Research at Risk:
Ransomware Attack on Physics and Astronomy Case Study

Aug 1, 2021

Distribution: Public

Authors: Andrew Adams[1], Tom Siu, Julie Songer, Von Welch

[1] Engagement Lead, Andrew Adams

About Trusted CI

As the National Science Foundation Cybersecurity Center of Excellence, Trusted CI draws on expertise from multiple internationally recognized institutions, including Indiana University, the University of Illinois, the University of Wisconsin-Madison, and the Pittsburgh Supercomputing Center. Trusted CI collaborates with NSF-funded research organizations to focus on addressing the unique cybersecurity challenges faced by such entities. In addition to our leadership team, a world-class Advisory Committee adds its experience and a critical eye to the center's strategic decision-making.

Acknowledgments

Trusted CI's engagements are inherently collaborative; the authors would like to thank the following Michigan State University participants: Melissa Woo, executive vice president for Administration and Chief Information Officer, and Phillip Duxbury, dean of the College of Natural Science, for the collaborative effort that made this document possible.

This document is a product of Trusted CI. Trusted CI is supported by the National Science Foundation under Grant #1920430. For more information about Trusted CI, please visit: http://trustedci.org/. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

Using and Citing this Work

Cite this work using the following information:

A. Adams, T. Siu, J. Songer, and V. Welch, "Research at Risk: Ransomware attack on Physics and Astronomy Case Study," NSF Cybersecurity Center of Excellence, Trusted CI, trustedci.org, June 2021. Available: http://hdl.handle.net/2022/26638

Table of Contents

Background **3**

1 Introduction **3**

2 The Ransomware Attack on Physics and Astronomy **4**

3 Attack Timeline and Repercussions **5**

3.1 The Attack and Response 5

3.2 Research and Other Impacts to MSU 6

4 MSU/Trusted CI Interview Process **7**

5 Lessons Learned **8**

5.1 “We’re Better than You” Culture 9

5.2 “Going it Alone” with Inadequate Resources 9

5.3 “Productivity Trumping Security” Paradigm 10

5.4 Staff Security Training and Reporting Structure 10

6 Mitigation Strategies **11**

6.1 Building a Relationship with Centralized IT 12

Cybersecurity budget 13

6.2 Developing a Cybersecurity Program 13

6.3 Removing the Cybersecurity-hindering Culture 14

6.4 Basic Cybersecurity Hygiene 14

7 Conclusion **16**

Background

Ransomware is a form of cybercrime that has risen to the same level of concern as terrorism by the U.S. Department of Justice[2]. The United States suffered more than 65,000 ransomware attacks last year[3] and victims paid $350 million in ransom[4], with an unknown amount of collateral costs due to lost productivity. Historically, research organizations have been largely ignored by cybercriminals since they do not typically have data that is easily sold or otherwise monetized. Unfortunately, since ransomware works by extorting payments from victims to get their own data back, research organizations are no longer immune to being targeted by criminals. In this paper, we examine a ransomware attack on one research organization, the Physics and Astronomy department at Michigan State University, the impact on that research organization—measured in lost years of research—and lessons learned that other research organizations can apply to protect themselves. In the experience of Trusted CI, there was nothing extraordinary about the issues that led to this incident, and hence, we share these lessons with the goal of motivating other organizations to prevent future negative impacts to their research mission.

1 Introduction

By and large, cybercriminals have not targeted research organizations because they are not usually rich sources of data that attackers can easily monetize (credit card numbers, Social Security numbers, etc.). However, a new form of attack, ransomware, has risen over the past decade that changes the traditional model of cybercrime. In a ransomware attack, criminals encrypt a victim's data in order to deny the victim access to their own data, usually causing the victim to lose the ability to continue functioning. For example, in May of 2021 Colonial Pipeline in the eastern part of the United States suffered a ransomware attack resulting in being offline for a week[5], paying $4.4 million in ransom, and ultimately requiring months and many more millions of dollars to restore. More disturbing is the prolific increase in ransomware attacks. In a ZDNet report, Palo Alto Networks reports the average ransomware payout surged from

[2] https://www.cnbc.com/2021/06/03/us-to-give-ransomware-hacks-similar-priority-as-terrorism-official-says-.html

[3] https://www.npr.org/2021/06/09/1004684788/u-s-suffers-over-7-ransomware-attacks-an-hour-its-now-a-national-security-risk

[4] https://securityandtechnology.org/wp-content/uploads/2021/04/IST-Ransomware-Task-Force-Report.pdf

[5] https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636

$115,123 in 2019 to $312,493 in 2020, a 171 percent increase in one year[6]. In June of 2021, the U.S. Department of Justice gave ransomware similar prioritization as terrorism[7], and ZDNet estimated that ransomware damage could cost $20 billion in 2021 and $265 billion worldwide by 2031. These ransomware cost estimates are a warning to the research community that proper precautions must be taken to mitigate against these types of attacks.

A key factor regarding ransomware from the perspective of research organizations is that the data encrypted was not of value to the criminals, it was only of value to the victim. For example, Colonial Pipeline needed the encrypted data to run their business. This shift in paradigm puts nearly every organization at risk. Without planning ahead for cybersecurity exploits, universities and researchers stand to lose valuable resources, productivity, and research data. Additionally, universities and their researchers can suffer a blow to their reputations from cybersecurity attacks and face a public relations disaster. The purpose of this paper is to convey an example of a research organization that was hit by a ransomware attack, the impact it had in lost research productivity, and the lessons learned that other research organizations can apply to protect themselves.

2 The Ransomware Attack on Physics and Astronomy

A ransomware attack hit the Physics and Astronomy (PA) department at Michigan State University (MSU) in May 2020[8]. Several researchers were impacted in the aftermath of the attack, causing one to lose a year's worth of research and others to lose months of time and research. Additionally, PA systems were offline for most of the summer, and much of PA's data was not recovered.

The ransomware attack was also a big financial hit to MSU. University leadership decided not to pay the $6 million ransom demand, but the total remediation cost to the university was estimated to be $1,093,000. The costs included IT response and recovery time, PA staff and research time lost due to the shutdown, legal bills, notification of identity theft risk, and two years of credit monitoring and identity repair for personally identifiable information (PII) that was taken by the attackers.

---

[6] https://www.zdnet.com/article/the-cost-of-ransomware-around-the-globe-to-go-beyond-265-billion-in-the-next-decade/

[7] https://www.cnbc.com/2021/06/03/us-to-give-ransomware-hacks-similar-priority-as-terrorism-official-says-.html

[8] https://msutoday.msu.edu/news/2020/msu-provides-update-on-it-based-intrusion

While many organizations keep quiet about cyberattacks, MSU has decided to be transparent about its ransomware attack, hoping to encourage research communities to disclose similar incidents, and perhaps more importantly, to educate the open-science community about the threat of ransomware and other destructive types of cyberattacks. The overarching goal of this public report is to raise awareness about rising cybersecurity threats to higher education in hopes of driving safe cyberinfrastructure (CI) practices across university communities.

To achieve this, the CIO's office at MSU has engaged with Trusted CI, the NSF Cybersecurity Center of Excellence, with nearly a decade of success (https://www.trustedci.org/success-stories) in helping NSF-funded researchers mitigate cybersecurity risks. We encourage MSU's research peers to review our summary of the attack, its costs, and our process in evaluating the incident. Most importantly, we provide valuable lessons learned and mitigation strategies in hopes the research community will take action to prevent this type of attack from happening to them.

3 Attack Timeline and Repercussions

3.1 The Attack and Response

The PA department, part of the MSU College of Natural Science, was initially compromised on May 23, 2020. The ransomware attack was detected late on Memorial Day, May 25, and incident response (IR) began at 2am on May 26.

Taking advantage of a short-staffed holiday and a recently discovered Pulse Secure VPN vulnerability, the attackers intruded on the PA network via a test VPN server that was left running for two to three weeks without being patched. The threat actor, alleged to be part of the NetWalker criminal organization, was able to gain access to the internal network by leveraging the VPN vulnerability. Leveraging infrastructure vulnerabilities is a common way ransomware attacks are perpetrated, along with the stealing of passwords through phishing emails.

Once in, the hackers performed reconnaissance, eventually elevated their privileges, disabled security controls, and began distributing ransomware across the PA department's CI. Of critical importance, the attackers hit the PA active directory domain. Unfortunately, this domain not only contained research data, it held files containing personal identifiable information (PII),

some of it from the 90s. Finally, the attackers used pressure tactics to encourage payment by immediately publishing PII on the Internet. Despite the pressure to pay, MSU leadership made the decision not to pay the $6 million ransom.

An IR team was assembled to investigate the breach. The compromised development VPN was shut down immediately, along with nearly all of the PA CI. At the time of this report's publication, not all of PA's CI has been re-enabled. The pandemic created pros and cons for the IR team. Because of working remotely, IT staff were not on hand to physically pull network cables, however ubiquitous video conferencing helped IT staff work together immediately.

3.2 Research and Other Impacts to MSU

The disruption to the PA department lasted for most of the summer. PA systems were offline for more than a month until recovery efforts started on July 1. The network was quarantined—individual systems were opened to the network only after being vetted by MSU IT. The laboratory support systems were slowly brought back over a six-month period, and it took more than a year to bring the network-attached-storage (NAS) devices back online. Indeed, some servers are still not back online as of June 2021, and parts of the network are still locked down.

The aggregated time lost for staff and researchers was well more than a year—a single research project on its own lost a year's worth of data and had to start over from scratch. It's estimated that 50 to 70 percent of the research was halted due to the attack and some of the research could not start up again for six months. Access to labs was shut down, affecting the online teaching systems. In many cases, data was not recoverable, especially if a researcher had stored data on an individual system that wasn't backed up.

Additional costs were:

Financial cost — MSU estimates the total cost of the ransomware attack to be $1,093,000. This total includes hard costs from response and recovery, opportunity costs from staff time, legal costs, costs related to notification of identity theft—it was time consuming to determine the correct method for reporting the breach depending on the victim's nationality—and providing two years of credit monitoring and identity repair.

Data encryption and exfiltration — 700 GB of data were encrypted by the ransomware. Prior to encryption, however, the attackers exfiltrated approximately 8 GB of data in order to make good on their threat to expose sensitive data. This is a relatively new form of ransomware operator behavior. They work around the primary form of mitigation against ransomware, protected backups, by threatening to expose sensitive data.

In the MSU attack, the attackers exfiltrated data, including PII, affecting more than 9,000 students. NetWalker posted passports, driver licenses, and bank accounts as a pressure tactic. In total, 1.3 million files were exposed in the incident, and an estimated 127,000 files contained personal information. There's no evidence NetWalker knew they had research data. They either didn't care if they had research data or were simply unaware, but that didn't prevent them from having a serious impact on MSU's research productivity.

Summary — The key point here is that PA and MSU were negatively impacted, significantly, by one malicious actor that gained access through an unpatched VPN. Retrospectively, it is easy to say, "Well, if they just patched the VPN prior to the attack none of this would have happened," but that is only part of the truth. There were several, deeper issues that led to the attack's success. Some of these became apparent to both MSU IT and PA during the IR, and thus, they agreed to jointly document PA's insecure CI environment. The next three sections discuss how Trusted CI documented the issues and mitigations that other academia can pursue to avoid a similar pitfall.

4 MSU/Trusted CI Interview Process

To gather information for the report, Trusted CI conducted 10 interviews with key members of the PA department, the Dean of the College of Natural Science in which the PA department resides, and staff of the MSU Information Technology (IT) department, including members from the incident response, Research IT, Risk Analysis, System Administration, and Governance, Risk, and Compliance teams.

Sample questions that were asked of the interviewees are as follows:

1. Tell us about the incident and its ramifications?

2. Was research disrupted or was research data compromised, and if so, how long was it from discovery to restoration?
3. Do you have an estimate for how much PII, or data, or resources (money or time) were lost due to the incident?
4. How would you assess the cybersecurity training of the staff prior to the incident?
5. What key issues led to the incident?
6. In reflection, were you able to identify gaps in your cybertechnology tools or CI?
7. What were your lessons learned from the incident and what advice would you give your peers?

The distillation of the interviews is presented in the next section.

5 Lessons Learned

Clear patterns emerged from the interviews. Some were divergences between PA staff and MSU IT. For example, when responding to "how long was research disrupted?" the participants from MSU IT spoke in terms of months, i.e., laboratory servers were down for three months. The PA team, though, aggregated the actual research lost due to the unavailable CI and data, and responded to that question in years.

A second divergence surfaced in addressing the security skills of PA's IT staff. The participants from PA believed the security skills of the staff were acceptable. That is, the incident occurred not from a lack of security knowledge, but from conflicting priorities given to the staff. However, nearly all of the MSU IT interviewees thought the skills of the PA IT staff were deficient at the time of the attack. For one thing, the disaster recovery backup systems were not isolated and redundant. Instead, the PA backup drives were all connected to the same system, which was ultimately compromised.

The differences aside, there were three overarching cultural paradigms that emanated from the interviews, specifically: a "we're better than you" culture; a governing committee that condoned "productivity trumps security," and either insufficient security resources for an autonomous unit or the lack of dialogue with an external security resource. While these patterns didn't cause the intrusion, it's safe to say that these cultural influences created a vulnerable environment for the attackers to exploit.

5.1 "We're Better than You" Culture

One of the first departments to manage CI at MSU and over the past 20 to 30 years, PA developed an independent IT environment, its own internet access, VPNs, multiple active directories, and custom systems. Moreover, PA's IT staff predated MSU IT's security staff. Thus, PA had more experience, if not more knowledgeable staff, in managing CI than MSU IT for some of the past three decades. This history contributed to PA's insistence on controlling its own systems and equipment. Unfortunately, at some point in the past decade or two, PA's superior knowledge/experience was no longer an actuality—evidenced by aging infrastructure with unmaintained warranties in the PA IT environment—but by that time the culture was firmly rooted within PA.

The culture identified above left PA with a false sense of security. Prior to the attack, the PA interviewees believed they were more competent at system administration and cybersecurity than MSU IT. And since they were not up to date with the changing threat landscape, they didn't see the need to change their security posture in order to mitigate against, in particular, ransomware attacks.

5.2 "Going it Alone" with Inadequate Resources

The second pattern that emerged from the interviews most likely evolved from the first—PA staff believed they were better at IT and wanted to "go it alone." Operating apart is not necessarily a harbinger of malicious activity to come. A fully autonomous unit can have a strong security posture if sufficient resources and knowledgeable governance are allocated to cybersecurity. This, however, was not the case in PA.

IT operations within PA were governed by the Computer Operations Committee (COC), which was composed of PA faculty, who were part of the "we're better than you" culture previously identified. And it was the COC, in the vein of "going it alone," that shunned help from MSU IT—it was stated in the interviews that the COC actually pushed back on collaborating with and/or seeking aid from MSU IT.

Compounding these decisions by the COC was the fact that they either were unwilling to accept, or were simply unaware that the resources they had allocated for cybersecurity were inadequate. This void ensured that the COC's decision to "go it alone" was ultimately doomed.

There were attempts to create a dialogue between PA and MSU IT, and although the latter did succeed at setting up communication with other units at MSU in order to aid them, MSU IT's attempts to set up that key dialogue with PA failed, which in itself should have set off red flags and further attention. With that critical communication channel lacking, PA's CI could not benefit from the cybersecurity services that MSU IT offered, such as vulnerability scanning, intrusion detection, and patch management. Thus, MSU IT owns some responsibility here for they were aware of the services they offered and did not insist on better communication.

5.3 "Productivity Trumping Security" Paradigm

The third and final issue, perhaps also motivated through the culture found within the COC but certainly aided by the fact that there was no information security officer present and involved in the COC's decision process, can best be described as the old paradigm of "productivity trumping security." From the interviews, we learned that the PA IT staff was instructed by the COC to regularly prioritize faculty research over other maintenance tasks, including security.

A system where research productivity was trumping security maintenance was most evident in the lack of critical security patches for PA IT devices, specifically, the Pulse Secure VPN. Also, the NAS devices were used as the data-loss-prevention solution, as well as a perpetual cache for administration and research data, because it was always available and easy to access.

Granted, PA is certainly not the only unit or project in academia that suffers from this loose mode of operation that is far too easy to rely on. In relating this, our hope is others will accurately assess if they too have this trait. And if so, acknowledge and address it.

5.4 Staff Security Training and Reporting Structure

Although not a cultural issue per se, deficient security skills were a contributing factor in the incident. PA interviewees believed their IT staff at the time of the incident were capable in cybersecurity but lacked resources and direction in implementing and following security protocols. Their belief, however, akin to the poor direction from COC (see Section 4.3) may also have been influenced by the "we're better than you" culture (see Section 4.1) that was embedded in PA. In fact, poor security practices were in place, which included running an unpatched public-facing authentication service with access to all internal networks.

The PA IT lead had attended cybersecurity training a decade ago, so the material in that training was not relevant to the current threat landscape. The IT lead was (and is) knowledgeable with basic security hygiene, such as patching and monitoring infrastructure, but was not familiar with attack vectors and methods, like ransomware or keylogging. Thus, the lead was unaware of the level of risk inherent in following COC's "productivity trumping security" directions but did recognize that basic levels of security hygiene should occur and informed the COC of this. This request, however, oddly resulted in a junior administrator adopting responsibility for security. We note that this junior administrator did not receive any cybersecurity training.

6 Mitigation Strategies

As mentioned, there were three overarching cultural paradigms that emanated from the interviews, specifically: a "we're better than you" culture within PA; a "going it alone" attitude with inadequate cybersecurity resources; and a governing committee that condoned "productivity trumps security." While these patterns didn't cause the intrusion, these cultural influences created a vulnerable environment for the attackers to exploit.

Of these cultural paradigms, the "going it alone" mantra is the easiest of the cybersecurity issues to solve. It starts by opening up a dialogue with an institution's centralized IT and building a relationship between central IT and unit stakeholders. These communications should be regular with a focus on the security of critical assets.

To address "productivity trumping security," the solution is straightforward—develop and adopt a security program. This endeavor requires leadership support to ensure security policies are followed.

The "we're better than you" culture is more difficult to fix. In MSU's PA case, it took a humbling experience for the unit to acknowledge and eventually move past this culture.

Finally, we emphasize basic cybersecurity hygiene. If MSU's PA department had these practices in place, it would have reduced the impact of the ransomware attack. Among those actions:

- Delete sensitive data, and retain only what's needed
- Create segmented networks and backup systems

- Have an IR plan in place that includes a point of contact list and a chain of command
- Provide cybersecurity training for IT staff, and consult with cybersecurity experts that work with academia, such as Trusted CI (https://www.trustedci.org/).

6.1 Building a Relationship with Centralized IT

Of all the issues that plagued PA, inadequate cybersecurity resources is perhaps the most difficult to solve. However, the "going it alone" mantra is without question the easiest of the cybersecurity-hindering issues to address. It starts by opening up a dialogue with an institution's centralized IT. From that dialogue, the chief information security officer (CISO) can build a relationship that includes the unit stakeholders. These communications should be regular with a focus on the security of critical assets.

CISOs are advised to help units achieve their outcomes and aid them in seeing security as technology risk management. Put another way, CISOs can frame security in how it can help research and reduce risk, which in turn leads to better grants and reputations.

Most centralized IT departments have much to offer units, including:

- Vulnerability scanning
- Intrusion detection
- Centralized email systems with phishing and SPAM detection
- Data-loss-prevention (disaster recovery)
- Centralized account management with single sign-on and multi-factor authentication
- Password/secret managers
- Configuration management
- Patch management
- VPN access
- Log analysis
- Threat intelligence sharing
- Endpoint detection and remediation products
- Risk assessment and security planning services

And just as important, centralized IT has the staff to support the cybersecurity solutions listed above. At MSU, many of PA's internally run systems have now been off-boarded to MSU IT. The

fringe benefit—when units let go of local IT control, it allows them to fully focus on their mission of research and education.

Note, if a unit with adequate cybersecurity resources does choose to "go it alone," i.e., they want to maintain control over IT decisions, they (i) must have adequate cybersecurity resources in place, (ii) must have IT staff trained in cybersecurity, and (iii) department leadership must accept the risk of having full autonomy.

Cybersecurity budget

Admittedly, acquiring funds to support cybersecurity is not easy. Ideally, universities, colleges, and departments should dedicate funding for IT and cybersecurity resources, but it's difficult to retroactively reassign funds. Albeit, if research is disrupted or stolen, it will require valuable time and money to start over, and the potential cost to the institution's reputation may warrant that reassignment. That said, the best solution is to request the funding for cybersecurity staff and resources within the proposal to the NSF or other funding agencies.

6.2 Developing a Cybersecurity Program

Similar to "going it alone," a straightforward solution exists to address the paradigm of "productivity trumping security." The fact that this pattern is common within academia, however, implies that the paradigm is difficult to overcome. Indeed, the solution is to develop and adopt a security program. This endeavour requires adequate initial resources to stand up the program and perpetual leadership support to ensure security policies are followed. The security program, at a minimum, must (i) define responsibilities and roles for governance, (ii) document critical assets and the access controls necessary to protect them, (iii) allocate appropriate resources for cybersecurity, and (iv) include policies and procedures for maintaining cybersecurity hygiene.

If a unit or project adopts a sound program, it should be easy to make security decisions, and similarly it should be difficult to circumvent the security policies, procedures and controls that have been implemented. If an exception is made, that exception will be audited so accountability can be enforced. That in itself may be sufficient to deter most exceptions.

Trusted CI has worked with many research projects and centers in standing up a security program. This work has led to the development of the *Trusted CI Framework* (https://www.trustedci.org/framework) that projects, centers, and units can use to improve their cybersecurity posture. Other competing security program frameworks, such as NIST's Cybersecurity Framework and Risk Management Framework, ISO/IEC 27001, and control sets that your security program can leverage are found in Appendix C of the *Trusted CI Framework*.

Regardless of the framework chosen for developing a security program and the control sets adopted to secure your CI, it is critical that senior leadership fully supports the program. In actuality, that is one of the goals (referred to as Musts within the guide) that the *Trusted CI Framework* promulgates to the community. Moreover, leadership needs to impress upon department heads that cybersecurity hygiene must be prioritized over faculty requests or research duties. The risks of the current threat landscape and the importance of mitigating those threats need to be communicated to faculty and staff. Without senior leadership and other key stakeholder buy-in, the old paradigm will return.

6.3 Removing the Cybersecurity-hindering Culture

MSU's PA is certainly not the only unit/center/project with CI that suffers from the "we're better than you" culture. Unfortunately, there are no controls or simple fixes to this cybersecurity-constraining way of thinking. In MSU's PA case, it took a humbling experience for the unit to acknowledge and eventually move past this culture. Hopefully, other units that harbor this mindset are able to acknowledge that the culture exists, while also recognizing that it is an impediment to cybersecurity and try to overcome it before they too are humbled through a successful attack. Again, leadership is in the best position to address this.

6.4 Basic Cybersecurity Hygiene

Everything within this section would be covered by implementing a sound cybersecurity program (see 5.2), but we list a few key controls, policies and procedures that if MSU's PA department had in place, would have reduced the impact of the ransomware attack.

Delete unnecessary data — Ransomware attackers are at the top of their game in cybersecurity hacking, but they don't necessarily know the value of data-heavy research. However, they definitely know they can make money with PII. Information of that sort should be scrubbed

from servers and saved according to institutional and/or government regulations. Delete sensitive data, and retain only what's needed.

Isolate and test backups — The disaster recovery solution in PA consisted of NAS devices that were easily accessible. The current threat landscape, specifically ransomware, dictates that disaster recovery backups need to be a write-once storage device (e.g., WORM technology) and segmented or isolated from the local-area network. Moreover, once a solution is chosen and implemented, IT needs to periodically restore from the backups to ensure that the system operates as expected. Similarly, it is helpful if the solution possesses an integrity-checking ability that can be applied to the backups prior to restoration, ensuring that they have not been compromised.

Have an incident response plan — IR processes need to be in place before an attack occurs, including a point of contact list and chain of command. There should be continuity from incident to discovery to restoration. And if the institution's IT needs to be contacted, ensure that those contacts are up-to-date. PA's IT staff was handicapped during the incident by not having a clear playbook, by not knowing who or how to contact key staff, and because MSU's IT IR effort was split among different groups. Additionally, that playbook should have a posture the institution will take with regard to ransoms. In this case MSU was not going to pay a ransom.

Provide cybersecurity awareness training — Units should periodically require all IT staff to participate in cybersecurity awareness training. Not only will that ensure they understand basic cybersecurity hygiene, it will also expose them to the current threat landscape.

Take advantage of external experts — Finally, providing that the unit has moved past the dangerous "go it alone" mantra, we advise them to seek help from outside cybersecurity groups that focus on academia. The consultation is usually not free, however, some organizations operate through shared personnel resources the unit can supply. That is, if a unit can offer half of a full-time employee (FTE) for a period of three to six months, a consultation should be able to complete a cybersecurity review of the unit's CI. This is a great way to understand not only what you have in place, but what assets are critical and how best to secure them. With a full FTE or more, a unit can develop and implement a security program (see 5.2).

7 Conclusion

The rise in ransomware attacks puts open-science research at great risk. The issue is further complicated as many academic units have great autonomy, yet due to pre-existing culture, they may not be aware of the rapidly evolving threat landscape, and thus, fail to adequately secure their cyberinfrastructure. Such an event occurred in the Physics and Astronomy department at MSU. Fortunately, MSU chose to be transparent about the incident in an effort to encourage the academic community to learn from this real-world example, to better understand the damage caused by cyberattacks, and to take proactive steps to protect higher education cyberinfrastructure.