

Winter

NONPROFIT NEWSLETTER



NON - PROFIT!

CONTENTS

- Triaging Data Breaches: Part Two 2 - 5
- Tax Exempt & Government Entities Division Releases 2022 Program Letter 6 - 8
- Top Considerations for the Nonprofit Sector: Part Two 9 - 10
- Thinking Ahead: How Colleges & Universities Can Plan for Long-Term Success 11 - 12
- Other Items to Note 13



Triaging Data Breaches: Part Two

By Mark Antalík

In [Part One](#) of this two-part data breach triage series, we discussed identifying, understanding and communicating during a breach situation and how breaches should be managed. In this article, we will elaborate on perpetuation through digital forensics, as well as outline approaches to notification and identity monitoring. As discussed in Part One of this series, a well-designed breach response program that addresses the steps noted below will minimize the negative impact on both short and long-term business goals.

Steps Addressed in Part One of Article Series:

1. **Identify, Understand and Communicate** – processes to identify the potential threat, gain an understanding of the threat and its potential impact, and communicate with the appropriate agencies and other involved or impacted parties.
2. **Respond and Contain** – responses and efforts to contain or limit data breaches can have significant impacts on an organization's ability to recover from the incident.

Steps Addressed in Part Two of Article Series

1. **Perpetuation** – preservation of evidence will assist in remediating the current breach and may aid in identifying future attempted breaches.
2. **Notification and Identity Monitoring** – through internal or third-party services, affected parties can be notified of any activity related to their personal information and efforts to remediate and reduce potential impact.

Let's discuss perpetuation, and notification and identity monitoring in detail.

Perpetuation

Preservation of key information and evidence during and after a breach is vital to understanding the nature and scope of the incident. Organizations that actively deploy endpoint and network monitoring are better positioned to identify suspicious activity and contain the breach. Organizations that are not currently deploying such technology and processes are not only at greater risk of breach, but will find it more difficult to understand the nature and scope of the breach should one occur.

Many organizations already employ threat intelligence technology and teams to understand and mitigate data risk. However, once an incident occurs, cyber forensics teams need to dig deeper into the incident including gathering technical clues and indicators of the compromise. Gathering this data will help to identify both the nature and scope of the breach.

Understanding the nature of the breach is important so the breach can be contained and measures can be implemented to prevent similar attacks in the future. From a technical perspective, this may involve analyzing IP addresses, file names and hash values to inform further data investigations. The goal is to identify operational details about the motivation of the threat actors; uncover the tools, techniques and procedures used to infiltrate the system or environment; and gain strategic intelligence to evaluate the overarching risks associated with the incident.

As the cyber forensics team is gathering information about the nature of the breach, it needs to simultaneously identify the scope of the breach. Understanding what data may have been accessed or exfiltrated is often not an exact science. There are many technical layers and, only when combined with knowledge of the nature of the breach, can the potentially exfiltrated dataset truly be assessed. Organizations must collect, analyze and correlate both the data and the facts. Knowledge of the entire potentially exfiltrated dataset is critical to informing the required disclosures and notifications and to determining the scope and risk of intellectual property and other sensitive data loss.

Knowledge of the entire potentially exfiltrated dataset is critical to informing the required disclosures and notifications and to determining the scope and risk of intellectual property and other sensitive data loss.

As discussed in Part One of the article series, having a plan in place prior to the breach will provide explicit guidance for response resources, reduce emotional conflicts in tense breach situations, and demonstrate to clients, donors, and volunteers that your organization is in control of the situation and is concerned about protecting personal information. Having a business continuity plan provides situational awareness and decision-making support during the chaos of a crisis to get your organization back up and running as quickly as possible.

Notification and Identity Monitoring

There are several types of breach-related notifications. Compliance-related notifications include notifications to state, federal and global regulators; notifications to

FIVE IMPORTANT DATA BREACH TRENDS



Cyberattacks and security breaches will occur and will negatively impact the business.



According to most cybersecurity surveys, **over 60% of all data breaches originate from unauthorized access** from one of the organization's current or former employees, or third-party suppliers.



Achieving information security compliance with one or more government regulatory standards for information security (i.e., ISO 27001, NIST 800-171, HIPAA, NYDFS, etc.) is good, but not sufficient to holistically address cybersecurity.



Cyber liability insurance premiums are significantly increasing in cost and often do not cover all the damages caused by a cyber breach.



To achieve real information and data resilience, it is vital to **combine managed Monitoring, Detection and Response Managed Security Services with comprehensive disaster recovery (DR) and business continuity plans.**

impacted entities and individuals; and notifications to roles such as the organization's Data Protection Officer. Other notifications may include law enforcement, the board, stockholders, business partners and company executives – the degree to which these notifications occur will depend on the organization and the nature and/or scope of the breach.

From a jurisdictional regulatory impact perspective, consider building a map to visualize the exposure, plotting impacted entities and individuals (based on the information learned while investigating the nature and scope of the breach) to determine if there are any concentrations of impact that would suggest prioritizing notifications in particular jurisdictions. Domestic organizations are often surprised that they maintain data for individuals in the European Union, Asia Pacific or Latin America regions and identifying and visualizing this exposure can accelerate the notification process given how fast breach response situations move.

As the master notification list is being compiled, organizations need to identify notification letter requirements. Considerations include grouping notification content by region and data categories, defining the necessary notification letter template elements, identifying language/translation needs, determining call center and credit monitoring logistics and determining distribution method(s) for the notifications. An important aspect of notification is establishing a regulatory metrics report. The report documents jurisdictions, number and type of notifications, response rates and any exceptions identified during the process. These reports are critical to demonstrate regulatory due diligence and tracking through the notification process.

For instances requiring organizations to provide individuals with access to credit reports, along with individual credit monitoring tools, it is also important to have experienced professionals that are licensed to investigate credit issues.

Depending on the scope of the breach, a call center may be required to address stakeholder questions and issues, and comply with regulations. Call centers should be staffed with trained professionals with experience protecting sensitive data. Call center staff should follow

defined data handling procedures to maintain the security of any personal information logged during call center interactions. Consider developing training kits including scripts and FAQs. Consider call center logistics, physical security, local language requirements, staff management and scale. Consider the potential importance of industry experience for call center operators, potential to deploy offshore options and tracking of key performance indicators. Data breach call centers are typically established and maintained for 12-18 months following the incident. To mitigate the number of complaints to regulators, establish procedures to address and diffuse escalated situations.

Be prepared for additional breach requirements related to individual and consumer rights afforded by data protection regulations such as the European Union's General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA) and the Virginia Consumer Data Protection Act (CDPA). In summary, and not exhaustive, these regulations empower individuals to make requests such as a request to delete the individual's data, show the individual what data the organization stores about them or request that the organization correct the individual's data if there are inaccuracies. Under these regulations, organizations typically have 30 – 45 days (differs by regulation) to fulfill these requests. Many other states and global jurisdictions are in the process of enacting individual rights requirements beyond typical breach response obligations.

Individual rights requests often spike after a data incident, from a few per month, to potentially hundreds or thousands post breach. Right-sizing and scaling a process to address these individual rights can be challenging. Processes need to be set up to address the intake of the requests, verification that the individual is who they purport to be, coordination of the requests, research to identify the information requested, consolidation of data/information into template responses, review and dissemination of the data or information back to the individual and tracking every step in the process. Depending on the size and complexity of the organization, the individual rights response process can be resource intensive and time consuming. Consider exploring and deploying data protection software that can help automate parts of the individual rights request process.

Depending on the nature and scope of the breach, having a team to support the investigation into lost identity or impacted credit may be required. Identity monitoring services must be able to investigate compromised sensitive data like Social Security numbers, country IDs and medical information, while monitoring for personally identifiable information and protected health information on the dark web. Qualified fraud examiners can assist with restoring credit and applying appropriate protections moving forward. For instances requiring organizations to provide individuals with access to credit reports, along with individual credit monitoring tools, it is also important to have experienced professionals that are licensed to investigate credit issues.

As noted in Part One of this article series, a breach can be a real test of resiliency. Organizations must plan for a breach and be clear and transparent to clients,

Organizations who meet the crisis head on may be able to emerge stronger, be better prepared for the next incident and build a closer connection with their constituencies.

donors, volunteers and other third parties about how the organization collects, uses, stores, shares, protects and disposes of sensitive and personal data. Organizations who meet the crisis head on may be able to emerge stronger, be better prepared for the next incident and build a closer connection with their constituencies.

• • • •

CASE STUDY



BACKGROUND AND CHALLENGES

A large global organization experienced a massive data breach from a network intrusion spanning several months resulting in potential exfiltration of hundreds of terabytes of personal information, intellectual property and other sensitive data.



APPROACH

BDO delivered comprehensive incident response services, including identifying suspected exfiltrated data; categorizing data to determine national and international notification requirements; extracting entity information and compiling a master notification list; hosting and reviewing data; and proving additional intelligence to the client and its counsel regarding downstream data privacy and security regulatory requirements.



IMPACT

Through a combination of robotic process automation, data analytics and proprietary data triage workflows, BDO rapidly analyzed terabytes of source data, consolidated data elements, and extracted and normalized individual and entity information to generate an initial master notification list prior to any human document review. This technology-driven approach provided rapid insight into the nature and scope of the data and notification obligations, enabling the client and its counsel to make informed decisions regarding prioritization and risk.



Tax Exempt & Government Entities Division Releases 2022 Program Letter

By Jake Cook, CPA

The IRS Tax Exempt and Government Entities division released its fiscal year 2022 Program Letter on October 7, 2021, summarizing its plans for the upcoming year. The Program Letter addresses the division's projects and priorities for fiscal year 2022 for tax-exempt organizations, employee benefit plans, Indian tribal government and tax-exempt bonds.

The TE/GE division provides taxpayers assistance to properly file and pay their taxes while also enforcing the tax laws to maintain fairness for all.

The division reports that fiscal year 2022 will be a year of growth and change. TE/GE plans to invest in new resources to expand outreach to the tax-exempt sector and to increase their enforcement staff to balance their obligation to serve taxpayers as well as enforce the tax

laws. For nearly a decade, the TE/GE division's workforce has declined annually. New employees hired under the growth plan in fiscal year 2022 will focus on enforcement duties.

Insight

The hiring of new TE/GE agents focused on enforcement may mean that tax-exempt organizations could expect an increase in compliance audits and reviews. During these audits and reviews, taxpayers should be patient with the new agents.

The hiring of new TE/GE agents focused on enforcement may mean that tax-exempt organizations could expect an increase in compliance audits and reviews. During these audits and reviews, taxpayers should be patient with the new agents.

The TE/GE division plans to continue its efforts to create a user-friendly experience for the tax-exempt community. For example, it will continue to build on its 2021 investment in a new Chief Tax Experience Officer and the opening of the Taxpayer Experience Office, with a focus

on multilingual assistance, increased digital services, proactive outreach and advanced data analytics. It will be more important than ever to focus on the accuracy of filings, as selection for compliance audits and reviews will continue to become more data-driven than random sampling.

The TE/GE division works to carry out its plans while striving to improve efficiency and modernize processes to best utilize government resources. The new Program Letter focuses on the following actions for the upcoming year.

Strengthen Compliance Activities

Compliance strategies are issues approved by the TE/GE's Compliance Governance Board to identify, prioritize and allocate resources within the TE/GE filing population. The current priorities are:

- **Collaborate across the IRS on existing and emerging issues** – The focus will be on syndicated conservation easements, abusive charitable remainder trusts, ESOPs, COVID-related employer credits and continued review of potentially abusive promoter schemes with an impact on TE/GE.
- **Support examinations of high-income taxpayers with TE/GE issues** – The focus will include private foundations and the creation of a joint audit process in cooperation with the IRS Large Business and International and Small Business and Self-Employed divisions.
- **Partner with IRS Criminal Investigation and Research Applied Analytics & Statistics** – The focus is to identify cases with potentially significant noncompliance.

Improve Operational Efficiencies

As noted previously, the IRS is striving to improve efficiency by incorporating the following steps:

- **Review systems and processes** – The goal is to improve internal controls and performance measures and to continue to streamline enforcement-related procedures.
- **Support Enterprise Case Management efforts** – This will be accomplished by analyzing processes across TE/GE. The IRS currently has over 60 case management systems that it is working to combine into one system. This will provide the IRS with a more

The TE/GE division works to carry out its plans while striving to improve efficiency and modernize processes to best utilize government resources. The new Program Letter focuses on the following actions for the upcoming year.

comprehensive and timely view of each organization's account information, which should lead to quicker resolutions.

- **Explore, create, and refine opportunities and avenues** – The goal is to leverage diverse perspectives and insights to inform and enhance processes, enforcement activities and the taxpayer experience.

Maintain a Taxpayer-Focused Organization

The IRS is focused on assisting organizations with compliance through the following actions:

- **Collaborate with the Taxpayer Experience Office** – Expand outreach to the TE/GE community and create positive experiences for taxpayers in every interaction while helping taxpayers understand and meet their tax responsibilities.
- **Promote the e-filing of forms** – This would include Forms 1024 and 8038-CP as well as other exempt organization returns.
- **Develop online resources** – To promote online access to publicly disclosable filings.

Ensure Awareness and Collective Understanding

The IRS is striving to make changes and emphasize the collaborative nature of its relationship with taxpayers by:

- **Proactively communicating with the communities served** – Designed to encourage compliance with tax laws through expanded outreach, such as the TE/GE Small Entity Compliance Initiative.
- **Strengthening stakeholder partnerships** – Ensure the identification, development and delivery of effective messages.
- **Increasing the use of cross-functional teams** – To address business change initiatives.

Leverage Technology and Data Analytics

As many other organizations, the IRS is focusing on the utilization of technology and data analytics to:

- **Detect emerging issues using data analytics**
- **Launch taxpayer digital communications capabilities and use robotic process automation** – Utilize this to make processes more efficient and effective for organizations.
- **Improve access to, and use of, digitalized data** – Utilize data to identify issues with a high risk for noncompliance.
- **Leverage publicly available data** – Utilize this to streamline and automate the process for identifying the universe of hospitals subject to Affordable Care Act review.

The IRS is striving to make changes and emphasize the collaborative nature of its relationship with taxpayers.

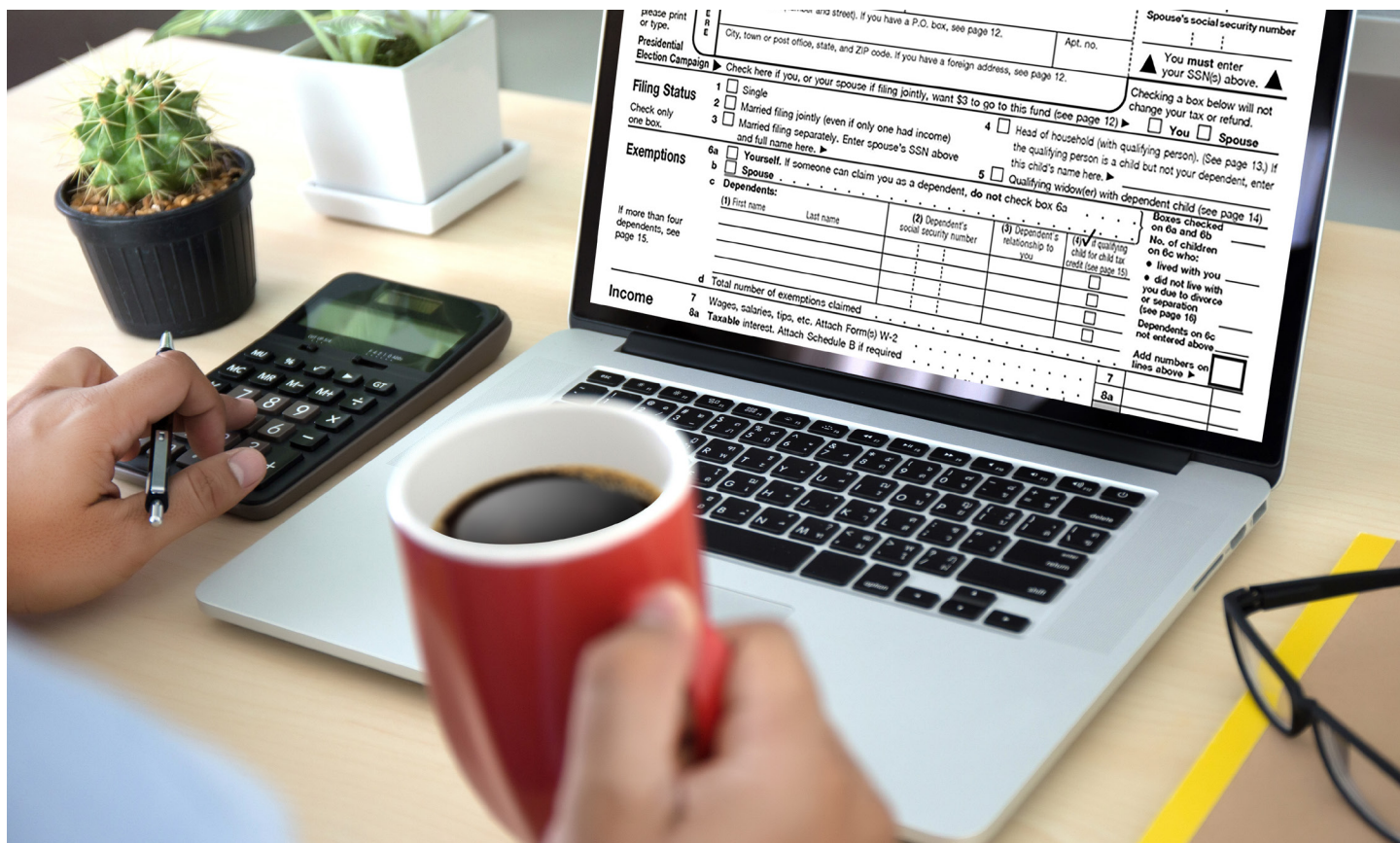
Develop IRS Workforce

To address past labor shortages, the Program Letter lists the following action plans:

- **Develop a recruitment and hiring strategy** – Focused on identifying, hiring and retaining TE/GE employees to improve responsiveness and efficiency.
- **Assess IRS employees' training needs** – Expand the skills of IRS employees to create a more flexible and well-trained workforce.
- **Enhance employee and manager development** – This will be accomplished through training, developmental assignments, coaching and mentoring.

Management at exempt organizations should be aware of the role the TE/GE division plays, consider the potential implications the plans outlined in the Program Letter may have on their organizations and consult with their tax advisors as necessary.

• • • •





Top Considerations for the Nonprofit Sector: Part Two

By Divya Gadre, CPA

Many nonprofits are dealing with the uncertainty of the ongoing pandemic as well as increased demand for their services. It's a delicate balancing act, but with proper systems and support, nonprofits are up for the challenge. The [first article](#) of this two-part series covered how the sector has benefited from COVID-19 relief funds, along with best practices for complying with new accounting standards, safeguarding against cyberattacks in a hybrid or fully remote working environment, automating manual processes for greater efficiency, and implementing a successful diversity, equity and inclusion (DEI) strategy.

In this second part of the article series, we highlight five additional considerations for nonprofits around succession planning, funding volatility, remote management and leadership, planning for disruption and change management.

1. Succession Planning

Each employee plays an integral role in your nonprofit's operations. An effective succession plan reflects this and will prepare your nonprofit for the departure of your chief executive officer as thoroughly as it would for the departure of your office manager.

A comprehensive succession plan is designed to ensure business continuity in the face of expected and unexpected departures alike. It focuses on retaining employees by offering opportunities for advancement to promising staff members and includes training initiatives to minimize the learning curve for new hires. It is important for nonprofit leadership to be transparent about the details of the succession plan and review the plan annually or semi-annually to confirm it addresses the latest needs and developments.

This should be discussed with the board as well and appropriately communicated to other stakeholders. During the pandemic, many organizations practiced and thrived with this approach and didn't think of it as a sensitive topic. Succession planning should be part of scenario planning and risk management planning.

2. Funding Volatility

From canceled events to shifts in donor behavior to stock market fluctuations, it's easy to see why funding volatility has become a challenge for many nonprofits. It's important to gain a clear understanding of your current funding mix, explore opportunities to enhance what's working well and consider discontinuing what isn't. This assessment will enable the organization to identify new programs that may offer more funding diversification to offset volatility.

As you consider new opportunities, you should review cash, accounts receivable and accounts payable daily. It's also important to maintain adequate operating reserves, create a cash forecasting model, develop and adopt a risk tolerance statement that defines

financial stability targets, and calculate key financial metrics for continuous monitoring.

3. Remote Management and Leadership

The pandemic has introduced hybrid and fully remote work models to many organizations, expanding nonprofits' pool of job candidates and offering existing employees greater flexibility. That said, remote work can come with challenges of its own. Lack of in-person and spontaneous interactions can exacerbate [existing information silos](#), as well as feelings of loneliness in already isolated employees. Managers may find it difficult to oversee operations in a remote environment, and employees may find the blur between professional and home life draining.

Fortunately, there are several steps nonprofits can take to make remote work more comfortable and productive for all parties. Most importantly, lead with empathy. An empathetic leadership style inspires employee loyalty, especially in this time of imposed social isolation and uncertainty. Consider scheduling regular one-on-one videoconferences where employees can share any personal concerns and professional progress. Additionally, reiterating praise in organization-wide videoconferences and taking every opportunity to encourage employee collaboration is important. By fostering a sense of community, you can help boost employee morale and reignite passion for your nonprofit's mission. While you can lead with a personal touch, note that it's also important to establish clear boundaries between personal and professional lives. For example, try to refrain from sending employees emails outside of business hours. After all, there's a fine line between working from home and living at work.

4. Planning for Disruption

Disruption is to be expected, but it doesn't have to throw your operation into a tailspin. You can plan for disruption by utilizing the following best practices:

- Engage in clear and honest communication with all stakeholders.
- Make informed decisions quickly and stand by them.
- Reward collaboration over competition by remaining open to employee feedback.
- Leverage technology to disseminate timely and accurate information to all levels of the organization.
- Start scenario planning and determine how you might react to a variety of contingencies.
- Take stock of what worked and what didn't in your response to previous crises.
- Establish a culture that blends structure with agility.
- Establish clear documentation on succession planning. Establish a playbook that clearly documents who is responsible for what when a cyberattack happens. (See related article, "Triaging Data Breaches" on page 1)

These steps will help your nonprofit adjust to dynamic conditions without losing sight of or the ability to achieve your mission.

5. Change Management

Change is hard. In fact, according to [Harvard Business Review](#), 78% of change management projects are unsuccessful. A variety of factors contribute to this bleak statistic, but many change management initiatives fail to align with corporate culture due to improperly defined objectives and poor project management. It can be especially challenging to explore operational changes without employee buy-in, as a nonprofit's staff is the heart of the organization. But be tactful—too much change at once can cause staff to lose momentum and confidence in the organization.

Impactful change requires clear communication as well as an obvious link between transformation and reward. Employees embrace change when they understand why it's happening, even if they disagree with it. You should also be sure to communicate how their roles will be impacted, so there aren't any surprises down the line. Create systems for measuring progress, hire employees who offer fresh perspectives and celebrate small wins to get everyone on board with your evolution. By linking transformation to realistic goals and rewards for your organization and its people, staff can feel more connected to the end results and be proud of the work involved.

There are many factors that nonprofits must consider as they look ahead. We've identified 10 through this two-part article series. Though these considerations may be daunting, a common thread runs through all best practices: Know where your nonprofit stands and strive to adapt to a changing environment through contingency planning, effective leadership and agile forecasting models.

• • • •



Thinking Ahead: How Colleges & Universities Can Plan for Long-Term Success

By LaShaun King

When considering how they should position their institutions over the long term, leaders of higher education institutions are accustomed to a familiar refrain.

The recurring questions they hear are:

- What trends are evident in enrollment and retention rates over time?
- How tuition-dependent is the institution?
- What is the institution's tuition discount rate, and how well is it monitored?
- What is the size of the institution's endowment, and is growth in line with the overall market?
- How much does the institution rely on debt financing for operations (outside of large capital projects)?

While financial health and viability remain important indicators of an institution's long-term success, another factor is growing in importance and intersecting with the above metrics: changes in student demographics. In order to plan for the future student body, educators and administrators must remain aware of these trends.

The Evolving Student Body

The Western Interstate Commission for Higher Education (WICHE) released [updated projections](#) in December 2020 for high school graduates. The study notes that students of color are making up a growing share of high school graduating classes. In 2019, white students were 51% of

high school graduating classes. They will decrease to 46% of the Class of 2025 and 43% of the Class of 2036. For those higher education institutions that have not yet enrolled significant numbers of students of color, determining how to attract and retain these students may raise new questions: How well do institutions understand the needs of such students? Do students of color feel welcome within the campus environment? Many students of color who are currently underrepresented in higher education need financial assistance. How can institutions that have relied on increasing enrollment to fill budget gaps find other ways to fund themselves in order to continue fulfilling their mission?

Independent students are an additional layer in the changing demographics. Per the Institute for Women's Policy Research (IWPR), approximately 51% of all U.S. higher education students were defined as independent, or having at least one of the following defining characteristics per the Free Application for Federal Student Aid (FAFSA):

- Being at least 24 years old
- Married
- A graduate or professional student
- A veteran

- An orphan, in foster care or ward of the court
- A member of the armed forces
- An emancipated minor
- Someone who is homeless or at risk of becoming homeless
- Someone with legal dependents other than a spouse

The [IWPR's 2018 paper](#) noted that 55% of women and 46% of men enrolled in higher education institutions are independent students. Per the IWPR paper, these students have a median age of 29, are mostly students of color, are likely to be a parent, have limited ability to pay for their education and are more likely to enroll part-time when compared to dependent students. COVID-19 has caused further strains—as noted in a [May 2021 article by Higher Ed Dive](#), the pandemic has increased stressors for independent students who are parents, particularly younger parents.

Facing the Future of Higher Education

So how can higher education institutions position themselves for success in the long term given changing student demographics? There are a couple of steps that leaders of higher education institutions can take now for future implementation in their strategic plans:

Assessing Enrollment Strategies to Increase Inclusion

Institutions should determine the changes necessary to enrollment strategies to attract students of color as well as independent students. Understand how such data will be collected, monitored and tracked going forward.

Some institutions have placed a direct emphasis on addressing increasing demographic changes, such as John Hopkins University, which developed its initial “Roadmap on Diversity and Inclusion” in 2016 and publishes annual progress reports.

The university also recently moved to permanent need-blind admissions, which resulted in its student population of underrepresented racial minority students growing from 14.9% in 2010 to 32.5% in 2019. Similarly, the University of Minnesota has staff members dedicated to recruiting students of color and uses direct marketing and recruiting tactics to increase representation of Black students specifically. Other institutions waived requiring SAT or ACT scores from applicants due to the ongoing

pandemic, and saw a surge of applications for the Fall 2020 and 2021 academic years — including an increase in applications from underrepresented student groups.

Other schools are partnering with community colleges to improve the pipeline of transfers from two-year institutions to those granting four-year degrees. While many state public institutions have already established these types of relationships, many private institutions are establishing these relationships for the first time in recent years. One example is in Ohio, where the Council of Independent Colleges has helped facilitate a program that allows students from 10 community colleges in the state to take classes following a specified pathway and transfer to one of 14 private institutions in Ohio to complete their degree without any loss of credits. These types of pathways support independent students, 44% of whom attend community college.

Reconsider the Campus Environment

Considering how the institution can make its own campus experience more welcoming and supportive of students of color and independent students is key to attracting and retaining those students.

John Hopkins University previously established an Office of Institutional Equity and an Office of Diversity & Inclusion to address both the on-campus experience for students from underrepresented populations as well as diversity within faculty. Loyola University Maryland has a President's Council for Diversity, Equity and Inclusion that monitors and supports university-wide initiatives alongside student and alumni boards.

As noted by the IWPR, institutions should also consider whether its part-time students have access to student support services (including the hours that such services are offered) and its existing financial aid policies, and whether they could be adjusted in ways that allow independent students to access more aid and potentially decrease work hours.

While there is no single strategy that will lead higher education institutions to long-term success, addressing the evolution of the student body is a good place to start. Taking active steps to make sure your organization is prepared to serve current and future students is a key move toward ensuring longevity.

• • • •



Other Items to Note

FASB Issues ASU 2021-09, Leases (Topic 842): Discount Rate for Lessees That Are Not Public Business Entities

On Nov. 11, 2021, the Financial Accounting Standards Board (FASB) released Accounting Standards Update (ASU) 2021-09 entitled, "Leases (Topic 842): Discount Rate for Lessees That Are Not Public Business Entities." This ASU covers all lessees who are not public business entities which includes private companies, not-for-profit organizations (whether or not they are conduit bond obligors) and employee benefit plans.

Topic 842 currently provides lessees that are not public business entities with a practical expedient that allows them to make an accounting policy election to use a risk-free rate as the discount rate for all leases. This practical expedient was provided to relieve those lessees from the cost and complexity of having to calculate an incremental borrowing rate. Private company stakeholders noted that using a risk-free discount rate (for example, a U.S. Treasury rate) is low compared with the expected average incremental borrowing rate and could increase the entity's lease liabilities and right-of-use assets recorded upon adoption of Topic 842 on the statement of financial position. FASB has addressed these concerns with the issuance of ASU 2021-09.

Under ASU 2021-09, lessees that are not public business entities will be able to make the risk-free rate election by class of underlying asset, rather than at the entity-wide level. An entity making this election will be required to disclose which asset classes it has elected to apply a risk-free rate.

The ASU does require that when the rate implicit in the lease is readily determinable for any individual lease, the lessee use that rate, rather than a risk-free rate or an incremental borrowing rate, regardless of whether it has made the risk-free rate election.

The effective date of ASU 2021-09 depends on whether or not the entity has adopted Topic 842 yet. If an entity has not adopted Topic 842 as of Nov. 11, 2021, it is required to adopt the ASU at the same time as it adopts Topic 842 using the existing transition provisions.

If an entity has already adopted Topic 842 in its financial statements as of Nov. 11, 2021, the provisions of this ASU are effective for fiscal years beginning after Dec. 15, 2021. Earlier application is permitted. These entities are required to apply the provisions of this ASU on a modified retrospective basis to leases that exist at the beginning of the fiscal year of adoption.

• • • •



For additional information regarding any article, please contact [Chris Hatcher](#), [Mark Cotter](#), or [Myron Fisher](#) via email or at 1.866.287.9604.

OFFICE LOCATIONS

114 N. Main Cross St., Flemingsburg, KY 41041

1019 Majestic Dr., Suite 370, Lexington, KY 40513

116 Sutton St., Maysville, KY 41056

713 W. Main St., Richmond, KY 40475

10180 Linn Station Rd., Suite A200

Louisville, KY 40223

