ellucian

Information security for higher education

Tools and practices for identifying, assessing, and managing risk

Contents

If you're losing sleep over the importance of securing your institution's vast data stores, you're in good company. Information security remains a top issue on EDUCAUSE's Top IT Issues 2021, as ranked by both IT and non-IT leaders across higher education.

The threats are constantly growing and changing. Work from home has opened up institutions to more attacks. Information security must support the strategy of the institution and promote goals like student success and graduation rates. There will never be a single static solution, and the work will never be done. But we can minimize risk by making smart, sustained investments in planning, policymaking, auditing, technology upgrades, and education.

Conduct a risk assessment

No one's immune to a data breach—but just how vulnerable are you?

When it comes to information security, taking a hard look at your institutional risk may not be easy. But it's a critical step toward keeping your campus safe.

So what does a risk assessment even look like? What and who are involved? And what are the end goals?

Here are some best practices to help you get started.

1. Get the right people in the room

While IT may lead the charge, your assessment will only have the necessary weight and impact if you engage a range of stakeholders. That's because, in addition to technology, people and processes are significant risk factors.

Engaging your team

Create a sense of urgency without creating a sense of panic, use non-technical talk that everyone can understand, and don't promise things that can't be delivered.

Stakeholders to engage:

1. **Executives.** Institutional leaders must set the tone that security involves everyone, and that it's okay to have a frank and honest discussion about possible weaknesses. Executive buy-in will also be crucial once the assessment is complete and you need to garner adequate resources to address vulnerabilities.

2. **Department heads.** In addition to providing access to systems and data, department heads must share ownership for any risks identified. That could mean overseeing changes to address threats—or, if that's not possible, assuming and planning for an acceptable level of risk.

3. **Finance, HR, and legal.** Because you'll be assessing policies and procedures that govern the use of personal and financial data across all departments, having representatives from finance, HR, and legal involved at every stage is a must.

4. **External auditors.** If you have the resources, you may consider hiring an external company to assess or audit your security risk. In addition to identifying technical vulnerabilities, expert auditors can also evaluate your risk of non-compliance with specific data privacy or usage guidelines. Since the latter can result in heavy fines or reputational damage, the investment may be worth it.

5. **Vendors and partners.** If there are third parties sharing or storing your data, their vulnerabilities might as well be your own.

2. Choose a methodology

There are many methodologies for conducting a risk assessment. Some are open source, some are proprietary, but all aim to answer the same basic questions:

- What assets do we need to protect?
- Who/what poses a threat to those assets?
- What would the impact be if those assets were stolen, damaged, or lost?
- What needs to happen in order to minimize our risk?

A good starting place for colleges and universities is the HECVAT, a questionnaire framework that was created for higher education to measure vendor risk. Over 100 colleges and universities and 30 solution providers and universities use the HECVAT to reduce risk.

Regardless of which methodology you choose, know that the assessment may force your institution to make some hard choices. That's because the activities you identify as necessary to mitigate risk may cost time or money you don't have. It then becomes important to prioritize.

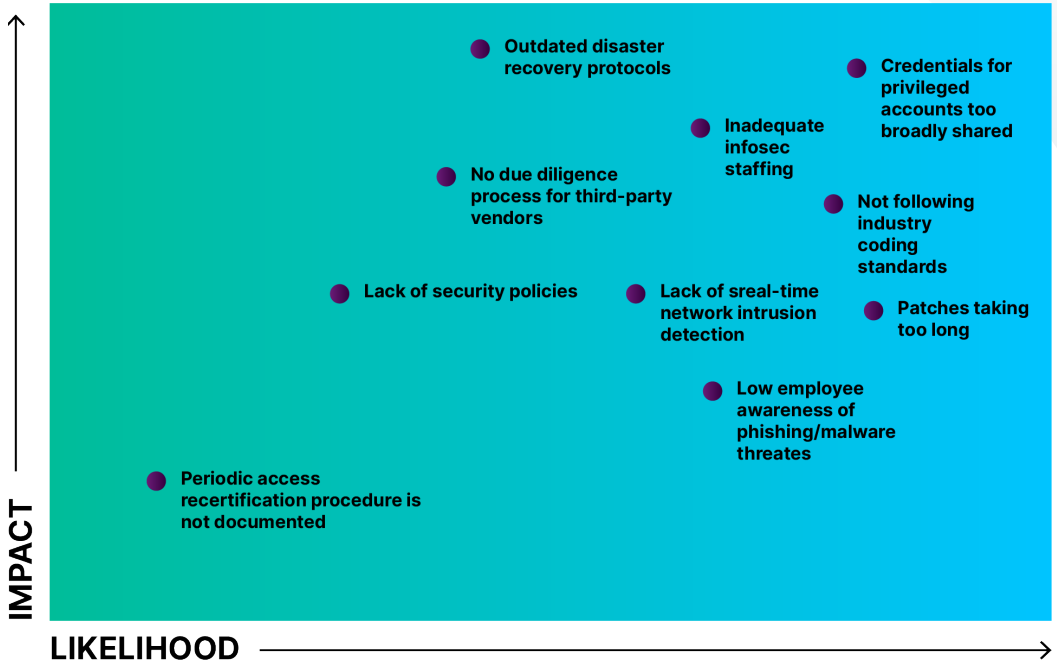
3. Prioritize threats

Not every threat is equally likely to occur, nor will they all have the same level of impact on the institution. If you have limited resources or are creating a timeline, it can help to locate threats on a map of likelihood vs. impact so you can begin to prioritize.

The map to the right shows what this might look like for a sample institution. In the upper right-hand corner, the blue zone, the institution has listed “credentials for privileged accounts being shared too broadly”—which is highly likely to cause significant impact. Maybe administrator passwords are being shared among multiple users, or they’re being left unchanged when new staff replace old. Regardless, inadequate control over access and identity rights is a threat the institution must address immediately.

Closer to the center, in the turquoise zone, the institution has listed “No due diligence process for third-party vendors.” Because there is no known imminent threat, the priority may be slightly lower. But, if the institution’s data were to be compromised due to a partner’s data breach, the impact would still be high. So any delay in addressing this threat implies an acceptance of risk. A map like this helps institutional leaders understand the tradeoffs, so they can have meaningful discussions about their tolerance for risk, allocation of resources, and financial, reputational, and operational impacts.

Sample threat prioritization



4. Make assessments ongoing

Because there are so many factors that impact security—not the least of which is rapidly evolving threats—it's not enough to conduct a single assessment.

Choose a schedule for regularly updating your assessment, whether annual, quarterly, etc. Internal self-assessments should be relatively frequent, while external auditors might be scheduled less often or for specific purposes.

It's also a good idea to engage regularly with peers and industry workgroups. Staying on top of the latest threats, mitigation techniques, technologies, and best practices is often too much for one institution. Attend cybersecurity events and pay attention to what's happening in other fields, such as government or healthcare.

When it comes to vigilance and continuous learning, you can't do too much.

Next steps

Once you've conducted a thorough risk assessment and set institutional priorities, the next step is to create an effective information security plan—including everything from technology to incident response to education.

Assess the strength of your infosec plan

The elements of a good plan (including how to address a breach)

Information with any value will always be at risk. Even institutions with world-class security systems know that a breach is still possible, even likely. The best strategy? Plan ahead. Plan for the short term, as well as the long. Plan for how you'll reduce risk, and how you'll address a breach. And continually revise your plan to keep pace as threats, legal requirements, and technology evolve.

To gauge the strength of your information security plan, answer the following 10 questions:

1. Do we know our security requirements?

In order to plan, budget for, and implement an effective security program, you must first understand 1. what needs to be protected and 2. what it will take to do the job right. This includes taking an inventory of:

- Your institution's data and information assets
- The technology, people, and processes that affect how that information is stored and shared
- Your partners and other external parties, and their security postures
- The tools and capabilities required to safeguard your assets

An important strategy for staying current and compliant is to create a strong partnership between your IT and legal departments.

Even systems and data that are not under the direct control of your central IT team should be included in this audit. The institution is responsible for protecting all of its information assets, regardless of ownership, so your plan must be comprehensive.

2. Are we staying up to date on legal and regulatory requirements?

In addition to your own internal requirements, there are a range of legal and regulatory requirements governing data privacy and protection. Requirements may vary by state, country, or type of institution, but failure to comply can impact your funding and reputation.

One strategy for staying current and compliant is to **create a strong partnership between your IT and legal departments**. Don't leave it to technical staff to interpret the law. Your legal department is best equipped to:

- Understand and monitor local, state, federal, and international regulations
- Put regulations in context as to how they relate to your institution and the level of risk involved
- Help manage compliance

3. Do we have adequate policies and standards?

Every school should have a clear set of policies and standards governing how institutional data gets used, stored, and shared. For example:

- Develop an "Acceptable Use" policy that dictates what employees and other users can or can't do on the institution's network and systems
- Set standards for passwords
- Create policies governing the use of personal devices on campus

The SANS Institute—a non-profit organization serving security professionals across multiple industries—offers templates for creating and implementing a range of information security policies.

All employees should be educated and expected to follow institutional policies and standards.

Ensure other users are informed of their responsibilities as well. Some organizations have a formal certification process for new employees—or all employees at regular intervals—to ensure compliance.

4. Are we tightly managing identity and access?

Identity and access management are about giving the right people access to the right information at the right time. If you don't **keep a tight rein on who's accessing what**, you leave multiple entry points for hackers.

- There are dozens of systems across campus that aren't linked and require separate IDs and passwords. To make life easy, **staff tend to use the same password** for a low-security system (like a survey app) as they do for a high-security system (like payroll). A hacker then only needs to break into the survey app to gain entry into payroll.
- There's **no clear process for changing or removing credentials when employees switch roles or leave the institution**. Perhaps a disgruntled former employee can still access financial information, or a staff member who has moved to a new department can still access information that's no longer relevant to her job.
- Ultimately, institutions need a unified, centralized system for managing identity and access, and it needs to be well integrated into daily business processes.

5. Have we engaged senior management and the board?

Security isn't just a technology challenge, it's a business imperative. Given the large potential impact of a data breach, senior management and board members must be highly engaged in information security planning. IT alone cannot **weigh risk vs. cost and ensure a culture of compliance at every level of the institution**.

When faced with decisions like whether to fund network security, senior leaders need to understand exactly what's at stake and accept responsibility for their decisions.

6. Are we providing adequate ongoing education?

Lack of awareness and education about security threats are among the biggest risks for most institutions. You must have a **well-documented and adequately resourced plan** for ongoing information security training. This could include everything from mandatory courses on phishing and malware to regular e-blasts on the latest threats to annual certification programs.

Educause offers a number of free resources institutions can use to educate faculty, staff, and students about cybersecurity.

7. Are we careful when choosing partners?

When retail giant Target experienced a massive data breach in 2013, it was not their own network that hackers broke into, but rather the network of a heating and air conditioning subcontractor that had worked at a number of Target stores.

No one remembers the name of that HVAC company, but they surely remember Target as a company that lost personal data. Target also paid a heavy financial price to rectify the situation and appease customers. The key takeaway? **You are ultimately responsible** for your students' and employees' personal data, even when—especially when—it's being shared with third-party vendors. Choose partners wisely.

Ask potential partners the same hard questions about the security of their information systems as you do about your own. Discuss auditing and compliance upfront. Put processes in place to hold them accountable. If they can't meet your standards, look for someone who can.

8. Are we using appropriate technology?

Technology can greatly enhance information security. The key is to **modernize and simplify**, since complexity only makes it harder to monitor and control who is accessing what.

- **Identify** and retire legacy systems and business processes that are needlessly cumbersome.
- **Streamline** the steps you use to grant system and data access, as well as those used to close the loop once an employee moves on.
- **Retire** out-of-date systems that no longer receive security patches.

As you build out your information security program, pick the right tools for each job. For example, if you have a highly secure environment, using non-standard laptops or allowing contractors network access might not be wise. On the other hand, if you're securing a simple website with limited connection to other systems, don't overcomplicate the security solution. Using resources wisely is key to winning the security battle on multiple fronts.

9. Do we aggressively follow up on incidents?

We live in a world where data breaches are a matter of "when," not "if." That's why responding appropriately to security incidents is as important as preventing them.

Gather data on incidents that will help you reduce recurring issues or prevent more damaging impact. Establish routines and best practices so you can mobilize quickly in the event of a breach. Review and analyze your trends. Data can also help you make the case for spending more money on things like firewalls or network intrusion detection.

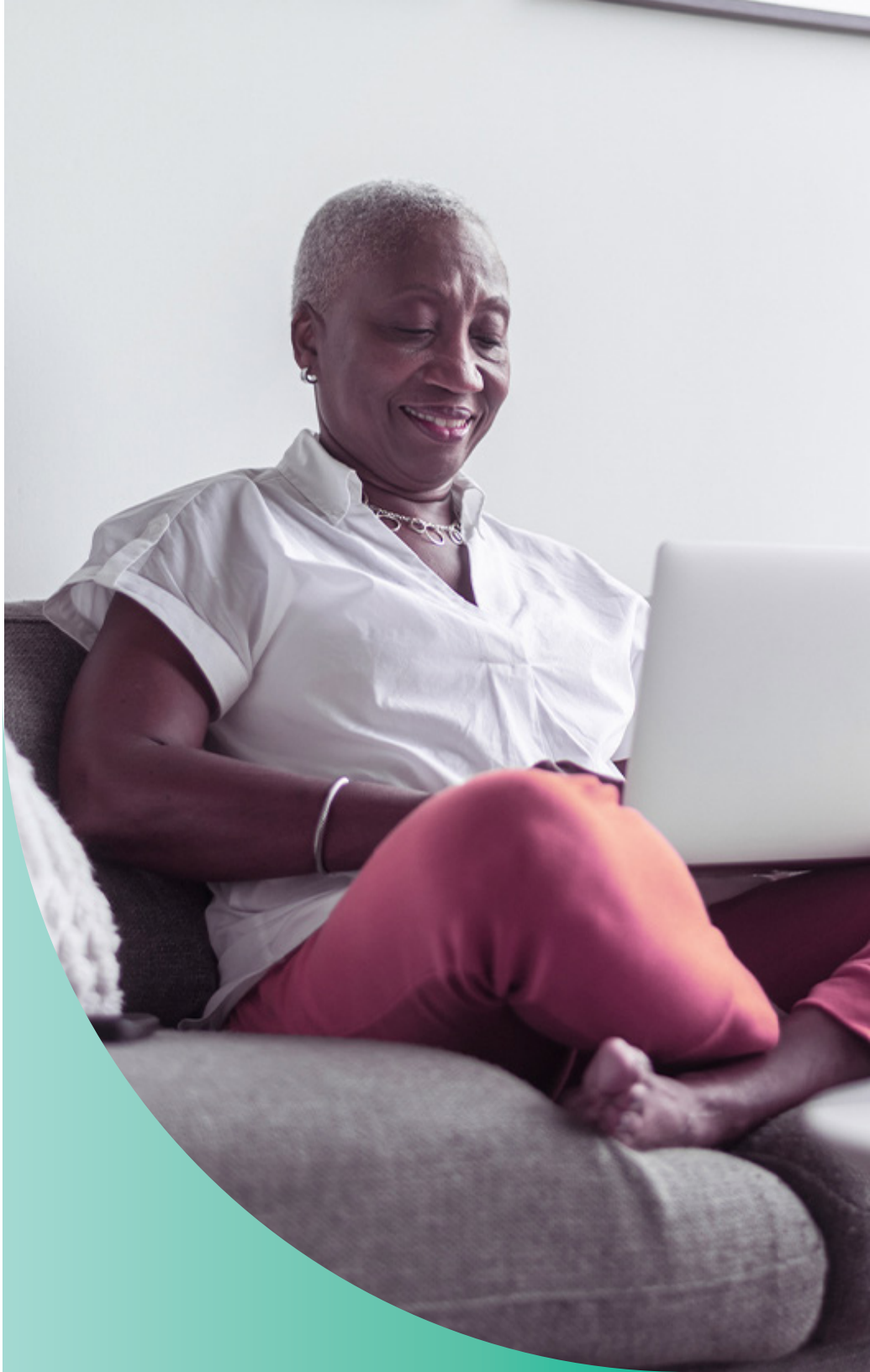
10. Are we making continuous investments?

Information security is an ongoing practice, not a one-time implementation. You will never be fully protected, because there will always be new threats. But with **careful planning—and a sustained investment of resources**—you can effectively mitigate risk.

Make sure that your annual and long-term budgets for information security reflect its level of importance to your business. Help decision-makers understand the link between data protection—or lack thereof—and successful recruiting, advising, fundraising, and other key functions. Stay actively engaged with industry forums and workgroups to understand evolving threats and security best practices.

Get comfortable with discomfort

Planning for something to go wrong, in a world where what can go wrong is constantly changing, is, in a word, uncomfortable. But if you can get comfortable with discomfort—becoming agile, alert, responsive, and realistic—you can create the level of security that faculty, staff, and students need to thrive.



Implement multi-factor authentication

A “belt and suspenders” approach

Phishing attacks are becoming more common and sophisticated every day. According to the FBI, phishing was the most common type of cybercrime in 2020. And, recent research from Proofpoint showed that 75% of organizations around the world experienced a phishing attack in 2020, both successful and unsuccessful.

And it isn’t just phishing that’s a threat to password security. The National Institute of Science and Technology (NIST) recommends complexity over length when creating passwords, and that companies get rid of periodic resets, which leads to the creation of less effective passwords.

Bottom line: even strong passwords are vulnerable and can’t be the only line of defense protecting an institution, its people, and its reputation from the impacts of data loss and theft.

That’s where multi-factor authentication (MFA) comes into play. It’s a belt-and-suspenders approach to data security that blunts the impact of a compromised password because the password becomes just one of several factors used to verify a user’s identity. But due to the perceived complexity and costs associated with MFA, it’s not yet a widespread practice in higher education.

That’s all about to change, for a host of good reasons.

First, **today's MFA systems are not the confusing, helpdesk-call-generating applications of the past.** They are user-friendly to the point that students, staff, faculty, and administrators can verify their identities with just an added tap on their smartphones, tablets, or smartwatches. At the same time, the proliferation of single sign-on technology means that the steps involved in MFA don't need to be repeated every time a user logs on to a new system.

Second, more and more IT departments are taking the time to ensure that any inconveniences that may arise don't create resistance to new security measures.

Third, **MFA integration into myriad software solutions is now much easier than before.**

There's even an ancillary benefit to MFA that is often overlooked: even with an added layer of protection it provides, it results in stronger, more vigilant password practices. With MFA in place, institutions can feel more confident following the NIST recommendation that passwords should not expire without reason. Having to create new passwords less often means users put more thought and effort into the passwords they create and make fewer calls to the helpdesk. Coming back to the belt-and-suspenders analogy, this means the suspenders are not only a fail-safe in the event of belt failure; they strengthen the belt itself.

At a time when even the best-trained among us can fall victim to phishing attacks, MFA helps ensure that an institution is never caught with its pants down.

> "The evolution of threats is ongoing. You have to skate to where the puck is going. Our partnership with Ellucian allows us to anticipate cyberbreaches and create the safeguards to provide the highest level of protection."
>
> Sister Paula Marie Buley
> President, Rivier University

Solve your cybersecurity “people problem”

Focus on people as much as technology to win the infosec game

Whether it’s an employee being tricked into giving up sensitive information, an insider hack, or inadequate policies on access and identity management, cracks in your human firewall are as dangerous as those in your digital firewall. You should be as focused on what’s happening inside the environment as much as what’s coming in from the outside. To ensure your employees are an asset rather than a threat to cybersecurity, make the following strategies part of your infosec plan.

1 Make annual security training mandatory for all employees

All employees, not just IT staff, should be aware of the threats and be equipped to respond appropriately. They should also understand institutional policies regarding the proper use of data and technology, as well as the consequences of noncompliance.

Make annual information security training, whether online or in person, mandatory for all employees. Don’t use the same content year after year. Threats and best practices evolve quickly, and so should your training materials. Train new employees as they join the organization.

Many institutions have a formal acknowledgment process that requires employees to demonstrate that they've completed the training and understand the material.

2 Provide ongoing education

Once-a-year training is not enough. Changing awareness and behavior doesn't happen overnight. And even after change occurs, it can only be maintained through continual reinforcement. Provide regular communications about information security using multiple channels, including:

- **Emails**. Send awareness-building emails on specific threats, best practices, new research and data, etc.
- **Videos.** Conduct short video interviews with your information security leaders and tape any live events or panel discussions for re-use.
- **Posters/signage.** Get creative and share infosec tips and graphics on posters, signage, or in display cases around the office.
- **Newsletters.** Include articles, links to resources, etc. in employee newsletters or other internal communications.
- **Webcasts.** Provide live online training on specific topics.
- **Events.** Hold infosec awareness events or town halls with speakers, games, merchandise, etc.

If you have the resources, consider a training partner. There are many vendors that provide content for all of these channels, which can be used as-is or adapted to meet your needs.

3 Partner with your communications team

Your communications team can greatly enhance the effectiveness of training materials and awareness-building campaigns. When it comes to developing the right messages for the right audiences, developing compelling copy and graphics, and pushing content out through multiple channels, they have the experience and resources required to make an impact.

4 Don't just inform, demonstrate

General education about the threats is important, but it's not enough. If you want people to identify with and retain information, put it in the context of their everyday lives. For example, don't send an email with a definition of "phishing." Send an actual mock phishing email to test whether employees fall prey (by clicking links/opening attachments). For those that do, provide training so they won't get tricked again.

Make sure all communications illustrate concepts with real-life examples. Incorporate practical exercises and test questions into your mandatory annual training to ensure employees have absorbed the information.

5 Develop a "security champions" program

Enlist passionate people across all areas of the institution (not just IT) to champion security, model best practices, support infosec events and campaigns, and continually raise awareness. Provide your champions with monthly or quarterly training and keep them engaged by demonstrating how their efforts are making an impact.

6 Take advantage of Cybersecurity Awareness Month

October is National Cyber Security Awareness Month. Take advantage of the momentum it generates to enhance your own cybersecurity campaign. during this month, such as contests, scavenger hunts, prizes, and desk toys with cybersecurity messaging. Share links to national campaign coverage, events, celebrity ads, and other activities on your social media feed or in your newsletter.

The National Cyber Security Alliance has an array of resources you can use.

7 Bring in guest speakers

While interviews with your own institutional leaders can work very well, sometimes bringing in an outside expert on cybersecurity can increase engagement. Look for speakers with unique stories or from well-known organizations that will pique employees' interest. Host speakers live in a town hall environment and/or make a video available for ongoing education.

8 Partner with HR

Creating a culture of commitment to security requires strong support from every department—especially HR.

The responsibility for protecting information should be incorporated into position descriptions, employee onboarding, and regular training. It should be part of institutional values, policies, and best practices.

As the liaison between leadership and employees, HR can also help foster a culture where it's okay to ask questions. If employees sense that hitting deadlines—with, for example, wire transfers or reports—is more important than exercising caution, they may choose to ignore security warning signs.

Mobile security tips

As we handle more of our personal, school, and work-related business on our tablets, smartphones, and smartwatches, cyber criminals are working harder to trick people into providing sensitive information and downloading malicious apps. Here's how you can protect yourself:

- Use Multi-Factor Authentication (MFA) to protect your personal accounts, including email, social media, and banking
- Enable your screen auto-lock feature
- Use passcodes, strong passwords, and biometric authentication to prevent easy intrusion
- Guard your screen in public places—you never know who's watching
- Use trusted Wi-Fi networks and use caution with public Wi-Fi
- Use complex passwords for mobile hot spots and turn the feature off you're not using it
- Only download apps from trusted sources
- Keep mobile device software and applications up to date
- Be on the lookout for phishing scams, and never click unknown links or attachments
- Evaluate embedded links and senders by pressing and holding links and tapping sender names to view details like full email address, date, and time stamps
- Educate yourself on Internet of Things (IoT) devices and how to protect yourself while using them

Stay safe in the cloud

Is the cloud less secure? Not if you do these three things.

It's clear that higher education is moving to the cloud. For most institutions, the benefits, like disaster-recovery, simply outweigh the risks. What's not clear is whether information security belongs solely in the "risk" column. In fact, the cloud offers great potential to improve data security, as long as you do three things:

1 Understand that it's not about where data lives, but how it's controlled

Many institutions equate having physical control of their data with better security. But that's simply not the case. On-campus data servers are often located in buildings to which many people have access. The process and tools for managing who can enter a facility, room, or floor may be more prone to error or breach than **appropriate rules restricting data movement** in the cloud.

In fact, what percentage of college or university servers are encased by multiple layers of physical security (fences, barricades, video surveillance, etc.), with entry requiring sophisticated badges, pins, and checkpoints monitored by trained staff whose only job is server protection? The best cloud providers can offer this level of protection because—unlike higher education institutions—security is their core business.

Another risk to storing data on campus is that a single event—whether a breach or natural disaster—can compromise all of your assets and bring operations to a halt. Most cloud providers, on the other hand, have data backed up to multiple geographical locations, as well as processing capability at multiple sites, making recovery easier and potential disruption lower.

Moving data to the cloud doesn't mean giving up control, but rather thinking differently about who controls what and how.

2 Embrace the shared responsibility model

Cloud offers tremendous potential to improve security, mobility, agility, and scale. But to realize these benefits, institutions must learn to rely more on partners. This means selecting a reputable cloud vendor and being transparent about, and committed to, a shared responsibility model.

To be clear, regardless of where its data and applications live, an institution will always bear responsibility for security and compliance. But in the cloud model, its role changes. Typically, cloud vendors secure and manage the physical infrastructure that stores and serves data, as well as any cloud-based (SaaS) applications the institution may be using. Meanwhile, the institution secures the operating system, networks, and on-premise applications used to access data and services in a public cloud (including user identity/access management).

Amazon Web Services offers a useful graphic showing how the cloud provider is responsible for security of the cloud, while the customer is responsible for security in the cloud. In other words, you are ultimately responsible for defining who can access what, how well data is encrypted, and how data flows between systems and applications.

The good news is: this is what your IT staff should be focused on. Once they're freed from day-to-day server maintenance and protection, they can approach how data is governed and utilized strategically across the institution to make better decisions.

3 Take advantage of the security benefits inherent to cloud

While you are still responsible for governing your data in the cloud, cloud providers offer an array of tools that don't cost extra to make this easier—and easier to do at scale:

- **Encryption.** Many vendors offer state-of-the-art encryption tools that you can use to improve protection of data you move to the cloud. (Just note that it's still your responsibility to use them and to secure access.)[21]
- **Multi-factor authentication (MFA).** MFA adds an extra layer of protection on top of a username and password, such as sending a text message with a randomly generated number that the user must enter to log in. MFA is becoming common practice for sensitive data, so take advantage of this capability if it's available.
- **Identity and access management.** As data proliferates across campus, assigning identity and access rights is more important—yet more complex—than ever. While only you can set policies and permissions, your cloud provider may offer tools that make it far easier to track the who, what, when, and where of data access at scale.

The Ellucian approach to cloud security

Data confidentiality, data integrity, and system availability are vital concerns in higher education.

From rigorous independent compliance audits, penetration testing, and security reviews to threat monitoring, logical security, and security incident response. Ellucian's cloud offerings use the Amazon Web Services (AWS) cloud infrastructure, making Ellucian the world's leading provider of software and services that power the essential work of colleges and universities.

Ellucian achieved its ISO27001:2013 certification in 2021. This certification is the international standard that defines best practices for implementing an information security program.

Next steps

The cloud represents a seismic shift in the way we use technology to manage the flow, use, sharing, and protection of data across higher education. Questions, concerns, and a measured pace of adoption are to be expected.

But as more institutions challenge the traditional model and discover the cloud to be as, if not more, secure, adoption will only accelerate.

Sources

“2021 State of the Phish.” Proofpoint, September 21, 2021. https://www.proofpoint.com/us/resources/threat-reports/state-of-phish.

“Cybersecurity Program.” EDUCAUSE.edu. Accessed October 4, 2021. https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program.

Grassi, Paul A, Michael E Garcia, and James L Fenton. “NIST Special Publication 800-63 Digital Identity Guidelines.” Digital Identity Guidelines, June 2017. https://pages.nist.gov/800-63-3/sp800-63-3.html.

“Higher Education Community Vendor Assessment Toolkit.” Higher Education Community Vendor Assessment Toolkit, April 15, 2021. https://library.educause.edu/resources/2020/4/higher-education-community-vendor-assessment-toolkit.

“Internet Crime Report 2020,” 2020. https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf.

“Multifactor Authentication Strengthens Cybersecurity across University Campus.” University Business Magazine, September 16, 2019. https://universitybusiness.com/multifactor-authentication-strengthens-cybersecurity-across-university-campus/.

“National Cyber Security Alliance.” Stay Safe Online, August 24, 2021. https://staysafeonline.org/.

“Security Policy Templates.” Information Security Policy Templates | SANS Institute. Accessed October 4, 2021. https://www.sans.org/information-security-policy/.

“Shared Responsibility Model.” Amazon. Francis Lefebvre, 2018. https://aws.amazon.com/compliance/shared-responsibility-model/.

“Top IT Issues, 2021: Emerging from the Pandemic.” EDUCAUSE Review. Accessed October 4, 2021. https://er.educause.edu/articles/2020/11/top-it-issues-2021-emerging-from-the-pandemic.

“Understanding Data Privacy – A Compliance Strategy Can Mitigate Cyber Threats.” Understanding Data Privacy – A Compliance Strategy Can Mitigate Cyber Threats | Thomson Reuters. Accessed October 4, 2021. https://legal.thomsonreuters.com/en/insights/articles/understanding-data-privacy-a-compliance-strategy-can-mitigate-cyber-threats.

Ellucian is the market leader charting the digital future of higher education with a portfolio of cloud-ready technology solutions and services. Serving more than 2,700 customers in over 50 countries, reaching over 26 million students, Ellucian delivers student information systems (SIS), finance and HR, financial aid, integration, analytics, recruiting, retention, and advancement software solutions. Ellucian also supports the higher education community with a range of professional services that includes application software implementation, management consulting, and grants services.

Visit Ellucian at www.ellucian.com.