NATIONAL STUDENT CLEARINGHOUSE

CYBERSECURITY REPORT

BROUGHT TO YOU BY:

ZIVARO

BRILLIANCE

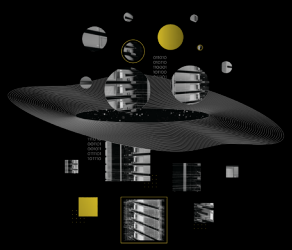
ZIVARO

BRILLIANCE

Zivaro provides industry-leading consulting and technology services that help clients realize real business value from their technology investments. With deep foundations in Hybrid IT, Cybersecurity, Collaboration and Big Data Analytics, we can support you across a broad spectrum of industries with IT strategy, planning, implementation and IT operations.

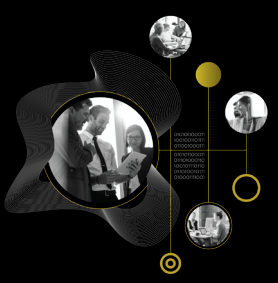
IT MODERNIZATION

SECURITY



CLOUD

INSIGHT



COLLABORATION

ZIVARO

BRILLIANCE

- Owner of Aegis Identity Trident Intellectual Property
- 20 year history of infrastructure management and consulting
- Robust Educational experience in K-12 and Higher Education
- Professional Services to enable success

OVERWATCHID™

- Identity Security Platform Software as a Service Company
- SSO, PAM, CASB, MFA combined in one platform
- Robust access management experience
- Product Management and Development providing product Road-map using updated technology and standards

IDENTITY SECURITY POWERED BY:

OVERWATCHID™ EDUCATION

- RePlatformed TridentHE and TridentK12 product
- Integrated Aegis Identity Education Focused Provisioning/De-Provisioning Engine & SDK

BUILT FOR EDUCATION

Solution Value

- Proven Provisioning/De-provisioning Suite
- New Standards based approach to application integration
- Improved interoperability using modern auth protocols
- Road-map to SaaS Based platform
- Less admin with more customization
- Instant scalability for student population
- Improved data privacy and data security

Organizational Value

- Registrars / Enrollment manager enablement
- Student outcomes focus
- Time Savings
- ID and policy management across platforms
- Scalability

NATIONAL STUDENT CLEARINGHOUSE®

Why Cybersecurity Matters:

and What Registrars, Enrollment Managers and Higher Education Should Do About It

Brought to you in partnership with

EDUCAUSE

REN-ISAC

The purpose of this white paper, jointly written by the National Student Clearinghouse, EDUCAUSE and REN-ISAC, is to build upon registrars', enrollment managers', IT's and higher education's day-to-day, nationwide dialog around cybersecurity and vulnerabilities.

The following insight is based on the Clearinghouse's 25-year record of maintaining the confidentiality and privacy of student records and frequent cybersecurity conversations with registrars, enrollment managers and other institution officials; EDUCAUSE and REN-ISAC's cybersecurity work over many years; and current best practices expressed in two recent major reports. The 2018 EDUCAUSE and Deloitte's Center for Higher Education Excellence report urges improved communication between the IT department and institutional leaders, including board members, to more effectively prevent attacks and recover after a cyber incident occurs. In addition, the 2018 Verizon Data Breach Investigations Report sheds light on what to watch for, what to do, and what not to do.

All of us in higher education have a vested interest in knowing cybersecurity best practices and being empowered to effectively navigate the myriad of cyber security challenges. To help all institutions, it is very clear that registrars and enrollment managers be included as critical players in any institution's cybersecurity team and decision-making conversations. We hope this paper helps elevate cybersecurity on your leadership agenda.

Registrars and enrollment managers have critically important roles to play in securing student data, and third-party services are a major risk.

Is your student data secure?

Why Registrars and Enrollment Managers Need to Care about Cybersecurity

Registrars and enrollment managers play central roles in an institution's cybersecurity posture. **The choices you make each day directly affect student data security.**

Securing data is a big challenge for higher education institutions. Universities and colleges collect a wide variety of personal information about their students, including Social Security numbers, birth dates, financial information, and contact information. Yet there can be a disconnect between that data's primary custodians and the information technology (IT) department that manages the systems on which the information is stored. It is imperative that both the registrar's office and enrollment management office are in lockstep with the IT department with respect to the institution's cybersecurity efforts, to guard against cyber threats.

Why Information Security is a Challenge

According to the 2017 Verizon Data Breach Investigation Report, **state-affiliated actors are targeting educational institutions.**[1] Thus, advanced, organized networks of cyberspies, which are sponsored by other countries, are actively targeting higher education institutions, as a recent FireEye report confirms.[2]

While it's tempting to think the institution's IT department is responsible for protecting and securing student data, cybersecurity is not solely an IT department issue. Registrars and enrollment managers are the business owners of the institution's most sensitive student data. As primary data stewards, **registrars and enrollment managers have an immensely important role to play in ensuring the security of student data.** Coordinating information security practices among all stakeholders is imperative.

A 2018 report from EDUCAUSE and Deloitte's Center for Higher Education Excellence concluded that university leaders need to pay better attention to cybersecurity issues. The report emphasizes that institutional leaders and IT staff need to communicate regularly about cybersecurity issues to prevent attacks, as well as to respond to incidents effectively.[3] A key step for university leaders is gaining a clear understanding of the institution's vulnerabilities and specific data security challenges.

Registrars and Enrollment Managers: Key Members of the Cybersecurity Team

Registrars and enrollment managers make daily decisions that have a direct impact on securing student data. You establish relationships with vendors and partners to manage the vast flow of information under your purview. Choosing third-party service providers for transcript ordering services, for instance, is a good example. If you don't have data security top of mind, you may make a choice that increases your institution's vulnerability.

[1]2017 Data Breach Investigations Report, 10th Edition. Verizon.
[2]https://www.fireeye.com/current-threats/apt-groups.html
[3]https://www2.deloitte.com/insights/us/en/industry/public-sector/cybersecurity-on-higher-education-leadership-agenda.html

What Every Registrar and Enrollment Manager Needs to Know

- The impact of a data breach, and how a breach can happen
- How student data is being secured
- What challenges the IT department faces to secure student data
- What happens if a breach occurs? What aspects of the breach response will the IT department handle, and what will be the responsibilities of the registrar's office and of the enrollment management office?

What Every Registrar and Enrollment Manager Needs to Do

- Meet regularly with your CIO and CISO to formulate incident response plans, risk management plans, and staff training programs
- Establish a strong working relationship with the financial aid administrator on your campus to ensure compliance with Gramm-Leach-Bliley Act (GLBA) information security rules protecting student data
- Regularly involve staff in information security discussions (make it a recurring meeting agenda item)
- Make information security and compliance requirements part of career management planning
- Work with your IT department to implement the suggestions in this document
- Inventory where your data resides and who is using it

How Breaches Happen

43%
were social attacks
(somebody used a social tool, such as email for the attack)[5]

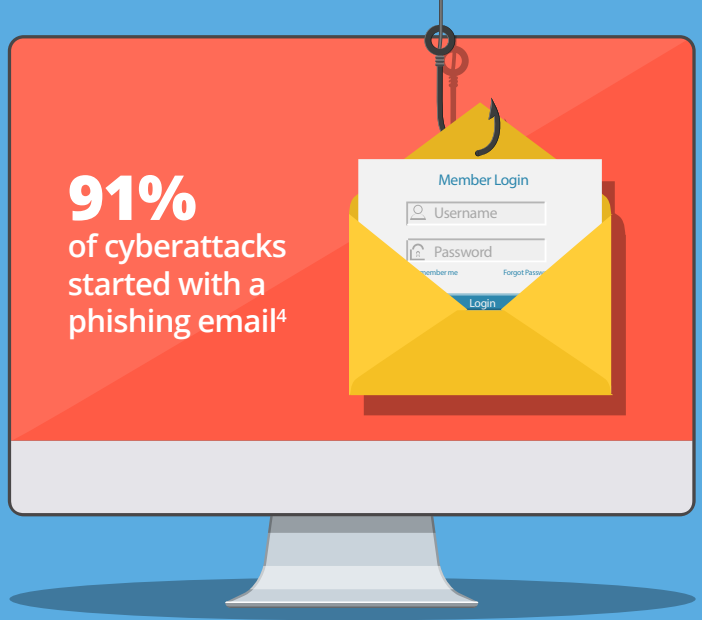
51%
included malware
(somebody installed unauthorized software)[5]

62%
of breaches featured hacking
(somebody attained unauthorized access)[5]

37.6%
of the breaches used desktops as the conduit to compromising data[6]

32.3%
of the breaches used people as a means to compromise data[6]

27%
were discovered by third parties
(somebody outside of the organization informed them that they were breached)[4]



91%
of cyberattacks started with a phishing email[4]

66%
of malware was installed via malicious email attachments[5]

81%
of hacking-related breaches leveraged either stolen and/or weak passwords
(somebody used unauthorized access to steal credentials and then installed unauthorized software)[5]

Cybersecurity Incidents Cost Money, Impact Your Institution's Reputation, and Can Hurt the Students You Serve

Breaches are expensive in many ways. Not only do they exact a financial cost in the millions, but they also harm the institution's reputation and erode trust.

According to a Ponemon Institute assessment, organizations took, on average, 191 days to identify a data breach and 66 days to contain it. The average number of breached records for organizations was 28,512. The average cost of a data breach was $200 per compromised record in the education industry sector. The average total cost of a data breach for an organization across all industry sectors amounts to over $7 million.[7]

Impact on Students

The most important cost to keep in mind is the long-term cost that students face after they have had their personal information stolen. Students trust their institutions to be diligent stewards of their data. Once the organization has been breached, however, there is no real way to make amends. The genie is out of the bottle, and the data is not coming back.

Students affected by cybersecurity breaches face significant short-term inconveniences that can translate to lifelong negative effects if their data is used. Students may have to:

- Change passwords across their accounts
- Request their credit reports
- Establish fraud alerts on their credit files
- Freeze their credit reports
- Dispute fraudulent activity
- Contact financial institutions
- Enroll in identity monitoring services
- Complete police reports
- Submit formal identity theft reports to the Federal Trade Commission (FTC)

The most important cost to keep in mind is the long-term cost that students face after they have had their personal information stolen, which can translate into lifelong negative effects if their data is used.

If a student's identity is stolen as a result of a data breach, that student faces even greater challenges. The student's credit reports could be affected, and student loans might be delayed or canceled. These stressors could have a measurable impact on institution performance.

[4]https://cofense.com/enterprise-phishing-susceptibility-report
[5]2017 Data Breach Investigations Report, 10th Edition. Verizon.
[6]Data Breach Digest. Verizon.
[7]https://www.ponemon.org/library/2017-cost-of-data-breach-study-united-states

Risk in Plain Sight: Third-Party Vendors

In a recent survey, "Data Risk in the Third-Party Ecosystem," the Ponemon Institute[8] found that:

- 56 percent of respondents (of 625 survey responses) confirmed that their organizations experienced a **data breach caused by one of their vendors**, an increase of 7 percent over the previous year.
- 57 percent of respondents said they are **unable to determine if vendors' safeguards and security policies are sufficient** to prevent a data breach.

Beware, **third-party vendors are a significant potential risk to your institution's data security.** A good example of potential third-party vulnerability arises from contracts with companies that market their services to the registrar or enrollment management office, purporting to streamline the office's workload by taking over some process or service. For example, one of the most popular third-party services that registrars outsource is transcript ordering services.

Third-party transcript ordering services appeal to some institutions because they alleviate the burden of receiving and fulfilling transcript requests from students and alumni. Like many things that seem too good to be true, there is a catch. To fulfill transcript orders, some of these services must be ***installed behind the institution's firewall.***

When a third-party vendor is granted access within the institution's IT security protections, the institution's security is in their hands. **Student data is only as secure as that third-party vendor.** If their systems are compromised, cyber criminals, rogue nation-states, and other bad actors have access to a highway running right into the institution's systems. At that point, both student data and the rest of the institution's valuable data is at risk.

If your third-party vendor's systems are compromised, both student data and the rest of the institution's valuable data is at risk.

Questions registrars, enrollment managers and other higher education staff should ask third-party vendors:

- How quickly and often does your organization patch servers?
- How quickly and often does your organization patch endpoints?
- If your organization uses additional third-party services, how do they patch their devices?
- If your organization's devices are hosted within our institution, who is responsible for patching and ensuring patches are kept up-to-date?
- Does your organization use multifactor authentication?
- Does your organization have an incident response plan in place?
- When and how will we be notified of any security incidents?

[8] https://www.ponemon.org/library/data-risk-in-the-third-party-ecosystem

Action steps for registrars, enrollment managers and other higher education staff currently using third-party services:

- Make sure you have strong cybersecurity-related clauses in your third-party agreements. These clauses should include breach notifications that require third parties to notify you if they have a breach.
- Find out whether your third-party providers have had independent security assessments of the services they provide. Require them to send you a copy of that assessment before signing a service contract and every year before renewing.
- Establish third-party agreements that require third parties to notify you when they share your data with any other organization.
- If you use third-party hardware or software behind your firewall, ensure you understand and are satisfied with how the third party validates the security of their product and how often they identify and fix security flaws (known as patching) with their products.

So What Can You Do? Action Steps for Registrars and Enrollment Managers

Although the threat is real, and the associated cost is high, improving your office's security can be done in a few steps. Here are the top recommendations.

1. Pinpoint your risks

The best way to do this is by meeting with your organization's IT department leaders. By partnering with them, you'll gain a clearer understanding of what they are able to do to protect data, and what security steps you are responsible for.

Questions to ask your institution's IT department:

- If we were to experience a breach, where and how would it happen? Where are the weak links?
- How can we resolve these weak links, and who is responsible for resolving them?
- Who or what is accessing our office's data and how?
- How fast are the devices accessing our data being patched? What is the patch rate?
- Are the devices supporting our data missing patches? If yes, why?

- Are all appropriate parts of the student information systems behind a firewall?
- How often are vulnerability scans performed? Who receives the reports and has responsibility for following up?
- What other barriers and challenges does the registrar's office and enrollment management office face in adopting a more secure posture?
- How can we address these barriers and challenges?
- Are there additional security measures recommended for the registrar's office and for the enrollment management office? What are they, and how do we start implementing them?

93% of breaches could have been avoided with basic cyber hygiene. [10]

2. Automate updates at endpoints

Endpoints, defined as any piece of computer hardware with an internet connection,[9] are a common source of vulnerability for an organization.

The Online Trust Alliance found that "93 percent of those breaches could have been avoided with basic cyber hygiene, such as regularly scanning platforms for vulnerabilities and quickly patching them."[10] According to Verizon's 2015 DBIR, "99.9 percent of exploited vulnerabilities were compromised more than a year after the CVE was published."[11] A CVE (common vulnerabilities and exposures) is a list of common identifiers for publicly known cybersecurity vulnerabilities.[12] This means that in almost every instance, a fix was available, but no one patched the device that was eventually compromised.

Setting all devices to update automatically is a simple, straightforward action that will significantly boost security of all endpoints in the registrar's office and the enrollment management office.

3. Be diligent about patching major systems

Student information systems are often large and complex, sometimes highly customized and configured, third-party software. Because of the complexity, customizations, dependencies, and demand for up-time, it's sometimes difficult to apply patches in a timely manner. Ensure that your institution has good patch management processes and critical patches are applied in a timely manner.

4. Implement multifactor authentication

Multifactor authentication (MFA) is a system that relies on more than one layer of security to authenticate a user. In single factor authentication, someone only needs a user ID and password to access data. In MFA, however, a user needs the ID and password, plus an extra authentication step. Often, the extra step is to enter a code sent via text message or generated by an authorized device or application, such as a constantly changing Virtual Private Network (VPN) token. Cybercriminals have become very good at stealing password information, but adding a second factor drastically reduces your risk of a breach.

[9]Endpoints can include desktop computers, laptop computers, tablets, smartphones, and other devices.
[10]https://otalliance.org/system/files/files/initiative/documents/ota_cyber_incident_trends_report_jan2018.pdf
[11]2015 Data Breach Investigations Report, 8th Edition. Verizon.
[12]https://cve.mitre.org

Implement MFA everywhere possible. This includes:

- Vital systems, such as systems that store Social Security numbers, student financial information, or anything that is personally identifying to anybody
- Any server that is publicly accessible, such as the webserver that hosts your web site
- Any device that allows users to access your organization remotely
- Third-party solution providers
- Cloud services
- Programs like remote desktop, Outlook Web Access
- Administrative access to web sites

Average total data breach cost for an organization across all industry sectors is $7+ million.[7]

5. Create an incident response plan

The best time to plan an incident response is before an incident happens. If an incident occurs, the stress of the crisis situation makes it difficult to approach communications strategically and respond appropriately.

Questions to ask:

- If our organization is breached and the breach involves a compromise of student data, what are the registrar's actions? What are enrollment management's actions?
- Do either the registrar's office or the enrollment management office have notification requirements to the organization? To students, faculty and staff? To any federal oversight?
- Once the breach is declared, how soon afterward must we notify faculty, staff, students, alumni, and business partners?

6. Know everyone who has access to your data, how, and why

Talk with your office staff, as well as your institution's IT department, to learn where student data is stored, who has access to the data you safeguard, and how that data is being used. A note on administrative access: the fewer users who are designated "administrators," the better. System administrators are prime targets for hackers and other cybercriminals. The best practice to apply is the principle of least privilege, wherein users can only access the minimum information needed to perform their work. Following this principle, both the registrar and enrollment manager should not have administrative access to institutional data and be a potential source of a breach.

7. Model good security practices and discuss best practices with your staff

Since information security is everyone's job, recognize and reward staff who educate themselves on information security and compliance requirements as they relate to your business function. Talk with your staff about best practices for handling student data, and make those discussions a regular part of your meetings. Think creatively about ways to remind faculty and students about the importance of keeping information safe.

8. Train your users against phishing

According to the 2016 Cofense report, 91 percent of cyberattacks started with a phishing email (legitimate-looking email designed to induce individuals to reveal sensitive information)[5]. Train users on the seriousness of the phishing problem, how to recognize phishing, and to report them. Create an environment that encourages users to report when they've been tricked. Respond quickly to those incidents. And, because phishing defenses are imperfect, be sure to implement the MFA recommendations made above.

9. Plan to have regular security review meetings with the IT department

Maintaining a secure posture requires constant diligence; the risks, threats, and demands are ever-changing. Develop a consistent and regular relationship with the IT department to review and improve your posture.

Conclusion

Cybersecurity should be on every registrar and enrollment manager's radar screen. Taking steps to understand your institution's current security capabilities and securing endpoints are excellent steps.

The question of third-party vendors is even more urgent. If you are using third-party vendors, do you know where your data is stored and how it is being secured? If not, it's time to find out. That is the only way you can fulfill your responsibility as a careful steward of student data.

Additional Resources

Ready to take the next step toward safeguarding your office's student data? The best way to start is by meeting with your institution's IT department and reviewing these additional resources:

- National Student Clearinghouse, Privacy Commitment, https://studentclearinghouse.org/about/our-privacy-commitment/
- Higher Education Information Security Council (HEISC), Information Security Guide: Effective Practices and Solutions for Higher Education (EDUCAUSE), https://spaces.at.internet2.edu/display/2014infosecurityguide/Home
- Higher Education Information Security Council (HEISC), Information Security Program Assessment Tool (EDUCAUSE), https://library.educause.edu/resources/2015/11/information-security-program-assessment-tool
- Higher Education Information Security Council (HEISC), Higher Education Cloud Vendor Assessment Tool (EDUCAUSE), https://library.educause.edu/resources/2016/10/higher-education-cloud-vendor-assessment-tool
- EDUCAUSE Center for Analysis and Research (ECAR) Research Paper, "Technology in Higher Education: Information Security Leadership", https://library.educause.edu/resources/2016/3/technology-in-higher-education-information-security-leadership
- EDUCAUSE and Deloitte's Center for Higher Education Excellence Report: Elevating Cybersecurity on the Higher Education Leadership Agenda, https://www2.deloitte.com/insights/us/en/industry/public-sector/cybersecurity-on-higher-education-leadership-agenda.html

NATIONAL STUDENT CLEARINGHOUSE®

2300 Dulles Station Boulevard, Suite 220
Herndon, VA 20171

studentclearinghouse.org

ZIVARO

BRILLIANCE

Todd Olson
VP of Sales
tolson@zivaro.com
303-594-5703
OverwatchID.Zivaro.com