ellucian

WHITE PAPER SERIES

Choosing a Security Framework to Protect Your Intellectual Capital

The right security framework can save your institution from a financial and PR nightmare.

Choosing a Security Framework to Protect Your Intellectual Capital

The right security framework can save your institution from a financial and PR nightmare.

Colleges and universities are more than repositories of knowledge. They are complex technological systems housing vast amounts of sensitive data—everything from research to student records. Health data, social security numbers, and financial information reside in campus databases, ready to be accessed by staff and faculty.

But that same information, necessary to keep the institution operating at peak efficiency, can also be accessed by hackers both on and off campus if it isn't adequately protected by a multi-layered, comprehensive system following the recommendations of a trusted security framework.

When a data breach occurs (and it is certainly a question of *when*, not *if*) the impacts can be staggering. By sheer numbers, millions of dollars may be lost, but the most severe damage may be to the institution's reputation. In the wake of a highly publicized breach, public trust in a school—whether public or private—will be seriously eroded. And regaining that trust takes a long time.

Adopting the "It won't happen to me" position is not a security strategy. In today's technological landscape, it's simply dangerous.

Some 50 percent of colleges and universities can expect some kind of attack. These attacks will vary in sophistication, from crude attempts to hack into the system to brazenly advanced schemes to steal information from within the institution. "It's not always a student in the back dormitory trying to break in and change his grades," says Brian Knotts, senior vice president of applied research at Ellucian. "During one of the most recent attacks, they actually created a data warehouse, inside of the company, to transmit the data out."

The fallout from an attack can be devastating. Attackers will gain possession of administrative data, intellectual property, student records—just about any piece of information on campus—and it is impossible to undo the damage once it has occurred.

But the problems for an institution don't end once the data has been nabbed. A college or university must then shell out millions for credit protection and inform all of those who have been infected. In the case of intellectual property loss, years of research and proprietary information may be lost. And the damage to reputation is incalculable. "Everybody reads the paper," Knotts says. "Those

are not the kind of headlines you want to make at your institution."

With so much at stake—from accidental, internal leaks to high-level hacks resulting in data loss and public relations nightmares—now is not the time for institutions to casually cobble together a security framework. It's time to consider thorough and thoughtful approaches to guarding sensitive information.

Courting disaster

For years, higher education institutions have considered themselves immune from cyberattacks. Or worse, have simply ignored the issue or do not know where to begin when protecting the organization. "A lot of people just don't know how to protect the institution," says Knotts.

But attacks on colleges and universities now account for some 17 percent of all data breaches, second only to the medical industry. And experts agree that that data breaches and cyberattacks on universities and colleges will continue to increase in frequency and sophistication.

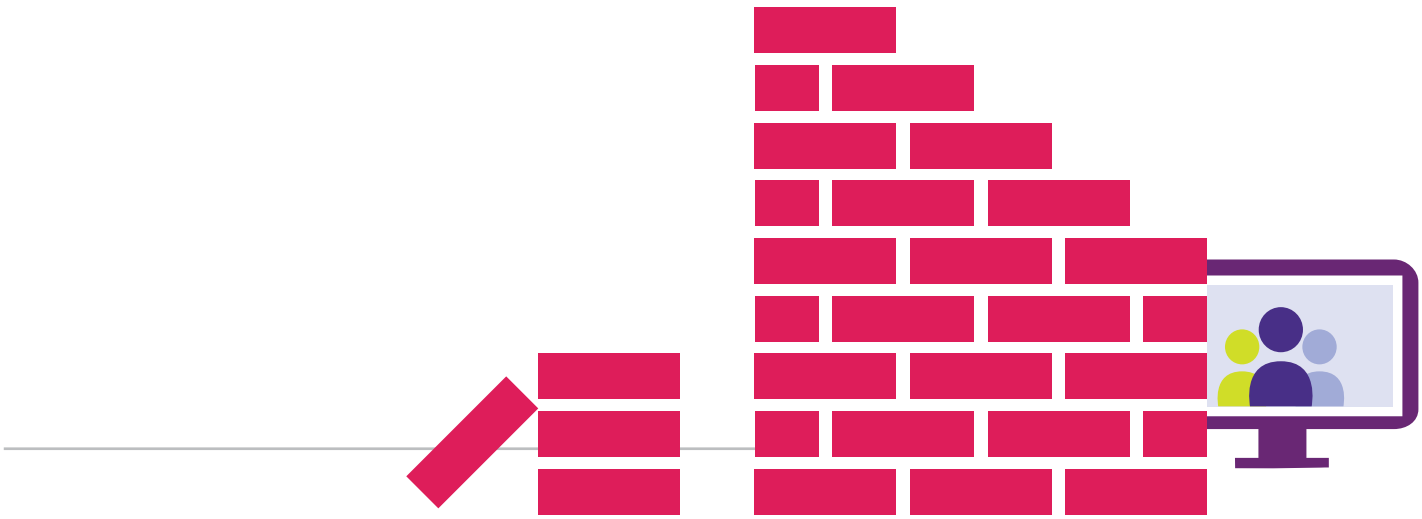
Each year, universities and colleges find themselves under attack—and those attacks show no sign of decreasing. A sophisticated cyberattack can expose research and personnel records, as well as sensitive student data. The final price tag for one of these attacks may climb into seven figures. Any institution operating without a dynamic, robust security framework is simply courting disaster.

Half measures won't cut it

Most institutions have developed or implemented some form of information security—and that's good. But simply employing a firewall is not enough. Institutions must adopt an aggressive and comprehensive approach to data security. You're not simply building virtual walls around sensitive information—you're meeting the attack before it even reaches your fortifications.

That's where a security framework comes in. A security framework is a comprehensive strategy for going toe-to-toe with potential threats while keeping data secure. It is a tool that provides methodology and a calculated process for assessing risk to determine where resources need to go in order to protect the information systems within an organization. And on a college or university campus, those systems can be exceedingly complex and spread out. A well thought-out and implemented framework will place an institution in a strong position to confront threats from hackers on or off campus, while helping to guide decision-making when it comes time to deal with potential threats. Failing to utilize an effective security framework is akin to entering a battle with no clear idea of your objectives, or even where the front lines are located.

Implementing a security framework is critical to ensure that an institution knows how its data will be protected, who may be accessing it, and when. "You want to really have a set of rules that are set up that watch these sensitive parts of the system," says Knotts. You need to go back and say, Where was that system accessed and why? So you want to create these layers of security, so you know where the information is coming from."



Five security framework methods

All security frameworks have pros and cons. There is no one-size-fits-all framework that would work for every institution. Colleges and universities are simply too varied, ranging from large multi-campus schools with numerous research databases to small private institutions which are largely self-contained. And the IT staff within those schools vary widely when it comes to training and expertise.

That's precisely why an institution must research the available security frameworks and balance the benefits and drawbacks of each approach. Institutions would benefit from investing the time and effort required to investigate all of the options before adopting a framework.

Generally speaking, there are five common security framework methods available to institutions that are looking to establish a thorough and complete system to protect campus data.

1 Factor Analysis of Information Risk (FAIR)

FAIR is designed to provide organizations concrete and reliable methods to ascertain and address risk. It was created to address a pressing need to standardize and codify how organizations manage risk. Previously, many experts believed that security practices were too haphazard, relying too much on intuition, industry lore, or the experiences of a limited number of information security professionals within the organization. Some of these elements are indeed valuable to manage risk, but the problem is this: Management can't rely on them to consistently make informed decisions about information risk.

FAIR tackles these weaknesses by setting up a method to systematically apply risk assessment to any asset, and to view an organization's total exposure to risk. The framework utilizes an analytical system to challenge or defend any determination of risk, and grants an organization tools to measure how its security profile may change over time, or with fluctuating budgets. In short, FAIR strives to standardize risk assessments and management by providing a common language available to any organization.

For more on FAIR, visit **http://fairwiki.riskmanagementinsight.com.**

2 National Institute of Standards and Technology's Risk Management Framework (NIST RMF)

The Risk Management Framework of the National Institute of Standards and Technology is a flexible security methodology that can be applied to the latest information systems, as well as those that have been around a while. The framework manages risk through implementation of security controls in systems while monitoring those controls, looking for changes and analyzing the long- and short-term impacts of those changes. It provides a regular report outlining aberrations and their effect on the system.

This security framework selects a set of security controls based on the Federal Information Processing Standards 199 security categorization, as well as that standards' minimum security requirements. The framework categorizes the information within each system based on the potential impact of a security issue, and then assesses all security controls to determine which

ones are being used correctly, operating as required, and doing what's needed to keep the system secure. The framework also authorizes access and operation to any information system based upon the risk level of individuals using it, or whether accessing any system would pose an unacceptable risk to the organization.

For more information, visit **http://csrc.nist.gov/groups/SMA/fisma/framework.html.**

3 Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE)

OCTAVE was developed by Carnegie Mellon University's computer emergency response team (more commonly known as CERT.) This security framework offers a strategic approach to information security.

OCTAVE is comprised of three models. The first is a basic version designed for organizations of 300 or more employees. This original version forms the foundation for the other two, with a host of techniques and tools for assessing risk and managing information security. The second model, called OCTAVE-S, is primarily for organizations with more constrained information security and risk-management resources. The third model, OCTAVE-Allegro, is much more pared down compared with the other two, but still offers a rigorous method for risk assessment and management.

For more information, visit **http://www.cert.org/resilience/products-services/octave/index.cfm.**

4 SANS 20 Critical Security Control

Critical Security Control is a highly effective security framework that takes the tools, products, and processes which have been most effective in "real world" applications and uses those security controls to safeguard data. By using this framework, the US State Department claims to have demonstrated a 94 percent reduction in security risk.

Critical Security Control applies a basic but effective idea to security: Use tools that have a proven record of getting the job done, and make everything simple and systematic. It emphasizes standardization and automation as a method to increase the effectiveness of the framework, and to help increase efficiency as well. By doing so, Critical Security Control is able to prioritize security functions with a proven track record against threats, and employ them comprehensively across the system.

For more information, visit **http://www.sans.org/critical-security-controls.**

5 Threat Agent Risk Assessment (TARA)

TARA was developed by Intel and utilizes a "predictive" system to assess risk. It combs through all of the possible threats to an organization's information security and provides a boiled down list of the most likely cyber dangers. The chief benefit of this approach is that it saves time and money by concentrating efforts on only those threats and vulnerabilities that are most likely to cause problems, rather than relying on a "shotgun" approach to ward off everything lurking out there.

This is a relatively new methodology, but it allows organizations to be proactive without shedding too much time and money. TARA identifies the greatest security risks to an organization and the potential outcomes associated with that risk—what damage is likely to occur, and how the breach will likely unfold. TARA then takes that information and examines it against the organization's current strengths and weaknesses

to see where problems may exist. It then spotlights those areas that are more vulnerable to the threat. The objective, simply put, is to focus efforts to avoid wasted resources on threats that just aren't likely.

For more information, visit **http://www.intel.com/Assets/en_US/PDF/whitepaper/wp_IT_Security_RiskAssessment.pdf.**

Making a choice—one, two, or a hybrid approach?

There is no "one size fits all" when it comes to selecting a security framework. Institutions must carefully weigh the pros and cons of each.

In some cases, institutions have elected to adopt more than one framework. These schools have plotted a security framework approach utilizing more than one of the systems outlined earlier. This is perfectly acceptable, but it is important to note that the institution must clearly map out its security strategy. Ambiguity while juggling more than one framework only sets the stage for failure.

A few institutions have elected to "cherry pick" elements of different frameworks to craft a system to their liking. This hybrid approach can offer more flexibility and functionality. For some institutions, this is clearly the best option. Institutions may cobble together their own framework, based on preferred elements of from those listed here, and might also utilize institution-specific tools, while branding the framework with their own moniker. (For example: University of XYZ Security Framework.) Such an approach has a considerable advantage: branding the framework with the institution's name will, in most cases, increase the likelihood of campus-wide buy-in from stakeholders who might otherwise be hesitant to adopt a framework. There is certainly nothing wrong with this approach—as long as the institution's IT professionals are well aware of which elements will be used. Clearly defining a structure is key to avoid chaos. This hybrid approach requires far more planning and may represent an added level of complexity that some institutions are not equipped to manage.

Regardless of which framework (or combination thereof) is selected, there is an important caveat. Institutions must research each framework for possible conflicts with national, state, or provincial regulations. Such regulations will vary widely, so it is incumbent upon each institution to research possible conflicts before heading down the path toward a particular framework.

Conclusion

Choosing the proper security framework isn't easy. It requires adequate research and buy-in from your institution's decision makers. The five frameworks outlined here provide varying styles and degrees of protection, with differing approaches, but they all seek to accomplish the same goal: rigorously defend the security of information systems from threats that will continue to increase in the coming decades.

Selecting a security framework is critical. Given the escalating threats to higher education—and the potential for catastrophic data loss and damages to a school's reputation—there is no time to equivocate. Institutions operating without a security framework must select one, and do so with great urgency—and they should select one that's flexible and dynamic, able to grow with the institution.

Banner® Data Defense combines multiple layers of IT security defense solutions, including an encryption package for your data and network, firewall, and audit tool, into one solution and offers implementation services to help you ensure data privacy, protect against threats, and maintain regulatory compliance. It's powerful technology, designed to give you peace of mind. Ellucian is committed to keeping data secure with a suite of products—including cloud and hosting services—capable of functioning within most security frameworks.

About Ellucian

Ellucian helps education institutions thrive in an open and dynamic world. We deliver a broad portfolio of technology solutions, developed in collaboration with a global education community, and provide strategic guidance to help education institutions of all kinds navigate change, achieve greater transparency, and drive efficiencies. More than 2,400 institutions in 40 countries around the world look to Ellucian for the ideas and insights that will move education forward, helping people everywhere discover their potential through learning.

To learn more, please visit **www.ellucian.com.**

ellucian

Headquarters: 4375 Fair Lakes Court, Fairfax, Virginia 22033, USA
Phone: +1 800.223.7036

www.ellucian.com