Ovum
TMT intelligence | informa

Security services play a key role in digital transformation for higher education

Publication Date: 27 Jun 2016 | Product code: IT0008-000274

Nicole Engelbert

Ovum view

Summary

Securing institutional assets is a critical step in a college or university's ability to embark on the road to digital transformation. A unique operating environment and mission for the higher education industry makes this a particularly difficult task. Nevertheless, institutions must commit to investing in security solutions and strategies that enable long-term flexibility and agility without compromising on performance. Shifting a growing percentage of the IT department's headcount and budget to security is not the answer. Rather, Ovum advises colleges and universities to partner with service and solution providers in order to access best-in-class capabilities from experts dedicated to the IT security market, freeing them to focus on their business transformation initiatives.

Colleges and universities have unique security requirements

Higher education presents a unique set of security challenges. The primary mission of any college or university is the transmission of knowledge. This can take many forms, including the development of cutting-edge research led by university faculty that transforms the way the world understands complex problems; classroom instruction – virtual or "bricks and mortar" – that develops a student's skills in his or her area of study; interactions among members of the university community that lead to personal development; and even collaboration among employers and faculty to develop programs of study better aligned to workforce needs. An environment that fosters these types of interactions must be exceptionally open. Research increasingly occurs collaboratively across multiple institutions, requiring faculty to access common data and technology solutions. Key stakeholders in program development, for example employers, community leaders, and policy-makers, are often neither employed by nor enrolled in the institution but must have the ability to access records and documents. More so than any other industry, the boundaries of the higher education enterprise are intentionally porous.

Yet, at the same time, institutions collect a staggering amount of confidential and highly valuable data, and as a result they are subject to considerable regulatory demands to ensure its protection. Social security and credit card numbers, health records, donor information, and research data, to name just a few, necessitate more robust data management techniques to ensure only authorized access from both a best practice and compliance perspective. For example, US institutions are subject to a slew of regulatory requirements, such as the Family Educational Rights and Privacy Act (FERPA) and Health Insurance Portability and Accountability Act (HIPAA) laws, as well as a myriad of requirements related to federal grant programs. Creating an open platform for engagement and collaboration while simultaneously ensuring only authorized access is a tall order indeed.

The challenge of finding the balance between openness and authorization is further exacerbated by the complexity of identity within most institutions, the frequency with which end-user identity changes, and how access occurs. Consider the following examples:

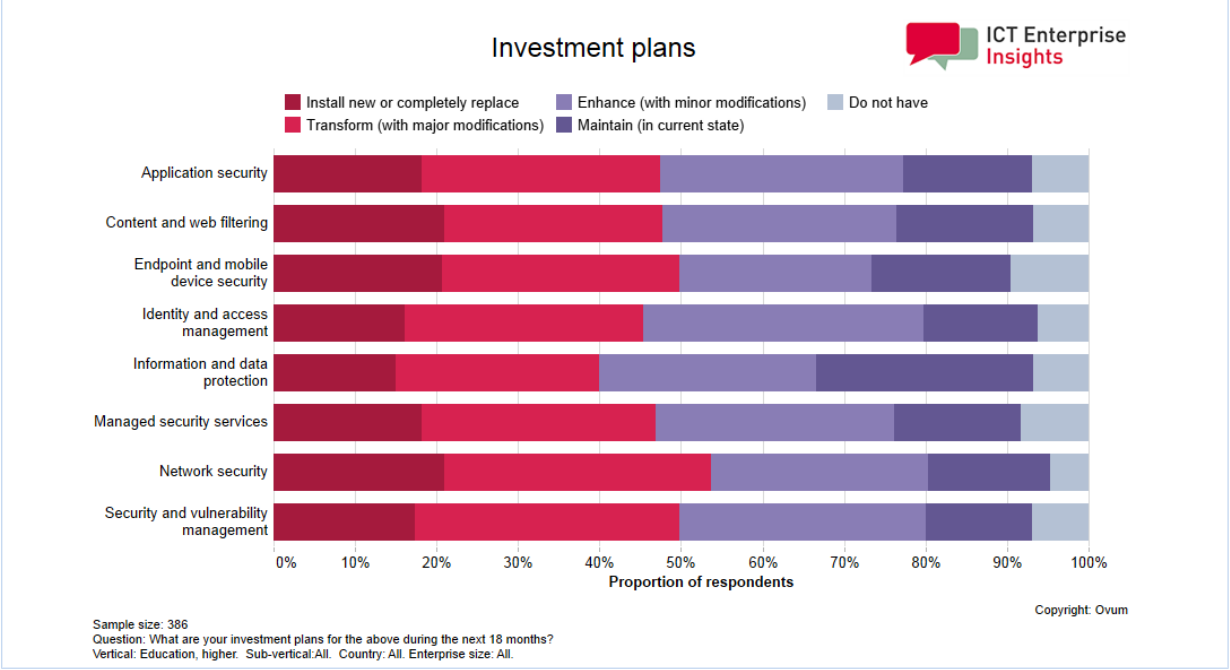
- a graduate student who is working as a residential life director at the undergraduate college
- a human resources associate who is also on the faculty of another institution but is collaborating on a federal research study
- an alumna who is on an employer advisory committee working on the development of a new academic program.

While these examples might seem extreme, they are all well within the bounds of standard operations for any research-intensive university. Moreover, because most colleges and universities operate on a semester- or term-based enrollment calendar, there tend to be large shifts in institutional identity every three to five months. Now let's consider a few common examples of how end users access institutional resources:

- a student reading academic journals online on a tablet while at a coffee shop off campus
- an employer advisory board member accessing accreditation documents on a collaboration platform from his or her corporate smartphone using the Wi-Fi in an airport lounge
- a faculty member downloading reports to his or her personal laptop from a cloud-delivered analytics solution purchased by a grant program but not managed by central IT.

Supporting, and ultimately securing, such a diverse array of device types, configurations, and access points adds further complexity. Consequently, managing identity and security in such an environment is an exceptionally difficult challenge for colleges and universities.

Figure 1: Security is an area of near-term investment for higher education



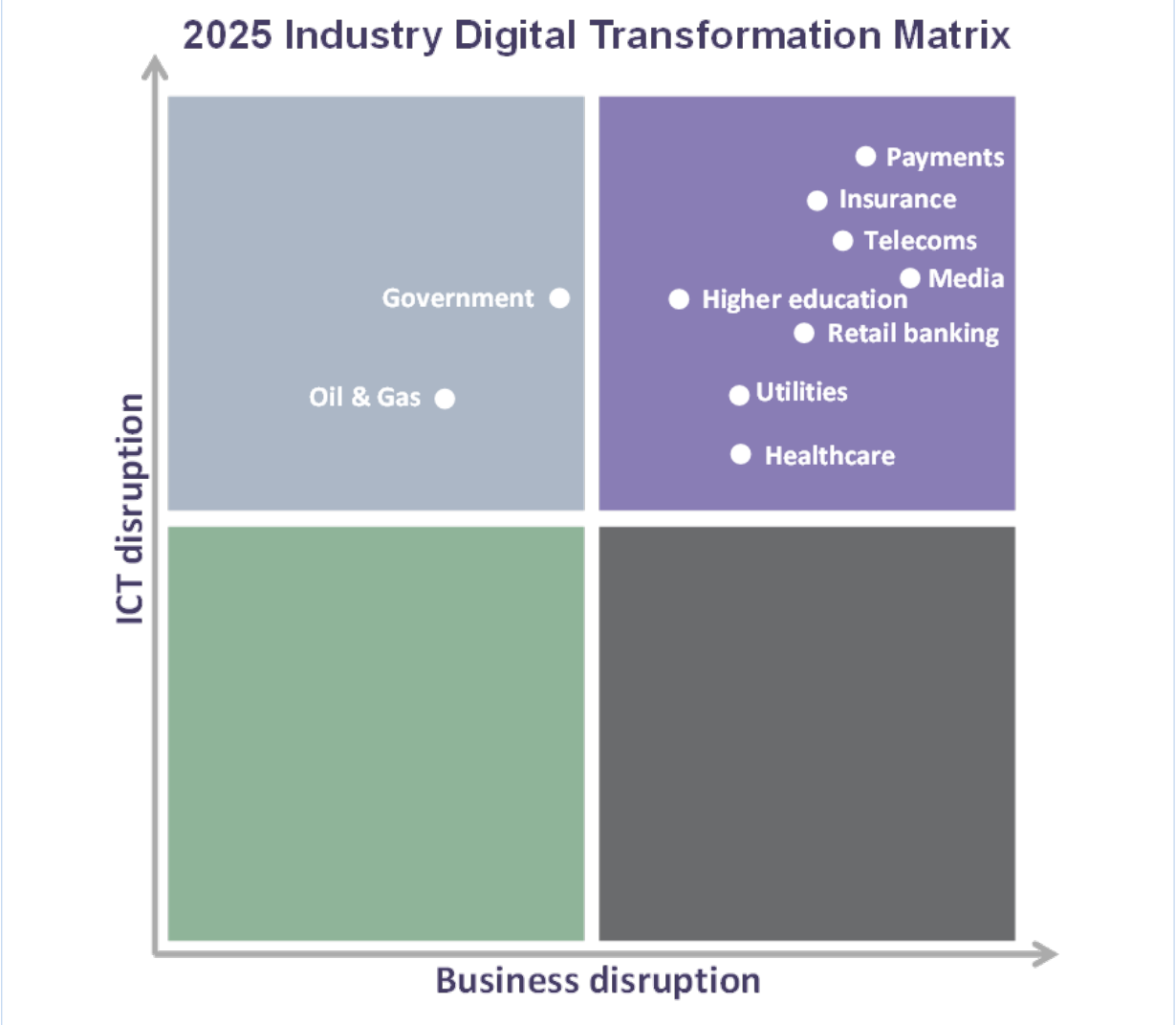
Source: Ovum ICT Enterprise Insights, Global 2015

It is, therefore, hardly surprising that colleges and universities are investing aggressively in security solutions across a broad array of areas. In Ovum's recent *ICT Enterprise Insights* survey, nearly 50% of IT decision-makers in higher education reported the intention to install new or transform with major modifications their security solutions over the next 18 months. Ovum believes that there is increasing recognition in the industry that more sophisticated approaches to managing identity and security are critical – almost foundational – to enable transformational initiatives such as improving student success, developing new academic programs, and increasing capacity for innovation.

Digital transformation depends on a more sophisticated security strategy

The topic of digital transformation is difficult to avoid. The degree of disruption facing the higher education industry is historic, driven in part by shifting student demographics, more rapid economic boom-and-bust cycles, globalization, workforce development requirements, technological innovation, and even consumer market trends. In light of these developments, existing models for delivering education services are being reconsidered in order to find more innovative, agile, and fiscally sustainable ones. Without question, colleges and universities recognize the critical role of technology in these new models, such as the creation of more robust online learning platforms (OLPs), leveraging big data techniques to solve complex research problems, utilizing telepresence to enhance virtual collaboration, and even using blockchain to maintain multi-institution transcripts. In Ovum's recent *Digital Economy 2025* research series, higher education was positioned in the top right-hand corner of the Digital Transformation Matrix, indicating the industry's strong likelihood of witnessing profound business and technological disruption, ultimately driving it to shift a growing percentage of its core services to a digital environment.

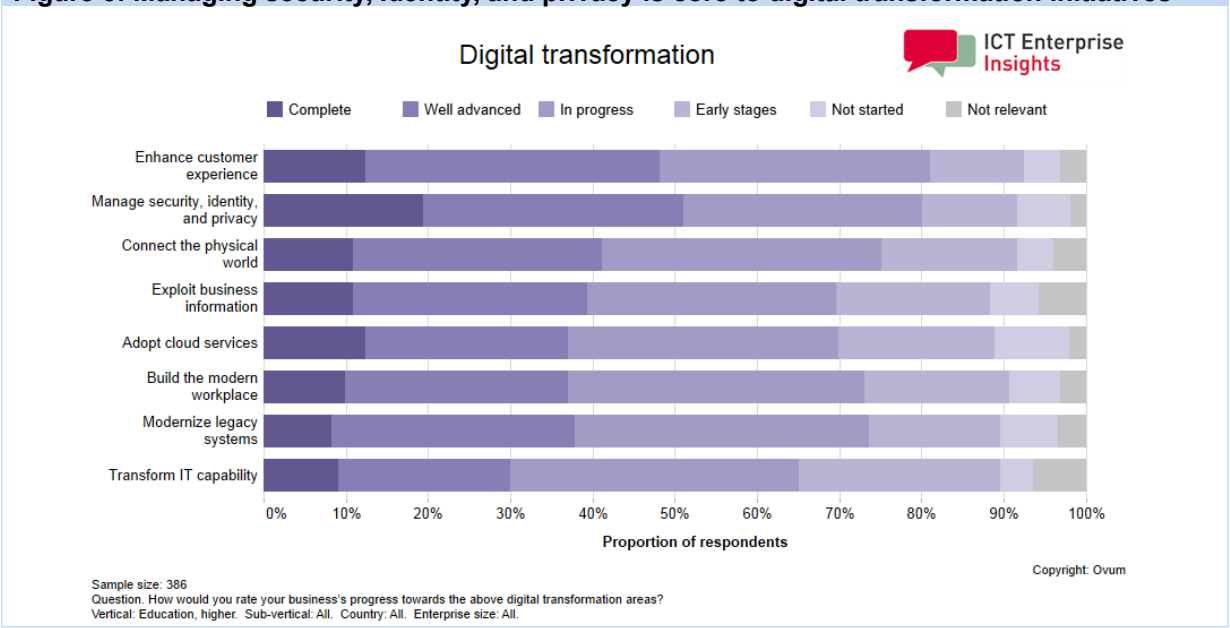
Figure 2: Ovum's Digital Transformation Matrix



Source: Ovum, Digital Economy 2025: Industry Context

While each of the technology examples given above has enormous potential, their ability to digitally transform higher education depends, at least in part, on the application of more robust security and identity management. OLP, collaboration with big data, telepresence, and blockchain all require a much greater degree of openness for participation, while simultaneously exposing the institution to a much higher degree of security risk. Colleges and universities included in Ovum's 2015 *ICT Enterprise Insights* survey echoed this concern, reporting managing security, identity, and privacy as the most advanced component of their digital transformation strategy. The challenge is to employ a strategy, technology, and services that are sufficiently future-proofed to be able to support rapidly evolving business requirements while contending with increasingly sophisticated security risks. Embarking on a successful digital transformation journey requires a far more advanced approach to security.

Figure 3: Managing security, identity, and privacy is core to digital transformation initiatives



Source: Ovum ICT Enterprise Insights Survey, Global 2015

Finding the right partner to deliver best-in-class service

At the most basic level, teaching, learning, and research is the core service of higher education. While the institutional mission might shift priorities and how services are delivered, every other function is a supporting or auxiliary one. Successful institutional transformation requires focusing on core functions and differentiators rather than spending attention and precious resources on non-core capabilities. This is not a new concept for the industry. Dining services, student loan administration, and bookstores, among other services, have long been outsourced as a strategy to reduce costs while maintaining or even improving service quality. With the growing acceptance of cloud technology, IT departments are also embracing the mandate to focus on their core service and entrust other functions to external experts. Because security and identity management is a rapidly evolving area, technical expertise is rare and, as a result, expensive. Few institutions, even the most wealthy, have the necessary resources to recruit and retain sufficient technical staff, at the right skill level, to even keep pace with the most basic requirements of securing institutional assets and data. Moreover, existing IT staff often "wear multiple hats," making it difficult for them to develop the highly specialized expertise required in this area.

Consequently, Ovum advises colleges and universities to partner with vendors capable of not only delivering advanced security solutions but also sustaining ongoing investment in them, thereby ensuring their ability to meet the needs of a continuously evolving set of institutional requirements and an escalating threat landscape. An established history of working with the industry is critical to the vendor's ability to understand and address the unique security requirements of higher education. However, Ovum believes that vendors also possessing expertise developed either horizontally or from other industries with more demanding or high-profile security requirements, such as retail, financial services, or even defense, are likely to bring a more proactive and cutting-edge approach to their solutions and services. At the end of the day, selecting the right vendor partner for security is a crucial step toward realizing value from a digital transformation strategy.

Appendix

Further reading

Making the Move from IT Maintenance to Innovation in Higher Education, IT0008-000269 (May 2016)

Digital Economy 2025: Industry Context, IT0008-000259 (April 2016)

2016 Trends to Watch: Security, IT0022-000522 (October 2015)

Authors

Nicole Engelbert, Director of Research & Analysis, Ovum Technology

nicole.engelbert@ovum.com

Ovum Consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Ovum’s consulting team may be able to help you. For more information about Ovum’s consulting capabilities, please contact us directly at consulting@ovum.com.

Copyright notice and disclaimer

Any views and/or opinions expressed in this product by individual authors or contributors are their personal views and/or opinions and do not necessarily reflect the views and/or opinions of Informa Telecoms and Media Limited.

CONTACT US

www.ovum.com
analystsupport@ovum.com

INTERNATIONAL OFFICES

Beijing
Dubai
Hong Kong
Hyderabad
Johannesburg
London
Melbourne
New York
San Francisco
Sao Paulo
Tokyo