Mitigate Information Security Threats
Safeguard Your Campus with 10 Best Practices to Combat Common Cybersecurity Vulnerabilities
Information security has always been a higher education concern, but it is now cited as the number one issue for higher education leaders. High-profile data breaches and cyber threats are forcing institutions to increase their focus on information security. Nearly 10 percent of security breaches in the U.S. target education institutions.

The job of ensuring information is secure on campus is challenging. IT teams must meet student, faculty, and staff demands for greater access to resources on a growing number of devices coming to and available on campuses while simultaneously protecting identities and networks from intrusion. Moreover, increased collaboration between academic institutions and corporate partners requires strengthening intellectual property protection and limiting extortion opportunities such as ransomware. Personalized learning, virtual labs, and online courses further complicate data stewardship strategies.

Academic institutions striving to prevent on-campus incidents of malicious and unintended data theft, as well as stop hackers worldwide interested in exposing major vulnerabilities on a large scale are looking to their IT teams to invest in approaches that more effectively counter digital attacks and cybercrimes. What is your institution doing to protect its reputation and combat the complex and evolving state of information security threats in education?

Bull’s-Eye on Education

Academic institutions are increasingly falling victim to cyberattacks for a variety of reasons:

- **Sensitive data is attractive** – Colleges and universities are city microcosms, containing virtually everything anyone might want to know about someone including academic performance, health details, financial status, patents pending, and more. Often large amounts of personally identifiable information (PII) including social security numbers, birth names with dates and addresses are stored in a single repository. Additionally, high-value and sensitive intellectual property and research is often sought after by outside, malicious parties. Unauthorized access to this information can have serious negative impacts.

- **Opportunity is great for success** – Large numbers of end users accessing websites and personal accounts through campus IT systems increase attackers’ odds. There is potential for breach every time a user logs in. Institutions also teach advanced computer science classes which include development skills that may be used improperly. Flat budgets and lack of cybersecurity expertise can increase intrusion success rates.

- **Response is slow** – Overextended and siloed IT staff makes it difficult for academic institutions to quickly remediate issues within the complex and diverse environments they manage—even when it comes to known vulnerabilities and attacks—opening the door to reoccurrence.

This e-book examines ways academic institutions can safeguard against the 10 most common cybersecurity vulnerabilities while improving security postures, processes, and technologies.
10 Security Best Practices

There is no quick fix when it comes to safeguarding all data—and it’s impossible to be 100 percent bulletproof to any vulnerability or attack. However, implementing the right solutions to prevent intrusions and recover faster from a breach can significantly improve an institution’s cybersecurity posture.

As part of a defense-in-depth approach, the following best practices can mitigate threats and risk while improving security initiatives campus wide:

1. Simplify and Securely Support Bring Your Own Device (BYOD) Requirements
2. Educate Students, Faculty, and Staff about Malware
3. Make Access Conditional to Enhance Secure Collaboration
4. Update, Virtualize, and Patch
5. Establish Endpoint Security Hygiene
7. Maintain Host-Based Security Systems
8. Isolate Networks
9. Limit Lateral Movement with Automation
10. Deploy Content Scanning and Run a Comprehensive Backup System
Simplify and Securely Support BYOD Requirements
1. Simplify and Securely Support BYOD Requirements

Let students, faculty, and staff bring the devices they want to campus and then easily and securely support the apps, data, and resources they need while streamlining device management. Modern end-user technologies such as the secure digital workspace make the possibility of limitless learning with continuous collaboration more secure, affordable, and achievable than ever.

The digital workspace unifies application delivery, identity, access, and policy management for all students, faculty, and staff and all of their devices. Consumer-simple and enterprise-secure, the VMware Digital Backpack for Education—powered by VMware Workspace ONE™—covers the full spectrum of institution and device-enablement options—from completely unmanaged, browser-based onboarding of end users using personal devices to enablement of fully managed institutional devices. Campuses can also deploy virtual desktops or research environments, and online learning or HR portals as part of a digital workspace strategy, ensuring applications and user personas are decoupled from operating systems (OSs) and managed from the software-defined data center.
To increase data protection, campus IT teams can:

- Deploy identity-based conditional access to information combined with granular data-loss prevention controls to mitigate the risks of data getting into the wrong hands.
- Establish a policy management system, that at a minimum, includes policy setting based on session length, device type, geographic location, application type, authentication type, and user group membership.

- Implement technology to quickly and remotely wipe devices clean, removing data and applications, in the event a device is compromised or lost, or when students and employees permanently leave your institution.
- Use virtual desktops and applications to prevent users from storing data on (and removing data from) endpoint devices.
Educate Students, Faculty, and Staff about Malware
2. Educate Students, Faculty, and Staff about Malware

Higher education’s on-going digital transformation—from e-learning to workflow collaboration to mobility—challenges IT departments to educate all system users about their roles in keeping data safe, particularly how they can inadvertently spread malware. Although training may be difficult to enforce among student populations, IT must advance cybersecurity education:

- Ensure anyone accessing campus systems knows about the dangers of clicking on links or downloading attachments from personal email accounts using shared systems.
- Help full- and part-time campus and online learning students understand that some websites contain malvertisements and can compromise web browsers that infect entire systems.
- Educate faculty and staff with access to systems about cyber threats. Explain their role in preventing the spread of malware, and at the end of training, test their vigilance.

If you are part of a campus staff seeking assistance with better securing end-user computing technologies, trusted third parties can help your team establish on-going training programs.

Increasing Opportunity for Intrusion

- 430+ million new unique malware pieces in 2015
- 36% increase over the prior year
- 75% of legitimate websites have unpatched vulnerabilities

---

Make Access Conditional to Enhance Collaboration
3. Make Access Conditional to Enhance Collaboration

Although many data breaches are still the result of negligence—innocently leaving an institution-furnished device in a restaurant or accidently downloading an app with access to core systems—others are malicious. Unfortunately, more damage than necessary is often incurred because too many users have unnecessarily broad access to too many applications and too much data.

Identity management enables campus IT teams to secure access to resources while also improving experiences, regardless of the devices individuals use. Through a single app catalog, users have one location to access all of their applications, taking advantage of a single sign-on (SSO) experience that removes end-user access friction. Users get the resources they need to be productive while IT maintains security and control of the environment.

Traditionally, IT has either had to manage devices with traditional mobile device management (MDM) techniques or use AppConfig which meant all devices had to first be enrolled to combat the potential for data loss. Now there’s a better way. Building on the identity-defined workspace, a managed workspace leverages the privacy protections inherent in iOS, Android, and Windows 10 to allow the native OS to enforce application policy—without exposing privacy-sensitive information to IT.

A digital workspace enables IT teams to transform experiences for BYO devices:

- Provide simple access to an app store and app launcher, and access to an application requiring greater protection through services activation.
- Enable the push of a certificate to a user’s device to anchor one-touch authentication, enforce PIN-strength policy, and enable IT to wipe only a protected application while enforcing cut, copy, paste, and open-in controls.
- Protect user privacy by preventing IT from accessing personal user data including applications, file storage, and GPS.
Update, Virtualize, and Patch
4. Update, Virtualize, and Patch

Many campus operations—think financial aid, campus security, health services, and other administrative functions—run critical processes that are dependent on legacy applications. Yet campuses can no longer afford to run these operations on unsupported, highly vulnerable, legacy systems because customized support for unsupported OSs is both cost-prohibitive and unsustainable.

To strengthen the security of existing legacy infrastructure and gain opportunities to budget for IT modernization projects, IT teams can virtualize applications. An agentless application virtualization solution accelerates application deployment and simplifies application migration by isolating applications from their underlying OSs to eliminate application conflict and streamline delivery and management.

Inconsistent patching processes also increase the risk of malware getting inside campus systems. This may be a factor of staff time or the inability to schedule planned downtime. Not patching in every case increases risk. Where users are running legacy applications with known vulnerabilities, IT must make faster decisions to modernize, including taking the following steps:

• Download and run all patches from third-party software providers.
• When migrating from prior Windows OS versions, migrate legacy web applications that rely on Internet Explorer by virtualizing Internet Explorer along with the application.
• If a security patch breaks the software, use a network virtualization with micro-segmentation solution such as VMware NSX® to quarantine non-updated software from the rest of the environment, protecting the data and network until the issue is resolved.
Establish Endpoint Security Hygiene
5. Establish Endpoint Security Hygiene

Hindsight is 20/20. Any campus that has experienced a public data breach can attest to it. Traditional, policy-based checklists of security functionality are no longer sufficient. Preventative measures are integral to a holistic cybersecurity strategy because campus data is now accessed anytime, anywhere across workstations, PCs, and mobile devices.

True, comprehensive mobile security includes protecting the following:

- **Devices** - Protect against malware, viruses, and suspicious device behaviors
- **Networking** - Block malicious networks and man-in-the-middle threats
- **Applications** - Scan, analyze, and validate public and private applications
- **Cloud** - Secure and monitor cloud services against data loss and cyber threats

The Mobile Security Alliance (MSA) unifies threat security for mobility against cyber attacks by integrating the industry’s leading security solutions with the VMware AirWatch® enterprise mobility management (EMM) compliance engine. This provides comprehensive cybersecurity with secure, simple, and scalable options to protect mobile devices, applications, networks, and cloud services.

Endpoint monitoring and auditing are also critical to a sustained detection strategy on non-mobile OSs, including Windows, Linux, UNIX, and Mac OS. Protection can be accomplished by combining the speed and scale of an endpoint security platform with layered OS migration technology to deliver an integrated solution for unified endpoint management and security. Modern solutions enable IT to gain new levels of cost efficiency while setting the bar for security health across the entire environment.

For campuses migrating to Windows 10, proven threat detection technologies and endpoint security hygiene such as VMware TrustPoint™ powered by Tanium, enable a single administrator to concurrently handle 100 or more migrations per day from a central console.
Make Decisions App by App and Resource by Resource

IT teams must be able to give different individuals differing levels of access to data, resources, and applications across desktops and mobile devices for academic institutions to have a successful defense-in-depth security strategy, yet IT management technologies sometimes fail to make it easy for administrators to do so. Students taking different courses, faculty teaching in specific disciplines, caregivers stationed in medical clinics, operations staff located across financial offices, and others require solutions that simplify distinctions by course, by app, and by resource.

Combining VMware NSX and AirWatch technologies, campus IT teams can assign specific mobile applications to specific data centers. Access to those then require proper credentials. They can also create application-level VPN access so an application only has access to a specific resource within the data center, rather than holding the keys to access data broadly across the data center.

A per-app virtual private network (VPN) solution such as VMware AirWatch Tunnel™ provides enhanced network security, seamless enterprise network access for end users, and simplified management for IT. At the same time, IT can rely on information container technology such as VMware AirWatch Content Locker™ to further limit access to more sensitive information.

- Provide a secure method to allow both internally built and public applications to access resources residing in a secure network on a per-app basis.
- Enhance data-loss prevention with app-level security and multifactor authentication.
- Support both Android and iOS device ecosystems natively, moving away from the shortcomings of traditional application tunneling solutions.
- Protect sensitive content in a container and give users a central application to securely access, store, update, and distribute the latest documents for their mobile devices.
Maintain Host-Based Security Systems
7. Maintain Host-Based Security Systems

Cyber attacks often take advantage of relatively weak or nonexistent security within a data center to move freely between different systems and restrict information. Both a strong perimeter and security controls within the data center are required for the best protection.

IT organizations can apply micro-segmentation with its fine-grained network controls supporting unit-level trust and flexible security policies all the way down to a network interface to better safeguard data. In a physical network, this would require deploying a physical firewall for every workload in the data center, which is why micro-segmentation until now has been cost-prohibitive and operationally unfeasible.

Network virtualization technology that includes micro-segmentation enables today’s higher education IT teams to

• Simplify network security by enabling each virtual machine (VM) to be its own perimeter.
• Align policies with logical groups—for example students, virtual labs, and faculty—to prevent threats from spreading.
• Create a matrix of policies on centralized, chokepoint firewalls for the correct security posture.

Malware primarily infects endpoints, which makes having micro-segmentation across virtualized desktops even more important. It prevents compromised hosts from talking to one another when properly segmented. Organizations can recover in a much more effective manner through recomposing the desktop to the previous state to stop the propagation of the infected host.

In a lab already running virtual desktop infrastructure (VDI), for example, IT administrators can further simplify network security while creating a zero-trust environment by adding the following practices:

• Firewall and filter traffic based on logical groupings such as a specific app’s traffic.
• Simplify, program, and automate the application of network security policy to desktop users and pools.
• Dynamically service-chain by tagging solutions available to share intelligence and gain automated, policy-integrated malware protection in rapidly changing security conditions.

Micro-segmentation simplifies network security.
Isolate Networks
8. Isolate Networks

As part of a best practice network security strategy, IT departments should programmatically provision and manage networks independent of underlying hardware. A network virtualization solution, such as VMware NSX, delivers the operational model of a VM for the network, reducing operational and capital expenses, which can be critical to budget-constrained institutions.

- Reproduce the entire network model in software, enabling any network topology—from simple to complex multitier networks—to be created and provisioned in seconds.
- Support a library of logical networking elements and services, such as logical switches, routers, firewalls, load balancers, VPNs, and workload security.
- Create isolated virtual networks through custom combinations of these capabilities.
- In combination with VMware Horizon® virtual desktops and AirWatch enterprise mobility management, NSX provides end-to-end security from the device to the data center.

NSX addresses malware threats and other key IT challenges with significant results:

- **Micro-segmentation for security** — Minimizes the risk and impact of data breaches with firewall controls and security for east-west traffic inside the data center. CapEx savings of 68 percent.
- **Automated IT** — Reduces manual errors and cycle time for network provisioning and management. Accelerates IT service delivery and time to market for new applications. OpEx savings of 56-86 percent.
- **IT optimization and refresh** — Catalyzes modern leaf / spine network fabrics, bare metal switches, open networking, and other data center optimizations through flexible infrastructure. CapEx savings of 66-88 percent.
- **Disaster recovery** — Reduces the risk and impact of unplanned outages through cloud-scale service availability. OpEx savings of $690,000 to tens of millions of dollars (USD) per incident.*

Limit Lateral Movement with Automation
9. Limit Lateral Movement with Automation

An intruder with a persistent, multipronged, resilient, and stealthy attack strategy can move inside a data center between systems relatively unencumbered, and steal sensitive data for weeks (or even longer) before being detected. Segmentation exists in data centers today but most network segments are much too large to be effective. They are typically created to restrict north-south traffic between the Internet and the data center or between client workstations and the data center.

To be completely effective, segmentation (and firewalling) must be possible down to the level of the individual workload, so that east-west traffic can also be secured. Campuses interested in stopping malware from continuing to multiply monthly can take steps to stop vulnerable apps from communicating with other systems on networks and in the data center. The fastest way to do this is by automatically segmenting compromised systems.

- Use behavior detection to prevent further attack by constraining communication between the infected host and others.
- Automate the quarantine of endpoints that become infected, effectively sandboxing the compromised machine.
Deploy Content Scanning and Run a Comprehensive Backup System
10. Deploy Content Scanning and Run a Comprehensive Backup System

There is a common misperception that malware only enters data center environments through Internet ports such as Port 80 from Web clients and Port 443 for web sites using SSL. Campuses cannot ignore the fact that malware enters through other pathways including DVDs, CDs, games, USB drives, IoT devices, and more.

Content scanning and blocking of all incoming files using an antivirus server can be deployed as yet another safeguard for mitigating cyber threats:

- Enable content scanning of all files coming into the campus network and prevent uploading until the scanner indicates a file isn’t infected.
- Reject files with malware and present an error message to users, informing them of the threat.
- Avoid accepting files that cannot be scanned and establish a policy for resubmitted files.
- Add capabilities such as advanced security service insertion that enables deep packet inspection (DPI) of encrypted outbound payloads from the data center.

Moreover, cyber attacks can happen at any time, putting data and communications in jeopardy and compromising learning and research. The right backup system can save time. Backup software simply makes a copy of files on storage separate from the main hard drive. The most effective recomposing requires a comprehensive backup system, yet it’s not enough to just have it running. The system must be regularly tested to ensure it is backing up what it’s supposed to, whether that is files, folders, or full disks.

- Schedule scans for new and changed files daily, weekly, or monthly—or better yet, continually.
- Copy entire hard drives, including system files, to store a complete disk image.
- Consider cloud backup on remote file servers in encrypted format.
- Regularly test backup systems to be sure they are operational, preventing further disaster.
Mitigate Cyber Threats

No campus can ever be completely protected from cyber threats because criminals are inventive. IT teams in education, however, can create a cybersecurity strategy that encompass a comprehensive and layered framework, combining a risk- and policy-based, defense-in-depth security approach. Your academic institution can follow the outlined best practices and team with a trusted advisor such as VMware to deploy solutions that reduce the negative impact of malware while improving security policies, processes, and technologies.

For campuses that have a Student Information System (SIS) from Ellucian, VMware offers integration between the Secure Digital Backpack for Education and SIS databases to help IT teams automate the delivery of a consistent and personalized secure digital workspace to every student for anytime, anywhere, any device access throughout their entire time at school. As students add classes to their schedules, the relevant apps and content for those classes are securely and automatically added to the students’ digital workspaces. Conversely, as classes are dropped, they are automatically removed making a simple end-user experience for students that requires no action on their part. Each secure digital workspace then follows a student throughout his or her life at school.

Together, VMware and MSA partners provide a robust set of solutions and a proven framework to address higher education technology and security needs.

For additional information and resources about how to mitigate information security threats, visit [http://www.vmware.com/solutions/industry/education.html](http://www.vmware.com/solutions/industry/education.html).