UNISYS | Securing Your Tomorrow®

The growing challenges of securing Australasian academia.

By Gergana Winzer

For many universities, research is critical not only to maintain links with industry, but also to generate income.

The education sector in Australia and New Zealand has become a prime target of malicious cyberattacks as is evident in the growing number of reported attacks on schools and universities over the last few years. These include the NSW Department of Education systems just before the start of the new school term in 2021, 11 schools in New Zealand affected by the Kaseya ransomware attack, and attacks on both the Australian National University (ANU) and Australian Catholic University (ACU). In addition, in July 2021 the Tertiary Education Quality and Standards Agency (TEQSA) alerted all Australian higher education institutions to an emerging cybersecurity risk targeting the edu.au domain.

The risk is not just that the number of attacks have increased, it is that they have become more sophisticated.

This surge in cyberattacks is not surprising. Many universities and higher-education institutions around the globe have expanded notably within the past two decades in terms of sites, staff, and students, putting more pressure on the IT technologies that support them. Unfortunately, traditional IT solutions such as Virtual Private Networks (VPNs) and traditional firewall-protected networks are struggling to deliver the access and security required – not just in the academic world, but also in the new working practices that are required across all organisations. The expansion of the perimeter creates more risk and threats, increasing the importance of building a cyber resilience model that works.

In addition, while many Australian and New Zealand tertiary institutions already offered digital remote learning, the impact of COVID-19 social distancing mandates required a rapid shift to virtual classrooms for all students at all levels of education. The classroom and lecture theatre were now in the loungeroom. With this expansion of the institution's perimeter comes greater vulnerability as it provides the attackers more points to target.

Why should education institutions care? Cyber incidents can harm their service delivery and reputation and may involve:

- Theft of information such as intellectual property or sensitive personal data
- Denial of access to critical technology
- Hijacking of systems for profit or malicious intent
- Financial losses

A strong cybersecurity approach comprises technologies, processes and controls designed to protect IT systems and sensitive data from cyberattacks. And rather than focus on simply preventing attacks, it requires a framework that ensures resilience by minimising the extent of a breach if it happens – and it will happen. A cybersecurity framework should cover threat identification, protection, detection, response and recovery of IT systems.

"NSW universities should strengthen cybersecurity frameworks and controls to protect sensitive data and prevent financial and reputational losses."

– NSW Auditor General's Report – Universities 2019 Audit Office of NSW

Consider just a few of the issues routinely encountered in the educational sector:

Aligning with Compliance Regulations. After major reforms were introduced in 2014, education organisations have to comply with the Australian Privacy Principles and in 2020 similar Privacy Principles were adopted in New Zealand. Before that they were subject to baseline standards such as Payment Card Industry Data Security Standards (PCIDSS) which were to a certain extent restrictive as only relative to the people, part of the network and processes, touching Payment Card data. In ANZ many have opted to adopt measures recommended by their national government to mitigate cybersecurity incidents: the Australian Government's Essential Eight mitigation strategies, and CERT NZ's ten critical controls in New Zealand.

Meanwhile, in Australia there is also debate about whether to include higher education under the revised Critical Infrastructure Bill which will require universities to comply with more government required regulations and cyber controls.

Ultimately, there is growing scrutiny and attention on how higher education protects its cyber infrastructure and data. This requires more budget and strategic thinking around how to secure the critical assets. And regulations constantly evolve so they need to keep track and do more than they are used to.

Creating a Secure Virtual Learning and Research Environment. All higher-education establishments are developing alternative ways of teaching in this COVID-affected world. Remote and virtual learning options are becoming the norm. This paradigm shift affects every stakeholder: staff, students, guest lecturers, research partners, private sector parties, suppliers and more. These stakeholders all need properly authorised, secure, yet easy to use access to the university facilities and to the individuals with whom they interact.

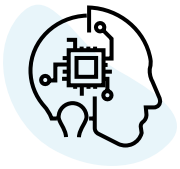
In addition, for many universities, research is critical not only to maintain links with industry, but also to generate income. However, enabling research through easy and secure access to data and collaboration is a challenge when researchers are spread across multiple sites. Now, during the global pandemic, these difficulties have been further heightened as more and more work needs to be carried out remotely, often outside the university's physical network infrastructure and the traditional firewall protection.

Effective Data Management and Protection. There are many systems within universities that deal with Personal Identifiable Information (PII), Intellectual Property (IP) and Payment card information. These systems have been upgraded and their security has been reviewed under the new Privacy Act requirements. However this must be ongoing as new vulnerabilities are discovered every day and attacks become even more sophisticated.

Overall, these issues show conclusively that academic institutions need both a secure way of segmenting their networks and the ability to provide anytime, anywhere secure access to vital resources, data, and applications.

The Limitations of Legacy Applications and the Demands of Compliance

Like many organisations responding to the need to accommodate new working patterns, universities and higher-education institutions often have infrastructures that are ill-equipped to handle new challenges, citing issues ranging from network bottlenecks to a lack of adequate security features such as role-based access, encryption in motion, and embedded software security. In addition, the lack of up-to-date security features means that achieving compliance with legislation and standards such as GDPR, CIDSS, APPs, E8, CERT NZ Top 10, NIST, CIS TOP20, ISO27001 and OWASP can be problematic.



"The last six months have shown us that it has never been more important for colleges to have the right digital infrastructure in order to be able to protect their systems … whatever the circumstance. This needs a whole-college approach and for a focus wider than just systems. It needs to include supporting leaders, teachers, and students to recognise threats, mitigate against them, and act decisively when something goes wrong."

– David Corke,
Director of Education and Skills Policy,
Association of Colleges

For those who make use of VPNs to provide secure remote access to corporate resources, the challenge is that once users are connected, they have access to large, if not to all sections of the network. This has the effect of putting sensitive data at risk because, if bad actors gain access, there are no further barriers to navigate. They are "home-free" to move where they want and steal what they want.

In terms of security failures, there are all too many examples in the news. For instance, multiple universities in the UK, US, and Canada were impacted in 2020 due to a ransomware attack against Blackbaud, a provider of alumni database software.[1]

Clearly, a better solution is required if universities and higher-education institutions are to gain the connectivity and security they need to thrive in today's world. The optimal solution will not require a "rip and replace" approach, but will instead enhance existing networks, minimising costs and disruption: whilst offering ecosystem-based approach to security integrating what is already there and justifying the existing investments where possible is desirable.

Solutions to Meet the Needs of Today's Universities

Universities tell us that they need two things: first, they need to ramp up the security of their networks to protect their staff, students, data, and research; and, second, they need to ensure that access is still easy and intuitive.

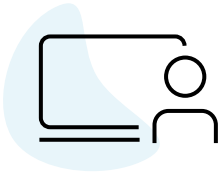
At Unisys, we provide a software-based overlay approach to network security that can be implemented with no impact to infrastructure, applications, or end users. It offers easily-managed identity-based network access and secure cryptographic segmentation with point-to-point encryption of data in motion. This solution is called Unisys Stealth® and can be readily added to legacy university applications to make them compliant and secure. Due to its point-to-point nature, this security can extend beyond traditional network boundaries; additionally, it can be used to reduce load on expensive and easily-attackable VPN infrastructure technology. In so doing, Stealth™ dramatically helps universities to separate trusted systems, users, and data from the untrusted.

This approach to micro-segmentation is transparent to users and applications. For example, if a university has a legacy application that needs to be secured, Stealth can be deployed as a network overlay technology to segment and secure the traffic for that application. The application will be far more secure yet will continue to work as normal. In fact, from a user perspective, Stealth actually simplifies access. Historically, a user might have had to log in, connect to a VPN, open a remote desktop session, and then access their application – a time-consuming and tedious process that is vulnerable at key times. In contrast, with Unisys Stealth, a user logs into the machine and simply starts the application. Stealth rapidly provides security by authenticating the user with the specific network security policies at login, and then dynamically establishes the secure tunnel to the application server exactly when it is needed.

Stealth offers a wealth of additional benefits as well, such as:

- Visibility: The Stealth Security dashboard which shows at a glance what is happening in the Stealth-protected network
- Network discovery and Stealth policy modelling so you can graphically see what is happening in your environment and secure it appropriately
- Ability to Respond and Recover: The ability to dynamically isolate suspicious endpoints or users to contain attacks from spreading and ensure forensic investigation is possible on those assets.

1. Sharma, Sonia. "Newcastle University hit by data breach aftersoftware supplier Blackbaud hacked," Chronicle Live, July 28, 2020.



In the midst of multiplied challenges, our Stealth-enabled solution stands as a proven, end-to-end solution that has been securing remote workforces for years.

Gergana Winzer
Gergana Winzer is the Industry Director of Cybersecurity, responsible for Asia Pacific at Unisys.

As an IT and cybersecurity professional for more than 14 years, Gergana's mission is to create, support and promote solutions that reduce cyber and data security risks thus empowering her clients to become cyber resilient.

She can be reached at gergana.winzer@unisys.com

- Protection: Cryptographic cloaking of assets on premises and in the cloud to make them invisible to bad actors
- Attack Surface control: A minimum of industrial-grade AES-256 encryption inside the perimeter and beyond
- Integrations: The protection of existing investments as a Zero Trust software suite that overlays almost any network, integrating with existing security software tooling
- Extensive integration and orchestration options to support current security monitoring and management software
- Interoperability and compatibility with existing network and security infrastructure

True Value for Higher Education

Universities are already profiting from the value that Unisys Stealth provides in a number of ways:

- **Strong compliance**. Because it is software-based, Stealth does not require any network hardware changes and is highly compatible with existing networks and security software. This helps smooth the way to compliance with legislation such as PCI-DSS and GDPR, as sensitive data can be readily separated from the rest of the network.
- **Efficient clearing**. Stealth enables student applications to be securely sent for evaluation to course heads who may be working remotely, enabling the university to quickly fill available places with the best-qualified students.
- **Remote access**. From teaching courses in a virtual environment to engaging in sensitive research, Stealth protects individuals and information irrespective of physical location or the device used, thereby ensuring that universities experience minimal disruption to their operations.

In the midst of multiplied challenges, our Stealth-enabled solution stands as a proven, end-to-end solution that has been securing remote workforces for years – even for users relying on untrusted devices and networks. The best news of all is that through the Unisys Always-On Access™ capability, universities and higher-education institutions can replace vulnerable VPNs with Zero Trust security now, at the exact moment easy-to-use secure access is needed the most.

If you would like to discuss the challenges that you are facing and find out how we can assist you in addressing them, please contact Gergana gergana.winzer@unisys.com and we will be happy to have a discussion with you.

For more information about our Unisys Stealth capabilities to help mitigate the risks around the major cyber attacks, visit www.unisys.com/offerings/security-solutions or contact us at unisysapac@unisys.com

For more information visit www.unisys.com

© 2021 Unisys Corporation. All rights reserved.

Unisys and other Unisys product and service names mentioned herein, as well as their respective logos, are trademarks or registered trademarks of Unisys Corporation. All other trademarks referenced herein are the property of their respective owners.