine the total research funding and overhead the institution receives. Using typical values of $500 million total with 50% overhead for an R1 institution, this amounts to $250 million annually.
- Estimate additional funding a program may enable from an increased ability to compete for awards with cybersecurity terms and conditions. Since this is not easy to calculate, we can lowball it at 1% of the total, which is $5 million.
- Determine the cost of incidents and breaches potentially prevented by a program. Using HIPAA as an example, lost data and productivity, litigation, patient notification, and the FTE effort to recover is estimated to be roughly $200 per patient record exposed. For a breach of 50,000 records, this translates into $10 million, excluding penalties that can also reach into millions.

Based on these numbers, we can easily draw the following conclusions:

- The cost of a research cybersecurity program ($500K) is a small fraction of the total overhead from sponsored research ($250 million).
- The program cost ($500K) is only 10% of the overhead ($5 million) from additional projects the program can enable.
- The program cost ($500K) is a small fraction of the cost of even a*single* breach ($10 million).

These may be usable as arguments in favor of a research cybersecurity program.

2. Dedicate personnel

Hiring the right people is key to program success. Unfortunately, there are very few qualified research cybersecurity professionals at present. The expertise gap will have to be filled by growing a new research cybersecurity workforce through training and practice. Until then, the

[16] While the numbers presented are not very precise, they should be in the right ballpark.

program will need an initial infusion of personnel who are interested in research cybersecurity and have (at least) a subset of the desired skills.

Designate a leader

A successful program requires a dedicated leader. Desired job qualifications include excellent interpersonal skills, ability to listen, empathy, experience in academia and in conducting or supporting research, research computing/IT experience, and a knowledge of security/compliance. A Ph.D. is also quite helpful to develop rapport with faculty. It is advisable to start by looking for potential, internal candidates. With luck, it may be possible to find a researcher with IT or security knowledge who is interested in helping other researchers. (At IU, the program is led by an ex-researcher with an IT, cybersecurity, and compliance background.) Program leader responsibilities include development, implementation, oversight, and refinement of the research cybersecurity program, liaison with internal and external stakeholders and the leadership, ombudsmanship/advocacy for researchers, and training and mentorship of new research cybersecurity personnel.

Designate analysts

The program also needs analysts who work in the trenches to deliver research cybersecurity to researchers. Desired qualifications include excellent interpersonal skills, empathy, ability to listen, customer support experience, IT/security experience, and a knowledge of academia and/or research. (At IU, we have successfully hired a junior IT person with no research and little cybersecurity experience and training and mentoring him to become a highly effective research cybersecurity analyst within a year.) A search may also reveal an IT-savvy undergraduate or graduate student interested in pursuing a research cybersecurity career.

Note: When reviewing candidates for research cybersecurity positions, intrinsic qualities of the person (such as attitude, service orientation, etc.) are much more important than formal skill sets. It is always possible to teach a person cybersecurity, but one cannot easily instill a desire to have a positive impact on research.

3. Provide training

Research cybersecurity requires taking into account many factors not appreciated or known today. Since trained research cybersecurity personnel are still a rarity, a new workforce wishing to engage in research cybersecurity must be trained to acquire the skills necessary (even experienced cybersecurity professionals need training)[17]. The research cybersecurity fundamentals and principles described earlier are the best places to start this training, followed by topics discussed in this paper, both in general and in the local, campus-specific context.

[17] IU offers research cybersecurity training. assessments, consulting, and assistance.

4. Survey the landscape

A successful research cybersecurity program requires an understanding of the local research landscape and campus stakeholders. It requires learning who the players are, what they do, how they work, what they need, what the risks to research are, and developing a strategy to mitigate those risks. The following enumerates the steps necessary to accomplish this.

Identify stakeholders and understand roles

Research takes a village, not just researchers. A variety of players are responsible for making the research mission a success. The following provides a comprehensive list of the stakeholders that should be in scope and their role.

- *Research faculty*: The primary researchers on campus. They range from well-established faculty to those who are beginning their career and striving to get tenure.
- *Graduate students*: The worker bees of research. Employed by faculty and paid through research grants and contracts, they not only get their hands dirty with equipment or fieldwork but often manage systems and technology also within research groups.
- *Office of the vice president for research* Responsible for all aspects of research on campus (except actually conducting it).
- *Sponsored research office*[18]: Typically, a part of the Office of the Vice President for Research, it manages all grants, contracts, data use agreements, cooperative agreements, and other vehicles through which research funding arrives on campus.
- *The institutional review board (IRB)*: Oversees and approves all human research on campus. IRBs comprise experts in relevant research fields and staff that oversees the IRB process itself. Different campuses have different offices managing the IRBs, but most are typically part of an office of vice president for research.
- *Departmental IT*: Located in the departments, they support researchers directly. Some departments also provide IT services that may be used by other departments. Some researchers prefer to run their own technology resources to maintain control.
- *Large campus support centers*: Provide support to individual departments or those that have banded together to establish them. For example, IU has a large Social Sciences Research Commons that provides dedicated support to social science researchers in a large number of departments.
- *Research computing*: Provides technology resources that are dedicated to research. This may include high performance computing, storage, visualization, and support. They may also offer solutions for regulated data and other, specialized research needs. They are either part of central IT or a standalone unit.

[18] Sometimes known as the Office of Research, Office of Research Administration, or Office of Sponsored Programs.

- *Central IT*: Provides technology to support the university's mission at large. Researchers typically use many central IT services such as email and file storage.
- *Central helpdesk*: Handles IT questions from campus constituents at large. Typically part of central IT.
- *Information security office (ISO)*: Responsible for protecting the entire campus, it provides institutional security governance. It also runs cybersecurity technologies and procedures such as intrusion detection/prevention systems, incident response, and forensics.
- *Information policy office*: Creates and maintains IT and security policies. Some campuses do not have a separate policy office but integrate policy management into the security office.
- *Information privacy office*: Responsible for protecting user privacy in both analog and digital forms. They may also oversee compliance regimes such as GDPR and HIPAA privacy.
- *Export control office*: Handles research subject to export control regulations.
- *Research compliance office*: Responsible for overseeing ethical conduct of research, conflicts of interest, and research integrity. They also handle cybersecurity regulations on some campuses.
- *HIPAA privacy and security office*: Responsible for the implementation and enforcement of the HIPAA regulation in institutions that are HIPAA covered entities, typically those with a medical school.
- *Research coordinators*: Provide help to the researchers with IRB proposal preparation, etc., especially in medical schools.
- *Research facilitators:* Subject matter experts on some campuses who help researchers with regulated research and other needs and natural candidates to recruit into the program. They may be part of research computing, ISO, Office of the VP for Research, etc.
- *Data stewards*: Responsible for institutional data management. There may be a single data steward or multiple data stewards for different types of data, for instance health, research, finance, and student data. They may also approve the operation of systems subject to regulations.
- *General counsel*: Provides legal counsel to the campus at large. Resolves complex clauses and issues in research contracts or data use agreements, etc.
- *Internal audit*: Performs audits of university departments and areas, including research.
- *Technology transfer office*: Helps researchers bring their products to the market.
- *Libraries*: Assist researchers in various ways, including data management plans on some campuses.
- *Human resources*: Responsible for facilitating faculty and staff hiring, including background checks.
- *Facilities*: Manages campus buildings and other physical facilities. Installs and operates physical security systems for buildings and labs, including the Data Center(s).
- *Campus police:* Responsible for the physical security of buildings and personnel.
- *Graduate office*[19]: Assists graduate students.

[19] Also known as the Graduate Studies Office, Graduate School, etc.

- *Purchasing*: Responsible for acquisition of system, software, and services.
- *Office of diversity* Promotes diversity by promoting minorities and the underrepresented, including researchers. Some campuses also have a Women in Technology group.

While we have attempted to make the list above as exhaustive as possible, there may be others who are left out, for example a unit providing help to researchers with surveys or cores within medical schools that provide services such as medical imaging, biostatistics, tissue banking, etc. They and any other such stakeholders should also be included to achieve a thorough census of stakeholders.

Gather information and establish relationships

A research cybersecurity program must leverage *all* stakeholders that engage in or support research. In the process, it must develop a strong awareness of who and where the researchers are and the types of research they do. This information can be obtained by visiting department websites, research newsletters, press releases from the VP for research and others, and talking with sponsored research or Dean's offices.

For stakeholders that support research, the best approach is to begin by identifying existing and desired relationships. Most important are points of origin – offices, roles, and units through which most if not all researchers pass, in particular sponsored research, IT, IRB, and HR. They can not only provide information, but they are also the primary vehicles to gain access to researchers. Simply having existing relationships may not be enough; it needs to be refreshed in the research cybersecurity context.

The sponsored research office (SRO) is the most important point of origin and ally. It can provide information on researchers; who the primary research sponsors are (such as NSF, NIH, DOD, etc.) for the campus, common cybersecurity and compliance requirements in grants, contracts, and data use agreements (such as HIPAA, FISMA, DFARS, Export Controls, etc.); and challenges they pose to researchers and those who support them (including the SRO). It also maintains information on what/where research is taking place on campus (sometimes in a convenient database or dashboard) that can offer detailed data on sponsored research, including individual grants and contracts. This information will be extremely useful for a number of purposes later, including the targeting of specific researchers and research areas.

The office of the VP for research (OVPR) is the central hub for all research on campus. Getting to know the right people there and recruiting them as allies is more or less mandatory, both for informational purposes and to reach researchers. Support from the VP for research may be essential to even begin the research cybersecurity journey. Cooperation with the OVPR is greatly facilitated by casting the program in terms of the research cybersecurity principles, stressing the program as a research *enabler* that makes the OVPR's job easier.

Departmental IT/central helpdesk/support centers are highly desirable points of origin. They can provide information on researchers who use their services, what they use/need, common support issues, unmet needs, and areas of concern. Central IT and research computing can supply information on available technology and support solutions (including those for regulated data), how researchers use them, unmet needs, etc. They are also the best source of information on research IT data flows and workflows.

For research involving sensitive and regulated data, the IRB office can provide information about human subjects research on campus, including any cybersecurity issues they or the researchers face. It is also the place to learn about who and where the research coordinators are. Data Stewards/ISO/compliance offices/export control office can also be tapped for information on types of regulated data on campus, data classifications, where researchers go for help with cybersecurity/compliance, etc.

The *ultimate* point of origin is university HR. It allows the program to catch researchers early during the HR intake process itself through new faculty orientation and/or orientation materials. Departments sometimes also hold welcome gatherings for new faculty. A presence there can also pave the way to future customers.

While research cybersecurity is a part of the institutional cybersecurity program, it needs a more nuanced approach to risk mitigation in order to ameliorate the friction between institutional cybersecurity and researchers. This requires a *very* strong relationship, understanding, and synergy between the research cybersecurity program and the ISO. The reason, among others, is to avoid the program projecting an image that is misinterpreted by researchers as "the security office coming after my research, again."

Finally, care is necessary when establishing relationships with stakeholders that support research (we will cover researchers later). It requires doing homework first, meetings in person, going out to lunch, whatever it takes to build rapport. It also helps to know their pain points in advance, if possible, by gleaning it from other stakeholders, for instance. The purpose of the interactions is not only to seek information, but also to learn how the program can help the stakeholder (and vice versa), empower the researchers, and where it is likely to run into challenges. Relationships with stakeholders that support research are essential to building the consensus and cooperation critical to success.

A clever approach to bringing stakeholders together and greatly easing the path forward is to establish a committee to oversee the research cybersecurity program and to put all relevant stakeholders on it. This prevents any who were left out complaining later. (We used this mechanism to successfully get our HIPAA compliance project approved.) The downside is that it can also make

meetings and coordination challenging. Relationship building can be pursued piecemeal also, connecting with each stakeholder individually.

Inventory institutional policies and procedures

In scope are all institutional policies, procedures, and workflows that affect research or researchers in *any* way. This includes at the very least IT policies and procedures (including cyber insurance), data management policies and procedures, institutional data classification, sponsored research policies and procedures, human subjects research policies and procedures, privacy policies and procedures, regulatory policies and procedures (such as Export Control, HIPAA, etc.), software/services acquisition policies and procedures, research computing policies and procedures, and HR policies and procedures.

Understand research use cases and workflows

A research use case is a unit of technology-based action by a researcher to get research done, for instance sharing data with internal and external collaborators. A research workflow is a series of steps that they must take to address a use case. For the data sharing use case above, the workflow for a new researcher joining the campus might be to search a knowledge base (KB) or talk to Departmental IT to learn if there is an appropriate data-sharing service on campus, request an account, access the service through a browser or install a client, create a folder, upload or download files, add or delete permissions, and perform file operations. Many research use cases are common to all research (for instance long term data archival) or not research-specific at all (such as the data sharing example earlier). Others are highly specialized for research (for instance supercomputing, massive data storage, longitudinal surveys, etc.). Many use cases and workflows are fairly obvious, such as data sharing. Others will emerge from the information collected from stakeholders. Still others will appear after a program has been instituted and begins interacting with researchers routinely. The *SecureMyResearch Cookbook*[20] is a good source of common use cases and workflows. The recipe list[21] enumerates use cases while the recipe steps constitute secure workflows to address those use cases.

Inventory existing solutions

Implementing research cybersecurity requires a deep knowledge of existing institutional solutions. This is for two purposes: the knowledge can be used to (a) assess risk to research (as we will see below), and (b) help inject cybersecurity into research workflows.

The inventory should begin with the most important solutions, namely general IT and research computing systems and services Examples are email, file storage, database service, supercomputers,

[20] https://go.iu.edu/coobook
[21] https://uisapp2.iu.edu/confluence-prd/display/SMR/Recipes

high performance file systems, archival storage, data repositories, compliant systems and solutions, cloud services and solutions, and cybersecurity services such as vulnerability scanning and antivirus software. Learning about existing systems and services requires reviewing appropriate websites/KB and/or consultation with central IT/research computing. Departmental IT is also important since not all solutions will be central.

Specialized professional services not provided by IT but used by many researchers are another component, for example transcription, media destruction, language translation, OCR scanning, etc. Information about such services can be obtained from purchasing department or departmental IT.

Determine researcher needs

Most risk to research comes from *institutional lack of awareness* of researcher needs. When the campus fails to offer secure solutions that address research use cases and match the pace of research, it forces researchers working under a time crunch to naturally seek quicker but potentially risky methods to get work done. Determining needs is thus critical to research cybersecurity.

While the diversity of research and uniqueness of each project presents a confounding array of variables to challenge needs assessment, one can begin with the most common research use cases and workflows. The data sharing use case earlier can be used to illustrate the needs assessment process.

- Determine if the institution is providing a service that enables data sharing. If not, this is an unmet need.
- If it does, determine if the researchers can share data with external collaborators. If not, this is an unmet need.
- If they can, determine if sharing is possible instantly, without delay (remember, speed is of the essence). If not (for instance if it requires days to request institutional accounts for collaborators), it still counts as an unmet need.

These steps should be repeated for all use cases identified earlier. Individual steps of existing workflow may also reveal a need. In the data sharing case for instance, installing a client to access the service may not be clearly articulated, forcing the researcher to search for a solution instead of doing research. Another useful byproduct of identifying and documenting research use cases and workflows is the ability to anticipate future needs and proactively search/plan for secure solutions to meet those needs.

The steps above will help reveal the most common researcher needs. A comprehensive inventory of needs requires direct interaction with researchers. This becomes easier when researchers begin engaging with the program, but preemptive actions can be taken to start the process early. For example, existing relationships with researchers (or others) can be used to discover the most urgent

needs. Cold calls also work. We employed the "Can we come see your lab?" strategy to get the needed information from researchers without directly needing to ask about needs. We had them describe their research workflows during the lab visit and used the answers to gauge where cybersecurity could be baked in. We also asked them about potential or desired projects, allowing us to anticipate future needs.

Assess and mitigate risk to research[22]

Baking cybersecurity into research requires assessing where to inject it first. There are two primary sources of risk to research, namely unmet needs, and insecure workflows. The former usually dominates since institutional lack of awareness of needs is common, but the researchers' inability to prioritize cybersecurity is also a source of risk. Current strategies for cybersecurity risk assessment are not effective here since they are limited to infrastructure components such as systems, networks, and software. Research cybersecurity requires an entirely different approach.

To assess risk from unmet needs, it is necessary to determine if the institution is meeting the identified needs. Taking the data sharing example, if there is no solution to share data with external collaborators or if the solution is cumbersome or slow, the risk is that the researcher will use external means such as the public cloud or email for sharing. Depending on the data in question, the risk level may be high (for sensitive data) or low (for public data). The appropriate risk response in this case is to establish a secure institutional solution or a secure workflow that uses alternate, secure solutions to meet the need.

Another area where the institutional lack of awareness of unmet needs can lead to risk are gaps in institutional processes that do not account for edge cases. For example, consider a case where a graduate student would like to use cloud resources for their research project. If the institution requires that new cloud accounts be requested and created through a specific team, but the request form requires a departmental billing code, a graduate student that doesn't easily have access to a billing code and also doesn't understand the risks may simply opt to create a cloud computing account with the vendor directly and pay out of pocket. Understanding institutional research processes and identifying where researchers may get lost or slip through the cracks is critical both for accelerating research and reducing risk.

Assessing risk from existing workflows requires each step the researcher might employ to address common use cases to be investigated. A good example is researchers using their Microsoft Exchange calendar for appointments with study participants, then sharing their calendars with a colleague later. This leads to a risk of potentially exposing participant information.

Risk can also be introduced inadvertently due to the researchers misinterpreting controls. A case in point is full disk encryption. We have seen instances where the researcher uploaded sensitive data to

[22] Note that we do not say "risk to the institution". From our perspective, risk to the institution is the same as risk to research.

a public area under the impression that it remains encrypted upon arrival. They overextended what they were told, namely that their "workstation is encrypted." This could have been mitigated by a secure workflow that included a pre-encryption step/tool for sensitive data prior to transfer. Collecting and documenting insecure workflows takes time but prolonged, direct interactions with researchers and information collected from stakeholders that support research ultimately provides the needed information.

5. Develop solutions

The results of the risk assessment inform the types, design, location, and implementation of solutions. For instance, a lack of secure systems may be addressed by retrofitting existing systems with controls or developing secure systems from scratch. To satisfy specific compliance regimes/security requirements, those systems may be hardened by adding the requisite controls. For each risk identified, solutions are facilitated by surveying the landscape to determine if it can be mitigated by an existing solution or a combination. If not, a new solution(s) may be needed. Developing these solutions may require bringing together stakeholders such as the OVPR, research computing, central IT, the ISO, compliance offices, and departmental IT.

Once solutions have been identified or implemented, secure workflows can be designed for specific use cases by picking the right combination and securely stringing them together (such as those in the cookbook).

6. Establish a research cybersecurity service

Research cybersecurity is most successful when it reduces or eliminates the security and compliance burden on the researcher. This takes a central research cybersecurity service, preferably providing consulting, self-service, and advocacy. Since the sole purpose of the service is to accelerate research, *speed* is its single most important characteristic. Every aspect of the service must be designed to minimize delay by dispensing with unnecessary bureaucracy, inefficiency, and redirection. It should be a one-stop shop for researchers. The following elucidates how a research cybersecurity service should be developed and implemented.

Areas covered

A good research cybersecurity service needs to address cybersecurity and compliance needs comprehensively. While the areas it covers will depend on local resources, structure, needs, and risks, it should strive ideally to resolve *any* cybersecurity issue that a researcher might face. The following enumerates the services researchers can expect from *SecureMyResearch*[23] as an example.

- Security requirements gathering.

[23] The service is also open to campus stakeholders that support research, but we do not list what we help them with as service offerings.

- Custom workflows to secure research projects.
- Identification of secure/compliant on-premises and vended technology solutions.
- Institutional interpretation of cybersecurity terms and conditions in grants, contracts, and data use agreements into solutions/actions for researchers.
- Designing custom solutions to meet rules and regulations.
- Proposal review prior to submission to ensure compliance with terms and conditions.
- Security assessment of current and planned projects.
- Security boilerplates and custom letters for institutional systems and other cybersecurity elements in grants, contracts, and DUAs.
- Documentation of compliance.
- A self-service cookbook.
- Advocacy for solutions and research-friendly policies and procedures.

These offerings require reviewing the research project, existing IT infrastructure if any, and relevant regulations, investigating solutions, interactions with vendors, consultation with various stakeholders, developing recipes, advocating for solutions, research into new technologies, solutions, and regulations, and third party assessment.

Preliminaries

An important aspect of the service is that it is instituted as a consultancy to which researchers come *voluntarily,* or are referred to by stakeholders that support research. The service should avoid giving the appearance of institutional cybersecurity governance. Even the slightest perception that the service is a directive is sufficient sometimes to push researchers away. IU offers *SecureMyResearch* out of the Center for Applied Cybersecurity Research (CACR)[24] which reports to the CIO but is not part of institutional cybersecurity. Having the word "research" in the name of the organization delivering the service has also been helpful. Having a researcher (even an ex-researcher) to be the face of the service is also advantageous.

Other recommendations include the following.

- Choosing a simple, easy-to-remember name for the service[25] that can be firmly lodged into the researchers' consciousness is *critical.* This name is all they should need to remember to access the service.
- Having a "servicename@yourdomain" email address and "servicename.yourdomain" website as the only user-facing online service identity. The use of a contact form that researchers are required to fill out to get support should be avoided as it introduces an additional time burden to consuming the service. Researchers should be able to initiate

[24] https://cacr.iu.edu
[25] such as *SecureMyResearch*

contact and service providers take the lead quickly and easily from there, determining needs and setting up consultations.
- Funneling the servicename@yourdomain into the institutional ticketing system.

Service components: consulting

Securing research is not a cybersecurity problem alone; it requires relationships and trust. One-on-one consulting is the critical design element of the service where this trust is built. Research cybersecurity consulting takes a highly sensitive, researcher-centric approach. The following enumerates the nuances.

- Instant response to tickets (personally, not via an auto-responder) creates a *highly* positive impression on researchers. This single act alone is sufficient for researchers to become repeat customers in many cases.
- Every ticket is an opportunity to begin a long-term relationship, not simply a request to resolve an issue.
- Instead of sending emails, it is better to offer an online meeting the same day or the next to facilitate a solution or to solicit more information. This is most critical during the first interaction and improves service perception by creating an opportunity to establish a human connection. Face-to-face or video meetings should be preferred since the ability to see the other person's face plays a key role in relationships. A meeting also eliminates inefficiencies of emailing back and forth, greatly accelerating problem resolution.
- It is important to learn as much as possible about the researcher prior to and during interactions. This includes information such as who they are, where they are on campus, the research project that generated the ticket, use case and workflows, whether they work with sensitive or regulated data, if they use Departmental IT, future work that might involve cybersecurity or compliance, etc. Acquiring as much data during the first meeting as time allows also helps speed up the ticket and allows for better next interaction.
- Information collected should be used to create a researcher profile database and consulted prior to/during the meeting or interaction. Referring to something specific about the previous interaction ("did you manage to do X"?) during a re-engagement is highly conducive to a long-term relationship. A follow up some time later after closing a ticket is also an excellent strategy.
- It is best to strive to resolve the ticket during the first meeting itself. Many tickets (nearly 80% for us) are amenable to this treatment. It makes the researchers appreciate the service and use it as an ongoing tool to accelerate their research.
- The support workflow should be as follows: understand the context/use case/issue, assess risk, identify solutions, combine them into a secure workflow to address the risk, document the steps, and provide them to the researcher to follow. Problems should be approached holistically, and entire workflows secured, including people, endpoints, data transfers/analysis/storage/disposal, etc.

- It may be tempting to redirect the researcher to another unit at times. It is best instead to get them what they need *as part of* the engagement. Researchers are often frustrated with a disjointed support experience, especially when it wastes precious time because "the left hand doesn't know what the right hand is doing." The service should strive to be a one-stop-shop; redirection should be used only when absolutely unavoidable.
- Leveraging appreciative customers to help spread the word to peers is the most effective strategy to socialize the service. Word of mouth will always be the primary mechanism that grows the service, not outreach campaigns.
- If a customer is especially appreciative because the service, for instance, has accelerated their research and made funding arrive on campus faster, it should be used as an opportunity to ask for a short testimonial. They will be very effective to include in annual reports and during requests for renewed funding.

Service components: self-service

Meeting the pace of research requires the ability to deliver instant service. Consulting is not always the best vehicle for this. For common use cases/needs, it is much faster to send the researchers to a self-service resource such as online documentation.

We designed our self-service gateway, the *SecureMyResearch Cookbook*, to provide researchers with instant solutions to common needs. It also reduced our consultancy workload and allowed us to hide cybersecurity in plain view by baking it into *recipes* that help researchers get work done. An important and clever feature of the cookbook is the search only returning *verbs* (such as "Share data with internal and external collaborators"). The verbs (recipe titles) match precisely what the researchers need *at that moment*. Clicking the result provides them with steps, satisfying their "just tell us what to do" desire. Some steps may be explicit cybersecurity actions but are not viewed as such by researchers due to being part of a recipe that is tied to getting something done. The cookbook is a mechanism for translating researcher needs into institutional workflows that bake in cybersecurity and compliance.

Service components: advocacy

Researchers are often frustrated by policies, procedures, and institutional inefficiencies that slow research down. This may include, for instance, an IRB form that is confusing, a months-long third party assessment[26] of a service, or the lack of a servicethat allows them to share data with external researchers. The final component of research cybersecurity is thus advocacy, a mechanism to address this aspect. The service should act as an ombudsman for the researchers by bringing their message back to the institution and pushing for changes and solutions.

[26] Researchers especially dislike third party assessments since they take months to complete. *SecureMyResearch* is piloting a rapid assessment alternative just for research where we work with researchers for quick risk analysis and inject security as needed. This has accelerated resolution in some cases from months to *minutes!*

7. Establish institutional workflows

As mentioned earlier, research cybersecurity must leverage all stakeholders to accelerate research. This is best accomplished by integrating the service into institutional workflows to minimize delay. Which workflows are appropriate will depend on the institution, but we can use *SecureMyResearch* as an example. Researchers are directed to the service via the following stakeholders/workflows.

- *Sponsored research*: when it notices cybersecurity terms and conditions in grants, contracts, and data use agreements that require interpretation, solutions, or compliance.
- *IRB*: when it receives a proposal where researchers are using an external system to store sensitive data that has never been through the institutional third-party assessment (3PA) process. The 3PA process often takes a long time, greatly slowing them down. We work with the researchers to review the proposal, understand the context, engage with the vendor if necessary, and perform a rapid risk assessment. This accelerates the IRB processes from months to hours (even minutes) in many cases. An important aspect of the workflow is that the assessment requests come indirectly, via the data stewards, to keep us out of institutional cybersecurity governance. We are offered as consultants that can help accelerate approval.
- *Information security office:* when it discovers security issues having to do with research or when Departmental IT needs help with security for research projects.
- *Data stewards*: when they receive requests for approval of research software (in the cloud, for instance) or research systems with sensitive data.
- *HIPAA privacy and security office*: when it encounters a researcher needing help with implementing the Security Rule.
- *Research computing*: when it has researchers with workflows on its systems that need to be secured or assessed for compliance.
- *Central helpdesk, Departmental IT, campus support centers, research coordinators/research facilitators*: when a researcher comes to them looking for help with cybersecurity and compliance.
- *Human Resources*: when new faculty arrive on campus. The service is featured during orientation.
- *Large campus support centers.* when they are consulting on research projects that have specific security requirements or when they have identified a common need on behalf of researchers that is not currently addressed by the institution.

8. Launch the service

While the research cybersecurity program ultimately spreads by word of mouth, initial outreach is also important to seed the process. A carefully planned, formal campaign is essential for a favorable service launch. To ensure best results, it is useful to have the stakeholders that support research review the service first, followed by a pilot for a small group of researchers. Their feedback should be used to improve the service prior to launch.

Careful attention to messaging is also critical during launch to make a good first impression. The campaign should always use positive language and messages should be worded solely in terms of accelerating research, increasing funding prospects, and giving researchers a sense of security about their research.

The campaign needs to leverage every outlet/means conceivable to spread the message. This includes email, campus newspaper, radio, social media, tables at campus events, swag, websites, etc. Another outreach strategy is to get invited to presentations at faculty meetings, new faculty orientation, and graduate student groups. Communication mechanisms used by stakeholders such as sponsored research, human resources, library, IRB, research coordinators, and others should also be leveraged for outreach. Finally, it never hurts to proselytize one on one whenever possible. Also, the service should be featured on all important institutional websites, for instance central IT, VP for research, IRB, ISO, etc.

9. Maintain and refine the program

A research cybersecurity program requires constant care and improvement in order to survive and grow. For ongoing maintenance, it is necessary to carefully preserve the service's consultancy image and a sensitivity to perception. This is facilitated by avoiding entanglements with cybersecurity governance workflows that are *externally* visible to researchers, for instance incident response. Maintaining the program also means nurturing existing relationships and building new ones. This requires necessary due diligence to stay informed about new faculty, new IT professionals, new terms in grants and contracts, and new institutional workflows. An active effort to get the service plugged into individual research projects and institutional workflows helps weave it irreversibly into the institutional fabric. Maintenance also requires visibility to researchers on an ongoing basis, requiring repeat socialization campaigns to remind existing researchers and inform new researchers. Program visibility to leadership is necessary by collecting testimonials and metrics to argue for continued funding. Success stories in the popular media on campus, especially with researchers featured prominently, are also an excellent strategy to raise the program's profile.

To refine the program, researcher feedback is needed during regular support workflow and via formal/informal surveys. Feedback from stakeholders that support research is also very important for improvements. When combined with metrics and testimonials, this feedback provides data that helps assess the health of the program. The results of the assessment provide insight into the corrections to be applied. Ideas for improvement may also come from other avenues, sometimes unexpected, as the program evolves.

Compliance

Compliance in research is not a new arrival. Campuses have been tackling HIPAA within medical schools since its inception nearly two decades ago. Due to attacks and breaches, a

number of rules and regulations since (especially recently) have forced many more, stricter cybersecurity terms and conditions into grants, contracts, and data use agreements. This has made compliance a major challenge for campuses, especially those with no prior exposure to regulated data. As mentioned earlier, our research cybersecurity journey began with HIPAA in 2007. Compliance has been a part of it ever since. The following describes how we handle compliance in research at present.

Due to limited resources and newly emerging compliance regimes, we were forced to move from the original, HIPAA-specific methodology to a more general approach to compliance. Nearly a decade ago, we decided to adopt a mature cybersecurity standard to allow us to "do cybersecurity once and compliance often." We aligned our research cyberinfrastructure with the NIST Risk Management Framework (RMF) by applying tailored controls from the NIST SP 800-53 control catalog. Since the controls prescribed by most rules and regulations map to the RMF/800-53, this gives us a unified approach to all compliance. We leverage systems aligned with the RMF to bake compliance into regulated data workflows (as can be seen in the cookbook recipes). Researchers come to or are directed to *SecureMyResearch* via established institutional workflows. We then simply *supply* compliance by mapping research use cases to pre-secured, compliant systems and workflows.

SecureMyResearch metrics

While our approach to research cybersecurity had enjoyed success at a modest scale in the School of Medicine, we had no expectations that *SecureMyResearch* would scale to the entire campus or be successful. It appeared to be popular as adoption increased, but this perception was purely subjective. Proving success requires hard numbers. This motivated the development of a number of research cybersecurity specific metrics, namely number of tickets, resolution time, numbers and breakdown of customers by school/department/status (faculty, staff, or graduate student), amount of sponsored funding facilitated, research acceleration (especially when it is months to minutes), diversity of issues, regulated/unregulated research, cookbook use, and repeat customers. The following provides a subset of facts and figures for *SecureMyResearch*'s inaugural year (FY 2021).

- Over 200 researcher engagements.
- Facilitated over $230 million in sponsored research.
- Achieved rapid service adoption within a single year.
- Reached roughly 25% of all IU faculty in 70% of all academic departments and centers.
- Invited to give presentations at faculty and other meetings.
- Handled service tickets covering a wide variety of research use cases.

- Established long-term relationships with stakeholders[27] that support research.
    - Became a critical resource for the IU Office of Research Administration in resolving cybersecurity terms in grants, contracts, and data use agreements.
    - Helped researchers negotiate/interpret highly challenging contract terms and conditions.
    - Invited to be a key component of research software risk assessment for IRB submissions.
    - Became integrated into support workflows for social sciences departments by being invited by a large social sciences research center.
    - Became integrated into clinical research services workflows in several departments.
- Expanded coverage beyond traditional, compliance-driven clinical- and defense-related research to areas such as physics, computer science, earth and atmospheric sciences, social sciences.
- Significantly accelerated research, in many cases from months to minutes, by resolving cybersecurity and compliance issues.
- Cookbook recipes viewed 7000 times, obviating the need for tickets.

While still a surprise, this shows that our approach to research cybersecurity is indeed delivering results, adding value, reducing risk, and accelerating research.

Conclusions

Due to the prevailing misalignment between cybersecurity and research, many institutions of higher learning have been forced to leave research to its own devices. Two decades of invaluable lessons from clinical researchers and metrics from *SecureMyResearch* at IU show that this is no longer necessary. Cybersecurity *can* be applied successfully to research when it focuses on the research mission and is supplied to researchers, allowing them to do what they do best, namely research. It is most effective when hidden within institutional solutions and workflows that allow researchers to get work done.

Implementing research cybersecurity also requires highly nuanced processes and principles and can reverse the perception of cybersecurity as an obstacle to research. Establishing a research cybersecurity program is not trivial, but it is a worthy effort, with substantial rewards that include research acceleration, more competitive researchers, and an expansion of the institution's research funding footprint.

Research cybersecurity uses a mindset and approach that deviates from traditional cybersecurity practice. It requires a new breed of cybersecurity professionals who must have

[27] Data Stewards, University Information Policy Office, Office of Research Administration, Office of Research Compliance, Chief Privacy Officer, University HIPAA Privacy and Security Officers, IU Office of Vice President and General Counsel, Internal Audit, Human Resources, Purchasing, the Library, College of Arts & Sciences IT, Departmental IT professionals, Research Coordinators.

the necessary qualifications and training. The increasing interplay between cybersecurity, compliance, and research ensures that proper research cybersecurity is imminent. There is no better time to start than now.

Acknowledgements

We would like to thank a few key individuals that have had a significant impact on the development and success of our research cybersecurity effort over the years. This includes Craig Stewart, Bill Barnett, Von Welch, Fred Cate, and Brad Wheeler. We are particularly grateful to IU Offices of the Vice Presidents for IT and Research at Indiana University who provided the funding for *SecureMyResearch*. Without their vision and support, there would never have been an institutional research cybersecurity program at IU. Finally, we acknowledge the contributions of a number of colleagues who reviewed early drafts of the paper and provided valuable feedback. This includes Von Welch, Sean Peisert, Cyd Burrows-Schilling, Carolyn Ellis, Tim Daniel, and Mason Green. We thank them for their time and generosity.