HOW CYBER HYGIENE PROMOTES INFORMATION AND DATA SECURITY FOR RESEARCH INSTITUTIONS IN A NEW ERA FOR REMOTE WORK

By Anne Pifer, Merritt Neale, Matthew Tryniecki and Greg Smith

In March 2020, in-person teaching and learning were brought to a halt nearly overnight as governments, colleges and universities acted to prevent the spread of the COVID-19 virus. While higher education administrators and faculty scrambled to transition to a remote teaching and learning model as physical campuses were closed, they also struggled to respond to unique research needs regarding wet and dry lab operations and clinical research conduct. Instantly, many researchers began accessing data and continuing to track project plans from home, with or without appropriate information security safeguards provided by their institutions.

More than a year later, some institutions are rethinking the need to provide dedicated physical space for research faculty, staff and administrators who don't require labs or special equipment on campus. But cost savings and conveniences realized in this new model will not come without an abundance of complicated considerations for the deployment of dedicated virtual facilities that are required for personnel who operate off campus.

Permanent remote models for research conduct present significant threats and vulnerabilities to sensitive intellectual property unless careful configurations of both technology and business process controls are established. An uptick in cyber incidents targeting research institutions (universities and academic medical systems alike) as well as increasingly stringent sponsor requirements related to data protection and security present risks that are more than a threat to research integrity: Moving significant portions of the United States' broader research enterprise to a full-time remote model without adapting information security protocols could have dangerous implications for matters of national security.

To prevent the risk of purposeful or inadvertent exfiltration of federally funded research data and technologies to foreign entities, U.S. laws and policies for export control management regulate and limit the release of scientific and technological information and technologies to foreign nationals, both within and outside the country's borders. U.S. laws typically require permission, known as an export license, before provisioning access to certain technologies not in the public domain, or shipment or transport of specific items overseas.

Well before the pandemic, the federal government was ramping up efforts to protect U.S. research assets and close vulnerability gaps related to undue foreign influence, including:

- Instances of faculty members failing to disclose their participation in foreign talent programs.[1]

- Improper compliance with reporting requirements related to the receipt of foreign research grants, contracts and gifts.[2]
- Addressing higher education-specific compliance issues related to export controls.[3]

Awareness of the importance of securing the U.S. research enterprise and research data security intensified as American research institutions contributed to the global efforts to develop and roll out COVID-19 vaccines. In May 2020, the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) announced increasing cybersecurity threats to COVID-19-related research, including instances in which U.S. research organizations were targeted by Chinese-affiliated hackers in an attempt to identify and illicitly obtain valuable intellectual property and public health data related to vaccines, treatments and testing from research institution networks.

Many colleges and universities have already struggled to maintain basic controls and protocols in this area — and federal agencies have acknowledged regulations have been interpreted inconsistently. Research, information technology and security leaders recognize the increasing frequency of data breaches at research institutions, as well as the risks posed by the growing acceptance of remote research work. These leaders, therefore, must devote more attention and resources to achieve requisite information security compliance requirements and target maturity levels. They must also consider more frequent formal assessments of information technology environments against recognized information security frameworks, including the National Institute of Standards and Technology (NIST) and Department of Defense (DOD) standards for safeguarding sensitive research data.

Identifying Restricted Research Activities

The preponderance of university research portfolios is not subject to export controls, and some research contracts that are a part of a broader controlled initiative receive carveouts from federal sponsors specifically designed for colleges and universities, commonly known as the fundamental research exclusion (FRE). This determination is for "basic and applied research in science and engineering where the resulting information is ordinarily published and shared broadly within the scientific community" as well as research conducted with publicly available information. Exceptions to the FRE come into play when there are restrictions involved, which can occur on certain government-funded projects. Consequently, anything from biological research to algorithms can be subject to export controls and considered restricted research.

Colleges and universities are by now aware of Special Publication (SP) 800-171, issued by NIST, which contains a specific control framework and is contractually required in some federal government award mechanisms that support research involving controlled unclassified information (CUI). The Department of Defense's cybersecurity maturity model certification (CMMC), a broader, more robust cyber compliance program for DOD contractors, has also begun to draw attention across the higher education landscape, as instances when compliance with this framework is contractually required have also increased. In 2016, the Department of Education also recommended that colleges and universities look to the control framework provided in NIST SP 800-171 for guidance on information security protocols, even in the absence of CUI. Proactive assessment against both frameworks, even in the absence of a contractual requirement to comply, has become best practice. As research institutions continue to operate remotely, research leaders should be able to quickly identify which programs may require more stringent information security environments.

The decisions are based on the types of research that are occurring and the requirements of their sponsored awards, including which should potentially remain on-site due to institutional information security capabilities.

Assessing Vulnerabilities and Taking Action

For colleges and universities with faculty engaging in restricted research, a comprehensive evaluation of the volume and proximity of research activity will inform the level of risk and inform plans to secure data. Research data security road maps can begin with near-term solutions that can be implemented on an accelerated timeline. However, these road maps should also encompass long-term strategies leading to the development of a robust compliance infrastructure that can support more-complex research programs. Efforts should consider the pace at which standards and protocols can evolve to meet new threats and subsequent compliance requirements. While institutions with smaller research programs may not have research data security listed high on their resourcing priority lists for IT and compliance investments, just one infraction can have a significant impact.

Immediate areas of investigation and action to consider include:

- **Hardware and software policies** to ensure remote researchers are using equipment and programs issued by the institution instead of personal devices or unauthorized programs when engaging in research activities.
- **Licensing agreements** and potential security risks associated with third-party communication platforms and out-of-support virtual private network clients for remote work. (These increase risks of evolving supply chain hacks.)
- **Endpoint security controls** such as data loss prevention (DLP) tools and security information and event management (SIEM) systems to classify and monitor restricted data.
- **Virtual desktop infrastructure** for greater control over remote access to resources as well as encryption software to block keylogging spyware. (Security software can also remotely monitor keystrokes and take screenshots, but administrators must be careful to consider privacy concerns and applicable employment laws.)
- **Internal cybersecurity education programming** on how foreign hackers might use social engineering on remote faculty members and students (such as phishing and pretexting) to gain access to controlled information.

Long-term strategies and solutions require more time, effort and resources, but as higher education continues to consider both on-site and virtual models, and as requirements for baseline cybersecurity protocols continue to evolve, more intensive institutional investments in these areas will become increasingly necessary.

- **Comprehensive security management program:** In addition to evaluating remote research vulnerabilities, a holistic view includes technical, physical and administrative controls as well as compliance with regulations in other areas (such as federal laws restricting the release of medical and educational information, Europe's General Data Protection Regulation, etc.).
- **Secure technology enablers:** Next-generation platforms such as secure enclaves offered by major cloud vendors more efficiently capture and manage export compliance workflows, business processes and checkpoints.
- **Updated government standards, regulations and certifications:** If appropriate (e.g., an institution regularly contracts with DOD or engages in affected research activities), universities and colleges might examine obtaining a NIST 800-171 and/or CMMC certification with a special focus on how these complex controls will operate in a remote environment.

Enabling remote research presents new opportunities for colleges and universities, faculty, and students in terms of both innovation and efficiency, but it also presents heightened cybersecurity and compliance challenges. Acknowledging threats and vulnerabilities and proactively moving to align with applicable guidelines, certifications and laws can help ensure that sponsored research data, intellectual property, and technologies don't fall into the wrong hands.

[1] "Harvard University Professor Indicted on False Statement Charges." The United States Attorney's Office District of Massachusetts, June 9, 2020. https://www.justice.gov/usao-ma/pr/harvard-university-professor-indicted-false-statement-charges.

[2] Redden, Elizabeth. "Foreign Gift Investigations Expand and Intensify." Inside Higher Ed, Feb. 20, 2020. https://www.insidehighered.com/news/2020/02/20/education-department-escalates-inquiry-reporting-foreign-gifts-and-contracts.

[3] "State and Commerce Should Improve Guidance and Outreach to Address University-Specific Compliance Issues." United States Government Accountability Office, May 2020. https://www.gao.gov/assets/gao-20-394-highlights.pdf.

Key Takeaways

Think differently.

Be aware of the risks of research conducted remotely, especially when it involves controlled information, and the potential impact of noncompliance with U.S. laws and guidelines on matters of national security.

Plan differently.

Anticipate the range of the institution's vulnerabilities and potential risks to research when conducted remotely, and create short- and long-term strategies for addressing them.

Act differently.

Integrate more stringent controls across the research enterprise, maintain vigilance regarding potential threats to controlled research in the remote environment and actively monitor government regulations and updates.

HURON

huronconsultinggroup.com

21-2643