Securing Higher Education

Addressing five common security challenges for higher education providers

Introduction and purpose

A more connected world offers many advantages in terms of information sharing and communication.

But by its very nature, being more connected introduces new threats, as organisational boundaries become blurred. At the same time, the tools used by attackers have become more sophisticated but also easier to use.

This change in the threat domain is a constant challenge for all organisations, not least those delivering public-facing services, and the increasing prevalence of new threats, such as ransomware, demonstrates that attackers are adapting at a faster pace and organisations are struggling to respond.

As higher education institutions continue to use digital technology in innovative ways to build superior learning and research facilities, they will be even more exposed to threat. This risk is elevated further by the unique openness that universities must demonstrate to allow ever greater collaboration within academia and the public and private sectors.

In this document, we set out five common security challenges facing higher education establishments. In response, we propose that security should be treated as a system and blended into an architectural approach that more directly aligns business needs with the technology domain. And finally, we demonstrate solutions that help to create that security system, offering the best possible mitigation.

In the event of a successful cyber attack, higher education institutions face significant risks to their brand and reputation – two assets that are critical for attracting both students and important research funding. Universities also face financial and legal risks, as many rely on access to data from third-party organisations that could be personally or commercially sensitive.

These opposing needs create a unique set of challenges for higher education institutions that necessitate careful management to ensure the right balance. In turn, this balance requires a fully engaged set of stakeholders able to clearly communicate their business and security needs, so that the right controls can be in place to enable the best experience for staff, students, and researchers.

Striking this balance is essential, yet traditional approaches to information governance and security are failing to meet the challenge of dealing with a rapidly changing threat and business landscape. Security models focused solely on hardening the network perimeter and endpoints are failing and can no longer be relied on.

Contents

Five common security challenges for higher education organisations

The evolution of the threat domain has seen an increase in the number of vectors that need to be considered, along with the ever-present threats that are typically procedural (such as patching) or human behaviour related. Here we identify five threat vectors that are common to all higher education organisations and suggest how to mitigate these challenges.

1. Malware

Malware represents one of the greatest cyber threats to all organisations, including higher education. The near exponential rate at which new malware variants are released, alongside the inherent limitations of the current signature-based defences, is resulting in a high risk of infection.

Ransomware, for example, has seen a significant increase and has been responsible for several high-profile cyber incidents. It remains an easy route for criminals to extort significant sums of money from their victims. In addition to financial risks, a ransomware infection can have a significant impact on higher education operations, particularly if research systems are infected, rendering them unusable until they can be recovered.

A robust backup and recovery procedure continues to be one of the primary lines of defence against ransomware. However, in many cases the risk of initial infection can also be reduced through a combination of improved user education and the deployment of defensive controls that don't simply rely on signatures alone.

2. Security vs. openness

Unlike traditional enterprise organisations, higher education institutions are uniquely challenged by their lack of organisational boundaries. This openness is, of course, essential in order to support the high degree of collaboration required within the academic and research community. However, it also results in conflict between the need to maintain some degree of control while maintaining this openness.

In addition, students are some of the earliest adopters of new technology trends, especially cloud and social media applications. These must be carefully monitored for suspicious activity to ensure that the environment isn't exposed to increased risk.

Balancing the need for openness and security necessitates a more dynamic security architecture, one that is able to align closely to the needs of students, researchers and staff. Too tight and users will find routes around controls; too open and the environment is left exposed, leading to an elevated risk of damage to brand and reputation, and potentially even exposing the institution to legal and financial penalties.

3. Effective risk management

Alongside the security vs. openness challenge is the need to establish an effective and comprehensive risk management programme. The very nature of higher education institutions means that there are constant conflicts between the need for open collaboration and the understanding that a university may be handling highly sensitive data sets.

Establishing a risk management regime that recognises and identifies the importance of the data produced by the university and the threats posed against it is essential. This must be performed in collaboration between the university corporate function and the researchers and administrators who are responsible for collecting, managing, and publishing data.

Only once the risk is clearly understood can institutions develop a proportionate and targeted set of controls. Establishing this clear link between risk and control is essential in order to support sound security investment decisions and effectively manage the greatest risks to the institution.

Working with other higher education organisations is also key to minimising the risk of attack and limiting the damage caused by security breaches, from sharing intelligence about known threats to collaborating in the development of risk management procedures.

4. Incident response preparation

In the past, the focus and indeed the measure of security was based on blocking the threat. Security solutions were designed fundamentally to keep threats from infiltrating the network. However, the sheer complexity of modern networks, coupled with the sophistication of malware, means this approach to security is no longer viable.

Today, it is no longer if a security incident will occur, but when. In the face of this new reality, higher education institutions must implement robust incident response plans.

Such plans cannot be isolated to the IT function. The potential impact of a cyber attack on an organisation means that incident response plans must align to existing business continuity plans and should also take into account the processes for engaging external professional support and law enforcement agencies. These plans should also consider the implications of the mandatory breach notification requirements of the EU General Data Protection Regulation (GDPR), in force from May 2018, in which organisations must now report breaches of personal data to the relevant supervisory authority within 72 hours.

Finally, to remain effective, any incident response plan must be regularly tested and be subject to continual refinement based on the outcomes of each test. Again, sharing intelligence with other higher education institutions can assist in the development of such plans.

Contents

5. Executive leadership

Executive leadership is a regularly cited challenge for organisations attempting to build a comprehensive cybersecurity programme. Overall executive leadership is critical to developing and implementing a comprehensive cybersecurity strategy, but all too often, security is perceived as a technical problem and is quickly delegated to the IT department.

This means that executive leadership teams often provide only limited guidance to IT departments in the development of critical business applications. This lack of support can result in IT having only a partial understanding of the risks that need managing, resulting in a poorly applied set of controls. At worst, inadequate protection of the most sensitive assets can result in increased levels of risk.

It is critical, therefore, that executive teams clearly understand the impact of a cybersecurity breach, including loss of confidentiality, integrity, and availability of important research data, leading to damage to brand and reputation. Furthermore, due to the nature of higher education, it is important for non-IT stakeholders to be able to communicate their needs and the likely consequences should any data they are responsible for be breached.

To support executive understanding, IT teams need to improve their ability to communicate the implications of risk in a non-technical way and seek strong business guidance to prioritise investment.

Contents

Adopting an architectural approach to security

We have identified five important security considerations for higher education organisations. While each one can, of course, be addressed in isolation, the most reliable approach is to view all your security needs as part of one complete system.

Taking an architectural approach means treating security as an end-to-end system, rather than a distinct set of individual components. This overall structure should be easier to manage as well as being capable of sharing vital contextual and threat information to deliver a more responsive and effective outcome.

Guiding principles:

1. A policy shift is needed that considers security to be an enabler.
2. Institutions must accept that it is no longer a question of if but of when a security breach will occur.
3. Security controls must transcend the traditional ‘block’ approach taken and instead focus on improving detection and remediation times.
4. Security should be developed as a system. Distinct components should not operate in isolation; rather they should integrate to provide more accurate threat detection and reduce management complexity.

Why an architectural approach?

An architectural approach is fundamentally driven by the needs of the business. By first identifying the information assets and systems that support the business, an assessment can be performed to determine the relative impact should a compromise occur.

Compromise can take place across all three aspects of information security: confidentiality, integrity, and availability. This is an important shift, given that all too often emphasis is placed on the loss of confidentiality, when in fact a loss of availability or integrity can have a far greater impact.

Once the assets are understood and the impacts analysed, it is important to consider the threat. We have identified five areas for consideration here, but these are not exclusive, and further areas need to be determined at a local level, with equal focus applied to both internal and external threats.

As with any architectural approach, understanding the business context will help organisations understand the capabilities their technology needs to deliver, which in turn will improve the user experience. Security should therefore be considered systematically, moving away from point solutions that plug holes as they appear. Security controls then become transparent to the end user and prevent the need to bypass a control that appears overly restrictive from a workflow perspective.

In other words, security is an enabler for the business.

How can Cisco help?

Cisco's extensive security capability means we are uniquely positioned to meet your security requirements as an integral part of the network fabric, or through dedicated physical and virtual security appliances.

When developing a robust security architecture, it is helpful to think of a cyber attack as a continuum containing three main phases. Cisco has developed the simple mnemonic BDA, which represents the phases of before, during, and after an attack.

Before

This is the phase where most security investment takes place and includes the deployment of defensive capabilities such as firewalls and anti-malware. It is vital to understand that defensive controls, while important, will be breached, and so investment should be spread more evenly across the remaining phases.

During

Controls deployed in this phase focus on improved visibility, so that an attack can be rapidly identified and mitigated. Network segmentation also helps manage an attack in the 'during' phase. When implemented effectively, it can contain an attack to a limited subset of the network and IT estate.

After

The final phase is concerned with rapid remediation. It also includes forensic controls that can help identify how an attack occurred and which systems may have been affected.

When following the BDA model, it is important to deploy capabilities that span the entire attack continuum, focusing not only on defensive technologies, but also on essential elements that support rapid identification, containment, and remediation of a threat.

As the network represents the fabric of interconnectivity, it is uniquely positioned to deliver the increased visibility and control required to support rapid threat identification and containment. Technologies such as Cisco® NetFlow – a capability built into most Cisco network devices – provides real-time network telemetry, revealing who is talking to whom, over what protocol, and for how long. Through careful analysis of this telemetry, unusual patterns of activity can quickly be identified and investigated. Such patterns include excessive one-way data transfer, which could be evidence of data being stolen, or data being transmitted between internal systems and Internet-based machines that are located in suspicious places.

Contents

Segmentation

Segmentation is another important capability that is delivered by the network. Its importance is always increasing, especially in light of the need to connect a wider range of devices and user communities to a common network infrastructure. Segmentation has however, remained challenging, with many environments still relying on static segmentation, based simply upon physical location. Furthermore, the segmentation that is in place is not always used to enforce security controls, meaning that traffic is allowed to flow freely across the entire network.

Importantly, each distinct component is able to operate in conjunction with others, forming a tightly integrated security system that can share threat and context data. The overall result is a system that is more responsive to threat and is able to quickly identify issues as they emerge, allowing for rapid remediation and recovery. It also allows the organisation to operate unimpeded.

A top-down approach to security

Addressing the challenges covered in this paper requires a top-down approach to developing a cybersecurity strategy. Cisco Security Advisory services can support higher education organisations in achieving this goal by:

- Identifying organisational risks, based on analysis of the information and business impact if breach or loss were to occur
- Performing a gap analysis to identify areas of weakness between the required level of control versus the current state
- Highlighting strategic areas for security investment across the organisational, policy, and technology domains to support the secure delivery of front-line services

Digital technology has the potential to have a truly profound and highly beneficial impact on higher education. However, this ever-increasing reliance on technology requires a comprehensive security architecture that is driven from the top down.

Cisco is uniquely placed to support higher education providers as they develop this vital capability. Contact us to find out how.

Cisco TrustSec® encompasses a range of capabilities that enable software-defined network segmentation. This is the ability to dynamically apply a segmentation policy as a user or device connects to the network, either wired or wirelessly.

Cisco TrustSec can capture details about the connected endpoint to inform policy decision making. These details can range from simple user identifiers to device types, installed software and compliance with software policies (such as whether the device has the latest patches installed). By gathering this

Contents

information, the system is able to make an informed decision and enforce a predefined security policy, helping ensure that the device is given the access it needs and no more. For example, this information could be used to enforce dynamic segmentation between different research projects where a high degree of control is required over distinct sets of research data.

Security innovation

Cisco NetFlow and TrustSec represent just two of the many innovations that Cisco has developed to embed security into the fabric of the network. The Cisco portfolio also includes a full suite of capabilities, ranging from perimeter access control and intrusion prevention to advanced network and endpoint anti-malware solutions and context data. The overall result is a system that is more responsive to threat and is able to quickly identify issues as they emerge, allowing for rapid remediation and recovery and helping ensure that the organisation is able to operate unimpeded.

Contact us

Cisco has a dedicated team supporting our UK education customers. The team's extensive industry knowledge means that they can identify the right Cisco solution for your needs.

Contact us for further information.

Authors

Mike Badham
Senior Solutions Architect – UK Health and Local Government, 020 8824 4138

Mark Jackson
Principal Information Assurance Architect – UK Public Sector, 020 8824 8535

cisco.co.uk/education