Enhancing Cybersecurity and Maintaining Compliance in Higher Education

To protect federal grant money and keep critical data secure, universities must standardize and mature their cybersecurity readiness

Cybersecurity is critical for higher education research institutions. Researchers who study topics ranging from healthcare to education to national security often handle sensitive information that could be vulnerable to cyberattack.

These cyberattacks are not hypothetical: they are already happening. In 2018, state-sponsored hackers were arrested for stealing data from 300 universities, including 144 in the United States. Along with accessing the emails of thousands of professors, the hackers also captured more than 30 terabytes of intellectual property and data — according to the FBI website, this is approximately three times the amount of print data in the Library of Congress.[1]

Growing Risk of Data Loss and Theft

The COVID-19 pandemic has increased the likelihood of a successful cyberattack within higher education. With many university departments working remotely during the pandemic, employees often access employer networks using their own (potentially unprotected) devices, increasing the risk of a security breach.

In early 2021, Oxford University's Division of Structural Biology (which had been researching COVID-19 vaccinations) suffered a data breach in which a criminal group accessed, and may have sold, sensitive data.[2]

To protect their intellectual property, universities need to strengthen cybersecurity across their data estates, particularly within their research departments.

Not only is cybersecurity critical for protecting information and keeping institutions secure from outside threats, it is also becoming mandatory. The Department of Defense (DoD) now requires higher education institutions (as well as federally funded research and development centers) that receive government research grants to meet the DoD Cybersecurity Maturity Model Certification (CMMC).

Once required solely for federal contractors, this certification verifies that a research institution is compliant with the government's required level of cybersecurity.

Beginning in fall 2021, a Controlled Third Party Assessment Organization (C3PAO) will audit research institutions to assess CMMC compliance.

There are multiple benefits for higher education research institutions that maintain CMMC compliance. First, compliance ensures institutions continue to receive funding for grants they have already applied for, and it may also increase the chances that an institution will receive future funding. Institutions who are not compliant run the risk of losing DoD funding they have already secured.

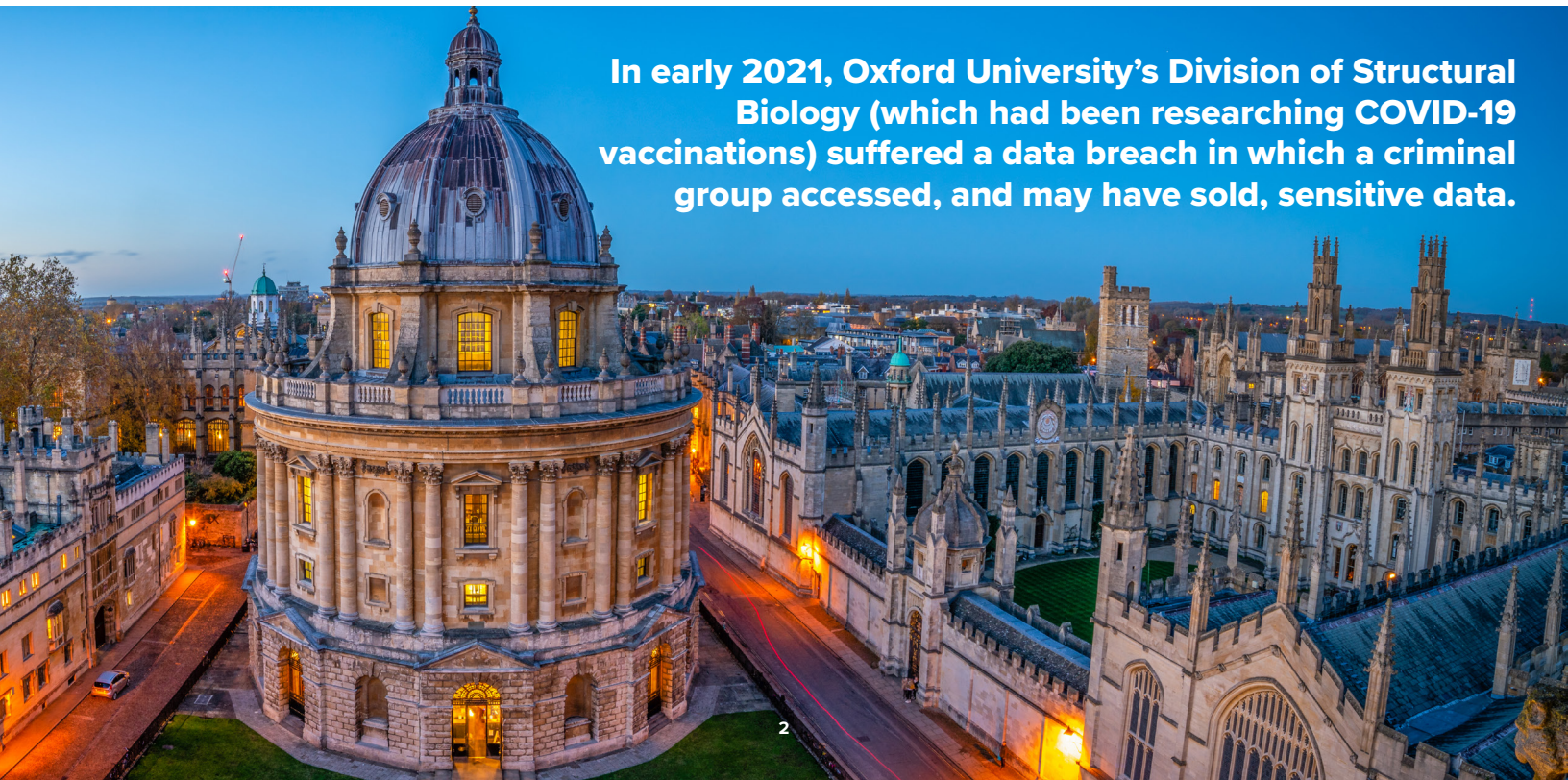
Meeting CMMC standards is thus "a revenue enhancement tool and a revenue protection tool," says Gary Buonacorsi, chief IT architect and SLED CTO of Tanium, a leading IT management and security company. This is critical for many academic research departments across disciplines that rely heavily on DoD funding.

Moreover, maintaining CMMC compliance can be a first step for universities to improve their cyber hygiene more broadly. As Buonacorsi explains, "compliance will not only help institutions maintain revenue, but it will also make it more difficult for cyber threat actors to engage in intellectual property theft. It will help create a hardened environment and will instill the value of practicing good cybersecurity in the higher education space."

Maintaining CMMC Compliance

The CMMC model measures an institution's cybersecurity through a maturity-level rating system. Each of the five designated levels includes particular processes and practices that an institution needs to follow to be CMMC compliant, and each level builds upon the one below it.

The processes range from "performed" (level one) to "optimized" (level five), and the practices range from "basic



cyber hygiene" (level one) to "advanced/progressive" (level five). The higher the achievement level, the more protected the institution is against potential cyber threats.

Each organization must achieve a particular maturity level, depending on a number of factors. These factors include the sensitivity of information being maintained, the type and likelihood of threats, implementation complexity and cost.

To maintain CMMC compliance, higher education institutions need to demonstrate adherence to the processes and practices of their assigned maturity level on an ongoing basis.

"Compliance is not something you can do one time and then forget," says Doug Thompson, technical solutions engineer for Tanium. "It is a process that requires institutions to put tools and procedures in place to ensure they do not become non-compliant and be better prepared for an audit at any time."

Unifying a Siloed System

One of the first steps a research institution needs to take to achieve CMMC compliance is to simply understand their environment: They need to know what software is running and what devices are in their network to protect it against threats.

This step is also one of the biggest challenges to maintaining compliance. Research departments within higher education institutions are accustomed to working independently. They typically run as autonomous entities, earning and spending their own research funds.

This independence often extends to information technology (IT): Many departments have their own IT infrastructure to protect their data.

Many universities therefore have a patchwork of cybersecurity solutions and point products, many of which do not speak to each other. This becomes a problem for maintaining CMMC compliance. Research departments often lack the operational and security expertise to maintain CMMC compliance themselves. But if an institution's IT leadership lacks full visibility into each department's security system, they cannot confirm these environments meet CMMC requirements.

In addition, it is increasingly hard for central IT departments to have full visibility into all assets on a network. Many researchers access employer networks on their own laptops, phones and other devices.

"Complexity equals risk plus cost," explains Buonacorsi. If institutions continue to purchase and implement new point products to resolve individual departmental problems, they will be creating an increasingly intricate environment that is rife with vulnerabilities and fails to meet CMMC requirements.

To achieve CMMC compliance, IT departments need to have full visibility into all assets on their network, as well as a clear process for enforcing those controls. This requires standardizing cybersecurity in a way that many research institutions are not yet doing.

Turning to Experts in Cybersecurity Software

To increase and improve cybersecurity while also maintaining compliance, universities can turn to expert providers in endpoint management and security solutions. This kind of software can provide the visibility IT leaders need, along with analytics and reporting that will quickly identify any potential threats.

When looking for the ideal solution for their institutions, university CISOs should select a product that can provide insight into their institution's cyber hygiene through a number of strategies.

To achieve CMMC compliance, IT departments need to have full visibility into all assets on their network, as well as a clear process for enforcing those controls.

For example, an effective solution will offer asset discovery, which allows institutional leaders to quickly wrap their arms around their environment. In the often-siloed space of higher education, IT leadership needs to quickly identify authorized and unauthorized devices and software.

Along with better visibility, the product should provide institutions with threat monitoring across the enterprise. A solution with unified endpoint management can evaluate and analyze millions of endpoints at once, quickly identifying and mitigating threats.

To maintain configuration compliance, an endpoint management and security solution should also have a configuration management tool. This helps an institution ensure all endpoints and servers are adhering to their configuration policy, preventing potential vulnerabilities.

Finally, the ideal solution will have clear and concise compliance reporting dashboards that update in real time. These should track and report on a network's security status, pointing out any vulnerability risk or exposure. With continuous reporting, IT leaders will always know whether or not they are in compliance, which will allow them to respond more easily to any CMMC audits.

“Compliance can help universities foster a culture of cybersecurity within higher education. Robust cybersecurity will now be a requirement for doing business, protecting intellectual property and securing revenue.”

Gary Buonacorsi, Chief IT Architect and SLED CTO, Tanium

With a multifaceted security tool that provides comprehensive endpoint management, threat monitoring and incident analysis all in one platform, universities will be able to protect their intellectual property and remain compliant.

The Future of Cybersecurity and Compliance

While the DoD is the first government agency to require research institutions to maintain CMMC compliance, it likely will not be the last.

Other federal programs, including those related to healthcare and education, may begin to require a similar certification for anyone receiving funding from their departments beginning in the next five to 10 years.

Most higher education institutions receive research funding in some form from the federal government, which continues to be the largest funder of academic research and development in the country.[3] Because of the prevalence of federal funding, and continued concerns about potential cybersecurity threats, CMMC compliance is likely going to impact the majority of research institutions in the coming years.

With multiple COVID-19 stimulus packages providing funding to colleges and universities (including the CARES Act Higher Education Emergency Relief Fund and the most recent American Rescue Plan Act of 2021), now is an opportune time for IT leaders to consider implementing an endpoint management and security system. With funding available, higher education leaders can begin to consider ways to protect the security of their institution and ensure the security of any federally funded grants now and in the future.

CMMC compliance has the potential to serve as a first step toward establishing more robust, standardized cybersecurity within universities.

“Compliance can help universities foster a culture of cybersecurity within higher education,” contends Buonacorsi. “Robust cybersecurity will now be a requirement for doing business, protecting intellectual property and securing revenue.”

This piece was developed and written by the The Center for Digital Education Content Studio, with information and input from Tanium.

Endnotes:

1. *https://www.fbi.gov/news/stories/nine-iranians-charged-in-hacking-scheme-032318*
2. *https://www.forbes.com/sites/thomasbrewster/2021/02/25/exclusive-hackers-break-into-biochemical-systems-at-oxford-uni-lab-studying-covid-19/?sh=2b9c5e612a39*
3. *https://ncses.nsf.gov/pubs/nsb20202/academic-r-d-in-the-united-states*

Produced by: CENTER FOR DIGITAL EDUCATION

For: TANIUM

The Center for Digital Education is a national research and advisory institute specializing in K-12 and higher education technology trends, policy and funding. The Center provides education and industry leaders with decision support and actionable insight to help effectively incorporate new technologies in the 21st century. **www.centerdigitaled.com**

Tanium offers a unified endpoint management and security platform that is built for the world’s most demanding IT environments. Many of the world’s largest and most sophisticated organizations, including nearly half of the Fortune 100, top retailers and financial institutions, and several branches of the US Armed Forces, rely on Tanium to make confident decisions, operate efficiently and effectively, and remain resilient against disruption. Tanium has been named to the Forbes Cloud 100 list of “Top 100 Private Companies in Cloud Computing” for five consecutive years and ranks 10th on FORTUNE’s list of the “100 Best Medium Workplaces.” Visit us at **www.tanium.com** and follow us on LinkedIn and Twitter.

© 2021 e.Republic. All rights reserved.