

CYBERSECURING THE COLLEGE CAMPUS

Digital Threats and Countermeasures for
Institutions of Higher Education



Contents

Executive Summary	3
The Digitisation of Educational Institutions	4
The Evolution of Cyberthreats Against Colleges.....	4
Why Colleges Across the World Suffer Cyberattacks	5
Motive	5
Means	5
What a Digitised Campus Looks Like – Processes, Activities, and Threats	6
Cost Imposed by a Successful Cyberattack	9
Direct Financial Costs	9
Indirect Financial Costs	9
Financial Penalties under the Proposed Personal Data Protection Act.....	9
Types of Cyberattacks against Colleges.....	10
External Threats	10
Phishing.....	10
Ransomware.....	11
Denial of Service.....	11
Business Email Compromise (BEC).....	12
Website Defacement	12
Internal Threats	13
Cybersecuring the Campus.....	14
Defining the Attack Surface	14
Digital.....	15
Online	15
Human.....	15
Physical	15
Policy Initiatives	16
Roles & Responsibilities	16
Permitted Use.....	16
Standards	17
Lifecycle Management	17
Penalties	17
Technology Solutions.....	17
Endpoint Security	17
Network Security	18
Encryption	18
Redundancy	19
Training and Awareness	19
Planning for the Future	20
K7 Security’s Solutions for Educational Institutions	21



Executive Summary

College campuses are open environments where a wide variety of stakeholders, devices, applications, and even networks intersect to achieve the goal of excellence in higher education. Digitising the institution unlocks productivity and enhances collaboration by allowing users to communicate using technology they are already familiar with in their personal lives. It also enables a transition from a classroom-centric to student-centric model of education.

This rosy digital picture does have its share of cyber thorns. Digital transformation of academia has been accompanied by an increase in cyberattacks against colleges across the world, with severe consequences. The UK alone reports **12 DDoS attacks per week** against colleges; a targeted campaign by threat actors stole over **\$3 billion in intellectual property** from 300 universities; a university paid over **\$1 million as a ransom** to attackers to recover access to its data.

The threats range from website defacement to ransomware and regrettably, threat actors can be found within the institution as well as outside. A digital campus will therefore also need to be a cybersecure campus if it is to maintain its academic reputation and avoid the often significant direct and indirect costs associated with a cyberattack.

This whitepaper from K7 Security has been prepared based on our experience working with and securing many institutions of higher learning, and examines

- Why colleges are frequently targeted by threat actors
- The direct and indirect costs imposed by a cyberattack
- The types of cyberthreats faced by colleges
- Internal and external threat actors
- The measures required to cybersecure your campus

We also discuss the human factor in maintaining cybersecurity and the training required to enable individuals to thwart cyber assaults. We conclude by exploring the preparation required for a future where digitally enabled adversarial actions are only like to increase in frequency and sophistication as colleges don a fully digital avatar.



The Digitisation of Educational Institutions

Paper has long held sway in the halls of educational institutions. From writing on them to publishing them, colleges have been synonymous with paper in its various forms over time. The proliferation of computers and the internet have released colleges from the monopoly of paper, but the dream of completely digital education has not yet been realised. Unfortunately even partial, or initial, digitisation opens the doors to cyberattacks. Before we examine cyberthreats and cyber defence in education, let us first understand how cyberattacks against educational institutions have evolved.

The Evolution of Cyberthreats Against Colleges

Hacking attacks against educational institutions are hardly anything new – the earliest known case may be from 1963, [when hackers tied up the tie-lines between Harvard and MIT](#).

21st century attacks reflect the type of technology that is available and used by colleges. Princeton University's head of admissions was [suspended in 2002 for hacking into a Yale University website](#), possibly due to the intense competition between the institutions for talented students. The incident prompted Yale to require secure passwords for access.

Cyberthreats can also emerge from current and former staff. A former librarian of the University of Hawaii [stole the personal information of 150,000](#) students, staff, and library patrons in 2005 to obtain loans fraudulently.

[Over \\$3 billion in intellectual property](#) was stolen from 300 universities across 22 countries over a period of 3 years from 2016. The campaign targeted more than 100,000 professors, often through spear phishing attacks.

Students can also launch highly destructive cyberattacks against their institution. [Rutgers University lost \\$3.5-9.5 million](#) due to a series of attacks by a student from 2014 to 2016 that [shut down parts of its IT infrastructure](#), like its central authentication server and a portal for delivering assignments and assessments, for days at a time.

These attacks show how cyberthreats against colleges and universities have evolved over time, but they are not confined to history books. Let us look at a few recent attacks:

- Newcastle University reported that it was hit by a cyberattack that [will take weeks to fix](#)
- Northumbria University suffered a cyberattack which led to [exams being cancelled](#)
- Luminate Education Group, which has 29,000 students and 2,000 staff, [was hit by a cyberattack](#)
- Myerscough College was hit by a [denial of service attack](#) on the day that exam results were to be published that also affected online enrolment
- Blackbaud, the world's largest provider of education administration, fundraising, and financial management software, suffered a ransomware attack and data breach that led to theft of data belonging to University of Birmingham, De Montfort University, University of Strathclyde, University of Exeter, University of York, Oxford Brookes University, Loughborough University, University of Leeds, University of London, University of Reading, and [many others](#)

What is most alarming about these reports is not just that there are so many of them; all of them were reported by the BBC from July to September 2020 for the United Kingdom. Universities and colleges from just one country suffered this many attacks (and perhaps many others other as well) over just 3 months.

We can see that the scale and sophistication of cyberattacks increase as time progresses and both society and colleges become increasingly IT enabled. Let us examine why colleges are frequently targeted by threat actors.





Why Colleges Across the World Suffer Cyberattacks

Any cyberattack, or any crime for the matter, occurs due to the intersection of means and motive.

Motive

While motives do vary, cyberattacks against colleges are largely driven by just one word: data. We repeatedly hear that data is the new gold, and educational institutions have a lot of this digital gold. The types of data that colleges have include

- Personal data of staff and students
- Academic records of staff and students
- Financial information of the institution and many stakeholders, including parents
- Medical information, such as blood group, disabilities, and allergies
- Research data
- Intellectual property

Cyberattackers can monetise the stolen data directly, by demanding a ransom or selling the data on the dark web; or indirectly, through identity theft.

The success of attacks like ransomware depends on the likelihood of the victim paying the ransom. Colleges provide a critical service and are perceived as more likely to pay the ransom, providing additional motive for a cyberattack. This perception is partly justified by some of the large ransoms that colleges have paid, which we will see later in this whitepaper.

Means

Colleges can appear to be easy targets for cyberattacks for several reasons:

- **Large IT Ecosystem** – The number of users, departments with specific needs, external stakeholder interaction, and variety of devices increase the attack surface, making it relatively easy for an attacker to find a point of entry
- **Open Environment** – The greater need for collaboration between students and staff, as well as amongst students and amongst staff, and the large number of personal devices that are used on campus, provide more opportunities for hackers to launch an attack
- **Curious Students** – Young students are keen to see what they can do with the tools at their disposal and may lack perspective on consequences, which can open the doors to cyberattacks

Now that we have understood the means and motives that drive cyberattacks against colleges, we can explore the process and activities in a digital campus and how these create opportunities for cyberthreats.





What a Digitised Campus Looks Like – Processes, Activities, and Threats

Many colleges aim for eventual completely-digital student lifecycle management. From initial enquiry to becoming an alumni member, the student and the organisation will be digitally enabled. This includes various processes and activities which have the potential to introduce vulnerabilities. Both external and internal threat actors may exploit these threat opportunities.

Process	Digital Activity	Potential Digital Threat
Enquiry	The student's initial email, call, or approach to an admission desk are all logged in a relationship management system	• Disruption/blocking of incoming enquiries • Manipulation/deletion of incoming enquiries • Leak of incoming enquiries to rival institutions
Admission	Documents are scanned and uploaded to the college's server, or digital documents are provided, for scrutiny. The admission process is completed and the outcome is communicated virtually	• Document deletion/substitution • Manipulation of verification status • Manipulation of admission status • Manipulation of automated communication to candidate
Fees	College fees to be paid for various academic activities are calculated and communicated to students. Online payment is received and reconciled against amount due and purpose of payment	• Manipulation of fee calculation • Disruption of communication to students • Allocation of fee received to wrong student/purpose • Manipulation of payment due status • Manipulation of reconciliations
Course/Class Allocation	Faculty and seat availability for courses (including optional classes and distance education) are automatically estimated. Communication to students on course availability is automated and confirmation of acceptance is digitally recorded and processed	• Manipulation of human, financial, and physical resource availability estimation • Disruption in student communication
Class Schedule	Student timetables and classroom allocations are automated and communicated to students	• Chaotic/contradictory time and classroom scheduling • Manipulation of attendance records • Disruption in student communication



Process	Digital Activity	Potential Digital Threat
Academic Results	Students' academic performance is digitally calculated, recorded, and published	• Manipulation of academic results, including backup of past results • Destruction of academic results, including backup of past results • Manipulation of communication of results to students
Internship Coordination	The entire internship programme, from interaction with participating employers to internship status and performance, is processed and stored digitally	• Blocking communication of interest to/from prospective/enrolled programme partners • Manipulating communication of internship availability to students • Manipulation of internship status and results
International Collaboration	Nurturing relationships, communication, coordination, and cooperation in joint research and student exchange programmes are digitally enabled	• Hoax enquiries to and even from the college • Souring relationships by blocking/altering communication • Disruption in collaboration and cooperation
Research Activities	Authorisation, funding, collaboration, and recording, registration, and monetisation of Intellectual Property (IP) are accomplished through digital processes	• Manipulation of research subjects and results • Manipulation and theft of funds • Destruction/theft of IP
Alumni Relationships	Digital facilitation of requests for transcripts, certificates, and communication for events and fundraisers	• Manipulation of records • Insertion of fake records • Fake requests for documents leading to identity theft • Fund siphoning through fake fundraisers
Human Resources Management	Recruitment and other human resource development measures are initiated and implemented through digital channels	• Manipulation of salary records • Manipulation of payment records • Deletion/manipulation of staff service history/academic qualifications • Manipulation of credential verification status • Fake staff on payroll



Process	Digital Activity	Potential Digital Threat
Administration/ Financial Management	Non-academic activities related to management of day-to-operations and relationships with vendors and other external stakeholders are handled through digital platforms	• Fake invoice submission • Vendor's poor cybersecurity operates as backdoor to the institution • Falsification of payment records to vendors
Hostel/Kitchen Management	Estimation and communication of availability and allocation of rooms, and capacity planning for the kitchen are automated	• Manipulation of room availability and allocation • Manipulation of hostel security/attendance records • Misappropriation of kitchen funds • Manipulation of patronage/utilisation records
Library Management	Purchasing, cataloguing, and lending of books (including digital books) are digitally enabled along with tracking, fines, and book requests	• Blocking book availability • Pilfering books by erasing catalogue, lending records • Resetting fines
Transport Management	Maintenance, fuel, payroll, scheduling, route management, tracking, communication, and capacity planning are automated and simplified through digitally integrated processes	• Fake invoices • Vehicle diversion for non-official use • Unauthorised destination modification • Student endangerment through route alteration • Manipulation of utilisation records
Marketing Automation	Outbound communication, including social media outreach, and response/action requests are automated	• Distribution of malicious/defamatory content • Suppression of timely response

No institution may have completely digitised all these processes, but many colleges are at different stages of progress towards this goal. This necessarily also means that colleges are at different stages of potential vulnerability to the listed digital threats. The large number of colleges around the world indicates that cyberattackers have many targets to choose from, and each may offer a number of vulnerabilities to exploit. An attack that works on one college may work on another with little to no modification, giving threat actors further incentive to devote their energies towards compromising institutions of higher learning.



Cost Imposed by a Successful Cyberattack

Any, and every, cyberattack on a college imposes a cost on the institution. We have seen the different types of threats that a college may face. These vulnerabilities may result in financial losses that may be broadly classified as direct and indirect financial costs.

Direct Financial Costs

Direct financial costs involve a (usually) immediate outflow of funds that can be directly attributed to the malicious activity. Affected costs include

- **Operating Costs** – False invoices, fake staff on payroll, and similar fraudulent claims cause a recurring outflow of funds that impacts both profitability and liquidity
- **Capital Expenditure** – Capacity underestimation/underutilisation of assets will cause an increase in capital outflow to restore capacity/capability and thereby increase the cost of capital of the organisation
- **Opportunity Cost** – Misallocation of funds, destruction of IP, and other such criminal activity prevent resources from being used optimally/monetised, reducing return on investment on projects implemented
- **Replacement Cost** – Theft, even of a library book by catalogue manipulation or of automobile fuel through route manipulation, causes an inflation in overheads due to the cost of replacement

Indirect Financial Costs

The outflow in these cases may not be immediate, may not be directly attributable to the malicious activity, and may be a lost inflow rather than a direct outflow:

- **Reputation Loss** – Destruction of academic results, student endangerment, document manipulation, and the spread of malicious/defamatory content through official channels can harm the college's reputation. This cost can be very difficult to quantify, but it is significant and can affect the very existence of the institution
- **Revenue Loss** – Blocks/leaks of student and partnership enquiries can result in missed opportunities with consequent impact on top-line growth
- **Compensation** – Destruction of documents/academic results, student endangerment, and defamatory content may require payment of compensation or reimbursement of affected parties in case of litigation or to avoid further reputation loss
- **Penalties** – Penalties are imposed on colleges by various regulators and even the courts. Data held by the college can be manipulated by a threat actor to make the college liable for penalties

Financial Penalties under the Proposed Personal Data Protection Act

India's proposed Personal Data Protection Act may significantly increase a college's responsibility to maintain data securely. Penalties under this act can be severe – [up to Rs. 15 crores or 4% of total worldwide turnover](#) (whichever is higher) for the previous financial year and the affected party can also seek compensation.

The act has been introduced but not passed, so we do not yet have instances of colleges being fined under this act. However, the experience of educational institutions in countries with similar protective legislation demonstrates that harsh penalties can and will be levied: the [University of Greenwich was fined £120,000](#) in 2018 due to an inadequately secured microsite that was developed for a training conference held in 2004.

It is clear that colleges can incur significant and varied costs due to cyberthreats, and have many avenues through which an attack can be launched. It is also clear that the consequences of poor cybersecurity can manifest years after the original security lapse occurred. Therefore a highly proactive and prudent cybersecurity posture is recommended for institutions of higher learning, which we will discuss after taking a closer look at common cyberattacks against colleges that we will need to defend against.



Types of Cyberattacks against Colleges

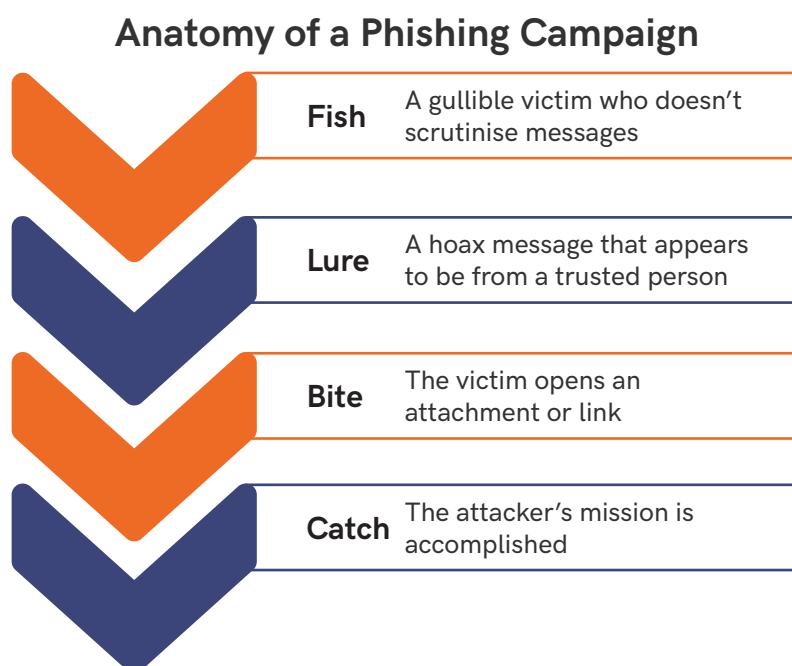
We have already discussed the various digital threats which colleges face. We will now discuss specific attacks/malware that are used to target colleges.

External Threats

These are some of the attacks favoured by threat actors external to the organisation. 'External' in this context is defined as those who do not have authorised access to the organisation's IT assets.

Phishing

Phishing is a form of social engineering where the victim is misled into performing an action that is prejudicial to their or their organisation's best interests, such as providing access to unauthorised users, altering records, sharing confidential information, or approving fraudulent transactions.



Phishing can be used for different types of campaigns. The protected health information of [over 9,500 patients was exposed](#) by a spear phishing attack (a phishing variant that targets specific individuals) at the Medical College of Wisconsin. Threat actors also launched a phishing campaign that [sent fake invoices](#) to students of Lancaster University.

We have already discussed a campaign against 300 universities across 22 countries where many professors were targeted through spear phishing attacks. [Emails were sent with seemingly authentic links](#) that made the professors believe they had logged out of their university accounts. The fake login pages then stole their credentials when they tried to log back in.

Phishing is a particularly dangerous type of cyberattack because it targets the user and not the device and it may originate outside the organisation e.g., social media may be used to contact the victim and earn their trust. It is therefore difficult to defend against as the victim may override security warnings because they trust the attacker. It is estimated that [91% of all attacks begin with phishing](#). Phishing can be used to deliver different types of malware, such as keyloggers and ransomware. Many of the threats that we described in our discussion on digital campuses are likely to be implemented through a phishing campaign when carried out by an external threat actor.



Ransomware

Ransomware offers an easy way for attackers to monetise their attacks, which makes it very popular with threat actors

Anatomy of a Ransomware Attack

Entry	Encrypt	Demand	Payoff
Ransomware enters the network typically through USB, email, or software exploit	Data on devices is encrypted, preventing access	Ransom is demanded to restore access, usually in untraceable cryptocurrency	Victim pays hacker the ransom and may receive decryption key if lucky

Colleges and universities are highly data dependent and cannot function without access to data, which makes them more likely to pay. Ransomware perpetrators are now also threatening to release the data to the public if a ransom isn't paid, forcing victims to pay to avoid data exposure even if they have data backups to counter the malicious encryption. A few examples of ransomware attacks on the academic world in 2020:



Institution	Ransomware	Ransom Paid
University of California, San Francisco	Netwalker	\$1,140,000
University of Utah	Unconfirmed (likely to be Netwalker)	\$457,059
Maastricht University	Clop	€220,000

The very large amounts of ransom that are being paid show how dangerous and effective these attacks are. Ransomware gangs need not always demand the ransom from the institution. In an unusual twist, students of Oberlin College, Grinnell College, and Hamilton College [received ransom demands of \\$3,800 each](#), later lowered to \$60, to retrieve their admission files after the colleges' admission data was encrypted by ransomware.

Ransomware creators have now joined the SaaS world and provide Ransomware-as-a-Service (RaaS) that allow criminals with limited technical knowledge to launch sophisticated attacks. RaaS offerings mimic legitimate SaaS offerings and even offer convenient dashboards to monitor attacks, and are advertised on the dark web much like legal software is advertised on the surface web. This indicates that the ransomware threat is going to increase as the number of attacks and attackers will keep growing.

Denial of Service

Denial of Service (DoS) or Distributed Denial of Service (DDoS) attacks are likely to be carried out to cause disruption by blocking access to the institution's IT assets. The motives are wide ranging and can include revenge, damage to reputation, causing an increase in costs, gathering information for another attack, and distracting attention from a security breach.



Anatomy of a Denial of Service Attack

Mobilise	Deploy	Profit
Recruit a single machine (DoS) or an entire botnet (DDoS)	Cause performance degradation or crash by flooding target device/network with traffic	Disruption which may be followed by extortion

Denial of Service attacks are relatively easy to launch as they can be bought for just [\\$10 per hour or \\$60 for 24 hours](#). The UK alone reports [12 DDoS attacks per week](#) against colleges, which indicates the frequency with which such attacks are launched against educational institutions.

Business Email Compromise (BEC)

A variant of phishing that particularly targets business email accounts to increase the appearance of authenticity, this attack can be used for direct monetary gain through misappropriation of funds or to cause reputation damage as described in our discussion on digital campuses.

Anatomy of Business Email Compromise

Survey	Cultivate	Harvest
Find a victim who is careless with email security	Gain the trust of the victim	Mislead the victim into transferring funds or performing other harmful actions

Being careless with email security is, unfortunately, a very common issue. [Poor passwords](#) and sharing information used for security questions on social media (e.g., mother's maiden name, name of pet) make it easy for threat actors to compromise email credentials. Malware, like keyloggers, can also be used to steal credentials. Once an email account is compromised, it can be used to send fund transfer requests. This makes BEC more difficult to identify as an attack as, unlike other forms of phishing, the sender's email address is genuine and it is only the message it contains that is fraudulent.

A BEC attack need not originate from within your organisation. A vendor's email may be compromised and used to send fake invoices to be paid to the attacker's account. This implies that cybersecurity cannot be limited to your organisation and should include external stakeholders.

While the term Business Email Compromise places the emphasis on email, the way large organisations communicate and collaborate is fast evolving and we should extend our diligence against such attacks to other communication contexts as well, such as social media messages or WhatsApp groups which can also have imposters disseminating malicious messages while masquerading as genuine members.



Website Defacement

Website defacement attacks are on the rise because they are relatively easy to accomplish and can have a large impact due to a college's website having both high external traffic and captive internal audience. The primary motives for such attacks are reputation loss, propaganda, and distribution of malicious code.



Identify	Compromise	Score
Scan for websites with vulnerabilities	Exploit vulnerability to takeover website	Display messages or implement drive-by malware download

There are a wide range of vulnerabilities that an attacker can exploit, such as open ports, unpatched servers, non-validated inputs, and non-escaped data. Note that a defaced website may not appear as defaced to your organisation – only website visitors may be impacted, delaying your organisation's incident detection and response. Defacement is also a wide term and may not include obvious defacement, such as posting messages on your website, and may extend to other malicious activities such as requesting access to a user's webcam through your website to make the request seem credible.

Website hacks, across education and other sectors, are quite common. The websites of Aligarh Muslim University, Army Institute of Management and Technology Greater Noida, Army Institute of Management Kolkata, Defence Institute of Advanced Technology, Delhi University, IIT (Delhi), IIT (Varanasi), and University of Kota [were all defaced on the same day](#). We can expect various forms of website defacement to increase as more educational services and processes become web enabled.

Internal Threats

An internal threat actor is anyone who is an insider to your organisation i.e., students, faculty, administrative and management staff, vendors, consultants, etc., who abuses their legitimate access to and knowledge of your organisation's data and systems to perform actions that are prejudicial to the interests of your organisation or to the interest of other stakeholders in your organisation.

Any of the threats listed in the initial discussion on digital campuses or examined under external threats can be executed with relative ease by insiders. It is not the types of attacks but the opportunity and conflict of interest that differentiate external and internal threat actors. An analysis of cybersecurity incidents discovered a pattern of attacks that strongly suggested that [attacks on 190 colleges and universities](#), especially denial-of-service attacks, were caused by insiders. The motivation behind an attack need not have anything to do with the institution; in one instance, an attack was launched by a student to gain an advantage over another student in an online game.

Internal threats are more difficult to counter than external threats because

- The attacker is inside the organisation and cannot be stopped by perimeter defences
- The attacker has legitimate access to internal IT resources and cannot be stopped by credential checks
- The attacker may be very familiar with the computing ecosystem in your organisation, including its weaknesses

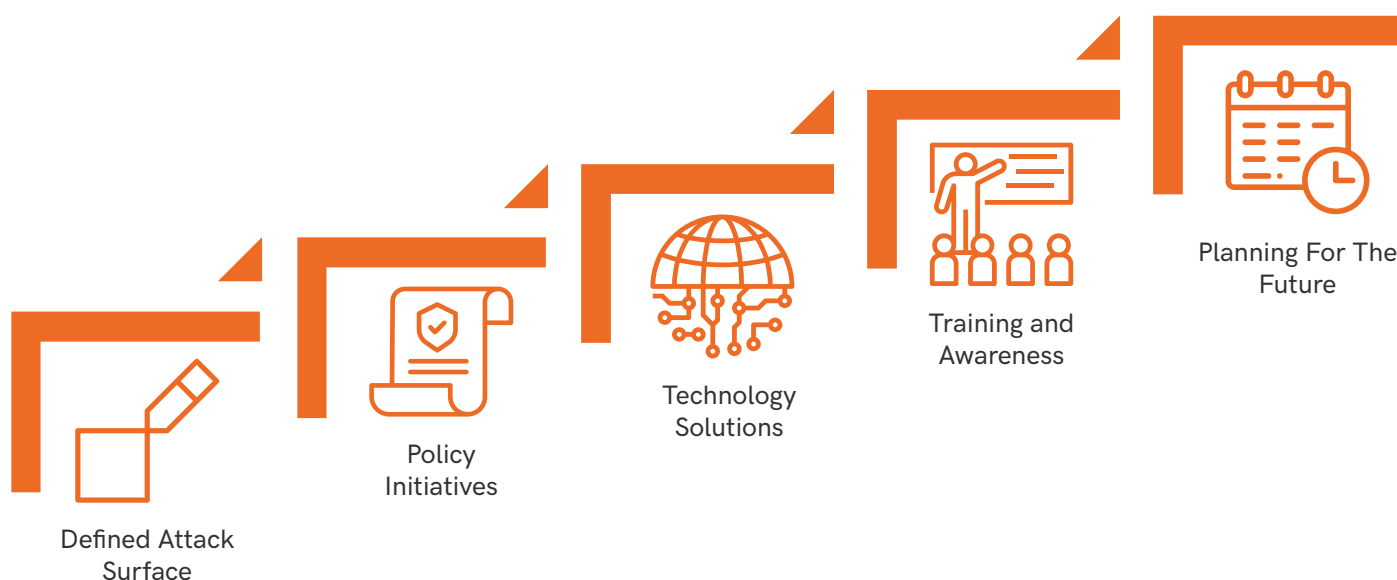
Now that we have understood how and why colleges are under increasing risk of cyberattack, we will examine the cyber defences that can be deployed to protect the institution.





Cybersecuring the Campus

Like all large and complex organisations, a college campus cannot be made cybersecure with just one tweak or solution. It requires a multi-pronged strategy, and different layers working in tandem, to mount an effective cyber defence against the threats of today and tomorrow.



Defining the Attack Surface

Your organisation's attack surface is made up of all the potential entry points that a threat actor could use to launch a successful cyberattack, such as the potential threats discussed at the beginning of this whitepaper. Even a single weak password (which indicates that the system allows weak passwords to be used) is a potential point of entry for an attacker. The attack surface can be assessed and defined using

- Security Audit
- Vulnerability Assessment
- Penetration Testing

The findings from these security evaluations must be analysed and any defects found must be rectified. Modern day cybersecurity has multiple facets and all of them must be evaluated to define the attack surface.

Digital	Online
 Applications, devices, networks, and data	 Web assets including apps and social media
Human	Physical
 Social engineering attack vectors	 Physical security of digital assets



Digital

- **Applications** – All applications used and their currently installed versions should be listed. Shadow IT (use of unauthorised applications and services) should also be documented
- **Devices** – All devices that form the IT ecosystem should be listed along with their security/patch update status. This includes personal devices of stakeholders that are used to access college digital resources, devices used in experiments/pilot projects such as IoT devices or research equipment, and devices that are leased or form part of a subscription service
- **Networks** – All networks in the college should be documented along with their security controls. Open ports should be identified. Network segmentation (or its absence) should also be noted
- **Data** – How data is stored and secured, along with backup policies should be noted. Who has access to which data, and how easy it is to gain access to data, should also be documented

Online

- **Website** – The college's website security should be evaluated including vulnerability to Cross-site Scripting (XSS) and SQL Injection, as well as vulnerabilities present in the Content Management System (CMS). The process to ensure that the domain name registration is renewed ahead of time should be verified (a lapsed domain name can be registered by an attacker to divert your audience to their website)
- **Mobile Apps** – The security status of any mobile apps developed by the college, including apps that may be listed on app stores but are not used/updated anymore, should be verified
- **Fake Websites/Apps** – A search should be performed to identify any unauthorised websites or apps that use the college's name, or even mimic the look and feel of the college's apps and website, to mislead users
- **Email** – The implementation of email security protocols, such as Domain Keys Identified Mail (DKIM), Domain-Based Message Authentication, Reports & Conformance (DMARC), and SPF (Sender Policy Framework) should be verified
- **Social Media** – A list of platforms on which the college is represented and security controls for each account should be prepared. A search for fake social media accounts in the name of the college should also be performed

Human

- **Social Engineering** – The potential for a social engineering attack (an attack that targets a user rather than a device) should be evaluated, and counter measures, such as enterprise anti-phishing protection and awareness training, should be assessed

Physical

- **Physical Security** – Physical access to a device can enable a successful cyberattack by allowing the attacker to use a mobile phone to photograph data on the device screen, or to steal the device to gain more time to compromise the device and extract data. Control over physical access to devices and networks should be recorded





Policy Initiatives

Every organisation needs a cybersecurity policy that lays down roles, responsibilities, standards, requirements, permitted use, and penalties. If your college does not have a cybersecurity policy, it is critical to create one as a reference document to be followed. If your college does have a cybersecurity policy, it should be updated to address any cybersecurity gaps discovered in the evaluation of the attack surface. Your cybersecurity policy should specifically address:

Roles & Responsibilities	Permitted Use	Standards	Lifecycle Management	Penalties
 Who does What and When, and who is responsible for enforcement	 How organisational IT assets may be used	 Cybersecurity standards such as password strength and encryption technologies	 Hardware, Software, and User lifecycle management	 Penalties for non-compliance

Roles & Responsibilities

Any form of access to the college's IT infrastructure has to be regulated. The cybersecurity policy should lay down guidelines for determining user roles and privileges and stipulate how such access is monitored. A maker-checker-approver system should be followed to prevent inappropriate access being granted and abuse of access legitimately obtained, to avoid many of the threats listed under the description of a digital campus.

The cybersecurity policy should also define a hierarchy of responsibilities at different organisational levels to ensure that the cybersecurity policy is enforced in day-to-day operations.

Permitted Use

We have previously discussed a cybersecurity incident caused by online gaming rivalry – but should your institution allow online gaming using campus resources? Your college's cybersecurity policy should provide guidelines on what your IT assets may be used for, how they may be used, and who may make use of specific privileges.

These will need to be carefully considered as senior faculty members and management may be allowed greater latitude due to their wider range of responsibilities while some departments, such as media studies, may need access to news and entertainment websites even for students. Depending on the purpose/seniority level, restrictions on use may be formulated as

- **Specifically Permitted** – Only specific use cases are allowed and other forms of use are not permitted. This is appropriate for most users
- **Specifically Excluded** – Everything is allowed except for some use that is not permitted. This is suitable for users at higher levels in the organisation's hierarchy

It should be noted here that permitted use may extend beyond IT asset access. Restrictions on hate speech, harassment, incitement, and other forms of hostile/offensive behaviour will need to apply to permitted use even if the malefactor does not target your organisation or any of its stakeholders as such conduct can still result in direct and indirect costs to your organisation. These restrictions on permitted use should also apply to those who manage your organisation's social media channels.



Standards

The policy should define the cybersecurity standards of the organisation. These can include password strength, multi-factor authentication, encryption technologies, cybersecurity requirements in procurement of hardware and software, audit intervals, and infrastructure segmentation. The [Assessing Security Requirements for Controlled Unclassified Information](#) document published by National Institutes of Standards and Technology (NIST) can be utilised as a starting point to determine the controls and safeguards appropriate for your institution.

Lifecycle Management

Every device, application, and user has a lifecycle in the context of your college that needs to be managed to ensure that entry, implementation, or access does not compromise cybersecurity. This should specifically include

- **Hardware Lifecycle Management** – This should ensure that the manufacturer’s commitment to providing frequent security updates is confirmed before procuring hardware; hardware deployment is recorded and monitored; lost/stolen devices can be retrieved or remotely wiped; and devices are sanitised before disposal. This university’s [hardware asset management statement](#) can provide a framework from which a similar statement can be prepared for your organisation
- **Software Lifecycle Management** – This should ensure that fragmentation is avoided by requiring different departments to use the same software for the same task, and all software is updated with the latest security patches available. This [university’s guide](#) can form the foundation for your college’s software lifecycle management policy
- **User Lifecycle Management** – This should ensure that cybersecurity is maintained from users’ onboarding to exit. Former employees’ data and network access privileges should be revoked immediately on exit and current employees should be granted access based on the [principle of least privilege](#)

Penalties

The cybersecurity policy will merely exist on paper unless there is a mechanism to enforce it and ensure compliance. This necessarily requires penalties both for non-compliance on the part of users and non-enforcement on the part of leaders. Your college can decide on appropriate penalties for your user-base based on the consequences that may result from non-compliance, but strict enforcement of penalties are essential to encourage compliance.

Technology Solutions

Endpoint Security

Every device that connects to your organisation’s network is an endpoint, and every endpoint has to be secured with a carrier-class cybersecurity solution like [K7 Endpoint Security \(K7 EPS\)](#). The solution should be easy to deploy and manage, support rapid rollout, and not impact device or network performance.

The endpoint security solution should include these features:

Device/Data Protection	Cybersecurity Management
• Malware Protection • Network Protection • Web Protection • Device Management & Control • Application Control	• Centralised and Remote Management • Hardware Asset Management • Group Based Administration • Security Incident Notifications • Cybersecurity Reports

It is imperative that every endpoint be secured. Even one unsecured endpoint can open the doors to a cyberattack that will spread from that endpoint to your entire organisation.



Network Security

Network security protects the perimeter of your organisation to prevent unauthorised access and activities from the external world. An in-depth examination of network security is beyond the scope of this whitepaper but your college's network should include basic security features including

- **Access Control** – This ensure that only authorised users are allowed to connect to your organisation's network and can connect only with the privileges assigned to them
- **Gateway Security** – Gateway security appliances, like [K7's Unified Threat Management](#) solutions, include a hardware firewall with Intrusion Detection System/Intrusion Prevention System (IDS/IPS), Denial-of-Service (DoS) attack protection, VPN, and inbound and outbound load balancing to protect your network
- **Segmentation** – Network segmentation effectively creates multiple internal networks. This hinders lateral movement of a cyberattack and reduces the possibility that a single compromised endpoint allocated to a minor task, or a guest being granted network access, can be used to launch an attack against the entire organisation

Network security requirements apply to both wired and wireless networks.

Encryption

Encryption of data is necessary to keep data secure even if it is stolen or intercepted. Data should be encrypted both at rest and in transit. Encryption should be applied wherever it can be applied, including

- **Devices** – Sensitive data stored on a device should be encrypted. This may require that the entire device, with all data stored on it, be encrypted
- **Storage** – Data storage, such as data backups, should be encrypted as a threat actor may try to compromise the data backup to extract confidential information. This means that even a USB storage device like a pen drive should be encrypted if it is used to backup, move, or share data
- **Cloud** – Data that is stored or shared using the cloud should be encrypted. This is especially important if your organisation, or any individual in your organisation, uses 3rd party cloud-based file sharing services where you don't have much, or any, control over how your data may be accessed or used by the cloud service provider or any of their employees
 - » Messenger services, and other communication tools, should also be considered cloud based data storage services in the context of institutional cybersecurity as they permit file sharing but they may not be secure. For instance, [WhatsApp data that is backed up on Google Drive isn't protected by encryption](#) which your organisation may need to consider when framing its communication policies
- **Website** – Your college's website should make use of HTTPS rather than HTTP to encrypt information that flows between the website's server and the user's browser to prevent the interception or hijacking of communication through Man-in-the-Middle (MitM) attacks

Determining whether data should be encrypted or not requires classification of data. Conducting a data classification exercise is worthwhile as it has [other benefits beyond enabling encryption](#), such as helping in creating access levels and compliance with data privacy legislation.





Redundancy

Redundancy is having a backup in the event of a failure in a device, network, or availability of key personnel with the ultimate goal of ensuring zero downtime. It improves resilience in the event of a cyberattack. Your organisation should consider having redundant resources for

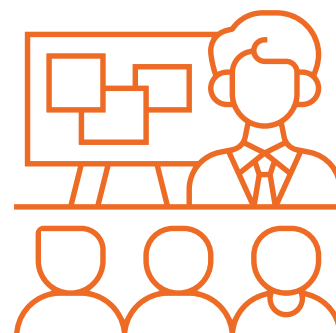
- **Computing** – Distributed computing uses a large number of small units (typically, applications running on computers) over a small number of large units. This ensures that a cyberattack on a single unit does not disrupt multiple services
- **Internet** – Provide connectivity from 2 different ISPs (Multi-WAN). They can operate in failover mode (secondary ISP is used only when primary fails) or in load balancing mode (data traffic is distributed across both ISPs simultaneously) to protect against a cyberattack that tries to disconnect you from the internet
- **People** – Any cybersecurity responsibility cannot lie in the hands of one person alone as a cyberattack can spread very quickly and backup personnel should be ready with the training and tools to act if primary personnel are not available

Training and Awareness

Technology solutions can stop attacks against devices, which is why threat actors create social engineering attacks that target the user instead. While technology can act as a secondary defence against some social engineering attacks like phishing, a well informed user remains the primary defence.

The extent of cybersecurity training required will vary across your organisation's hierarchy as roles, responsibilities, and access to sensitive resources expose users to different levels of risk. However, all staff should be trained on the fundamentals of cyber hygiene, including

- Creating strong passwords that are not reused or recycled
- Ensuring physical security of IT assets
- Identifying phishing attacks
- Verifying the bona fides of a message or sender
- Exercising caution before opening an attachment or clicking a link
- Precautions to be followed on mobile devices
- Essentials of network security for those who might need to work from home
- Whom to contact if a cyberattack is noticed



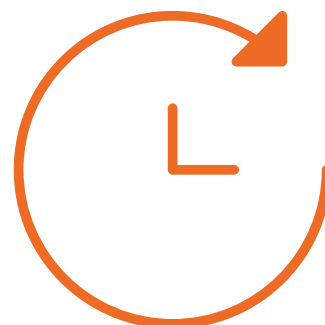
Creating a culture of cybersecurity in your organisation is necessary to prevent continuously evolving cyberattacks and therefore training should not be a one-time event. Cybersecurity tips and reminders should be frequently distributed to all stakeholders through notice boards, newsletters, and other internal communication channels. Cybersecurity refresher courses should also be conducted periodically to ensure that all users are aware of your organisation's cybersecurity policy, their responsibilities, and defensive measures against the latest cyberthreats.



Planning for the Future

The current state of digitisation in your campus will determine how many of the measures discussed in this whitepaper will be required in your organisation. Time and other constraints may also prevent you from implementing all the required measures. It is therefore prudent to frame a cybersecurity plan for your college that will sync with your digitisation schedule to ensure that all your digital assets are protected. This plan should cover

- **Upgrade/Replacement** – Obsolete IT assets (those that no longer receive security updates) should be upgraded or replaced. This requires identifying such assets and budgeting for their replacement cost
- **Procurement** – Cybersecurity should be a critical feature that your college requires in both hardware and software, and should be included in all your IT related tenders/RFPs. The vendor's credentials and reputation regarding cybersecurity and provision of security updates (during the entire lifetime of the product and not just at time of purchase) should be evaluated before a contract is signed or invoice approved
- **Training** – Identifying training requirements for specific roles and the means of implementing such training, either with internal resources or through external experts, is required to maximise the returns on your cybersecurity investments
- **Staffing** – Many colleges do not have in-house cybersecurity talent which affects their ability to prepare for, and speed of response to, a security incident. Including cybersecurity qualifications as a requirement when recruiting IT staff will address this talent deficit and reduce response lag
- **Processes** – Cybersecurity by design should be your guide when introducing a new academic, administrative, or financial process that has a digital component, or revamping an existing one. Processes should be designed to
 - » Reduce the attack surface
 - » Avoid identified risks
 - » Have cybersecurity as a default rather than an additional layer
 - » Give priority to cybersecurity issues
- **Compliance** – Regulations that may not apply to your organisation now may apply to you in future. Therefore, analyse draft legislation (such as India's [proposed Personal Data Protection Act](#)) and international security/privacy legislation which is likely to impact partnerships with foreign universities, and plan to introduce compliance with such regulations before they are made mandatory
- **Response** – Regard cybersecurity incidents as inevitable, and frame your technological, marketing, financial, and legal response to a successful cyberattack to reduce your response time and mitigate the impact of the attack. This should include adding disclaimers/liability limitations to any contracts you sign or terms and conditions attached to your college's services



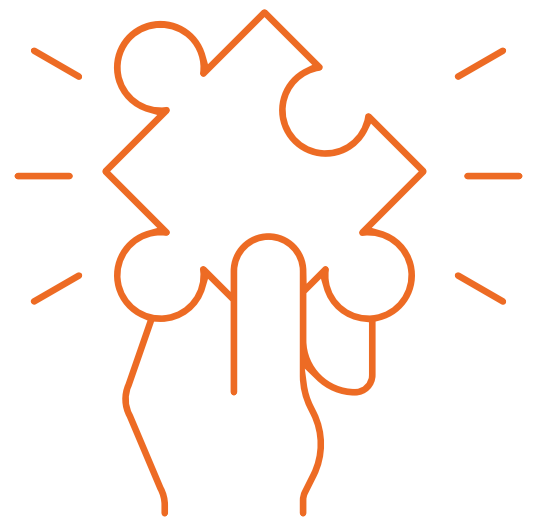


K7 Security's Solutions for Educational Institutions

K7 Security combines over 28 years' expertise in cybersecurity with a state-of-the-art threat research lab to deliver rapidly updated enterprise cybersecurity solutions that protect critical data and devices in many educational institutions across the world.

- **Endpoint Security** – Our Endpoint Security utilises multi-layered protection, heuristic malware detection, ransomware protection, and a dedicated firewall to help defend the growing number of connected devices within organisations against cyberattacks
- **Network Security** – Our Unified Threat Management, VPN Concentrator, and SD-WAN devices provide enhanced network security and secure connectivity between branch offices, headquarters, and the cloud

Our solutions are recognised across the world for 24x7 enterprise cyber protection. K7 Endpoint Security emerged as the winner against major international cybersecurity brands in the Performance Test conducted by AV-Comparatives (Austria).



Copyright © 2021 K7 Computing Private Limited, All Rights Reserved.

This work may not be sold, transferred, adapted, abridged, copied or reproduced in whole or in part in any manner or form or any media without the express prior written consent of authorised personnel of K7 Computing Private Limited. All product names and company names and logos mentioned herein are the trademarks or registered trademarks of their respective owners.

www.k7computing.com

