2026 DRU Cybersecurity Roundtable

May 13, 2026

Findings and insights from an educational and networking event hosted by the Disaster Resilient Universities (DRU) Network, Deloitte, and the University of Oregon

Executive Summary and Event Overview

On May 13, 2026, the 2026 DRU Cybersecurity Roundtable was held at the Deloitte office in Tempe, Arizona. The invitation-only roundtable convened senior leaders in enterprise risk management, emergency management, IT and information security from institutions of higher education (IHEs) across the country to identify and discuss ways that IHEs can enhance mitigation, preparedness, response, and recovery from cyberattacks. It featured a presentation and detailed analysis of trends in cybersecurity response challenges, as well as a case study workshop, facilitated peer-to-peer discussions, and networking.

The Disaster Resilient Universities (DRU) Advisory Committee, in collaboration with partners at Deloitte, URIMA, EDUCAUSE, IAEM-UCC, NACUBO and others, selected the invitees. The final group included participants from Lehigh University, Southern Methodist University, Arizona State University, California State University, University of Massachusetts, Carnegie Mellon University, University of Illinois, Portland State University, University of Oregon and Washington State University, as well as an editor from HigherEdRisk magazine.

This project was supported by a generous gift from Deloitte & Touche LLP (Deloitte). Points of view or opinions in this document are those of the authors.

About the DRU Network

The DRU Network has an online platform for communication, coordination, and collaboration among more than 1800 members representing approximately 800 institutions of higher education (IHEs). Its goals are to:

- Facilitate professional, peer-to-peer communication among members to help campuses mitigate, prepare for, respond to, operate during, and recover from natural disasters, acts of terrorism, or other crises or disasters.
- Provide post-secondary risk and safety administrators and practitioners ways to share research, studies, strategy documents, technical papers, process evaluations, and lessons learned.

Why the DRU Organized This Event

Cybersecurity poses a substantial risk to higher education institutions, and there's more to learn about how IHE executive teams can detect and manage cyberattacks.

Many IHEs have chief information security officers (CISOs), IT disaster recovery managers, and cybersecurity operations centers to monitor and respond to security incidents. However, the extent to which these individuals and groups are integrated with campus risk management, enterprise risk management, emergency managers, communications teams, and campus law enforcement remains unclear. This could lead to a siloed approach, even though budget constraints and escalating threats require IHEs to be efficient and resilient.

Accordingly, the objectives of the event were to:

- Identify areas where IHEs need more alignment to collaborate, prevent, prepare for, respond to, and recover from cyberattacks.
- Create a whitepaper/facilitator guide that contains a detailed list of questions, tactics and strategies that help IHEs prepare for and coordinate better during and after a cyberattack.

The Event

Top 5 Cybersecurity trends

During the event, Carlos Amaya, U.S. Cyber Principal at Deloitte, presented an overview of the current state of cyberattacks on IHEs. There are three notable trends.

1. **Cyberattack threats are intensifying**. The sophistication, the volume, and the intensity of threat actors coming after, disrupting, denying access to, or stealing data from IHEs are all rising.

2. **The attack surface is expanding.** First, IHEs had firewalls and perimeters. Then came the cloud, IoT, contracts that grant access to systems, AI agents, and similar technologies. These all increase the complexity – and sometimes the vulnerability – of IHE systems.

3. **The chief information security officer (CISO) scope is broadening.** The role has evolved from technician to strategist who determines priorities and decides how to secure missions and assets. In general, more chief information officers are being promoted to CISO and even CEO, reflecting the role's growing importance. Where that role has more maturity, the risk and security-resilience culture tends to be better. Higher education CISOs are navigating a threat environment that is broader, faster-moving, and more complex than ever, and it demands a shift from reactive defense to proactive institutional leadership.

For IHEs, these trends are presenting a variety of additional hurdles. Amaya also highlighted five of the most critical ones.

1. **Cybersecurity is now a campus-wide leadership challenge.** At the executive level, there's an understanding that cybersecurity has become a human capital and risk-management issue. Having a cybersecurity steering committee that includes people from outside of the

IHE's IT department can help nurture this understanding. Additionally, many IHEs are familiar with the National Institute of Standards and Technology (NIST) but may feel they have no control over certain aspects of their cyber landscape (such as privacy or ownership). Without proper governance, implementing adequate cybersecurity controls is hard. Furthermore, software vendors often tell IHEs that their products are easy to deploy. Still, the related governance, access, removal triggers, privacy limits, and other factors often make things more complicated and require input from finance, HR, legal and other teams – another reason IHE cybersecurity steering committees must have representation from beyond IT.

2. **Ransomware remains the dominant operational risk.** For threat actors, ransomware is low-hanging fruit, and IHEs often have security vulnerabilities that have existed for years and haven't been patched. Ransomware is present in 44% of all breaches, according to a recent Verizon Data Breach Investigations report. Recovery pressure and data sensitivities make IHEs prime targets for attacks. Plus, threat actors are now able to create exploits without having to know how to write code, making cyberattacks easier to create.

3. **Third-party and supply chain risk is rising fast.** Third-party involvement in breaches doubled to 30% in 2025. SaaS, edtech vendors, and other partners have become primary attack vectors, making it more important than ever for IHEs to identify and classify their critical service providers.

4. **AI is now a governance problem and an opportunity.** Campus leaders should understand their IHEs' AI risk appetites, and whether any departments within their IHEs have different risk appetites. IHEs should identify the stakeholders who benefit from AI and identify how to help those stakeholders use AI without creating unmitigated risk. AI is also an opportunity to build cybersecurity capabilities. For example, IHEs are adopting more agentic capabilities to stay ahead of threats, which is important – threat actors can now identify an IHE's vulnerabilities in just hours or minutes instead of months or years.

5. **Talent shortages are constraining the agenda.** Heavy workloads, understaffing, and reduced training budgets are forcing IHEs to focus on keeping the lights rather than modernizing their infrastructures or proactively reducing risk. CISOs are now expected to lead strategy and execution in addition to managing technology. CISOs are often peers with chief resilience officers. Tabletop exercises may include both the CISO and the chief risk officer, and it's not unusual for a CISO to report to a chief risk officer (though many report to the CIO).

Heard in the room: "We're lucky to have a CISO at our IHE, but a challenge with enterprise risk management and emergency management is that the senior leadership doesn't understand the scope of what we deal with in cyber. They focus on fires, active shooters, etc. Most of it is tangible stuff. When there's a change of administration, the CISO qualities are important, but the new people are usually focused on other stuff, while CISOs are trying to put parameters around

the new stuff. The CISO sometimes operates in a bubble. When an attack occurs, they have to remember to bring the CISO in, and then they don't know what the CISO is talking about."

The presentation also highlighted three IHE-specific sources of friction that CISOs, Enterprise Risk Managers, Emergency Managers, Risk Managers and other teams are facing in their efforts to thwart cyberattacks.

Friction point #1: Turnover. Frequent changes in leadership (presidents, provosts, deans, athletic directors, etc.) means that many people don't really know what each other's duties are, and often they don't have access to each other's job descriptions. Understanding and documenting roles and responsibilities is important for mitigating risk and responding effectively to cyberattacks.

Friction point #2: Silos. CIOs who don't understand how Emergency Managers or Enterprise Risk Managers can help or support them may find themselves acting as a go-between among various teams and departments during and after a cyberattack. IHEs can mitigate this potential bottleneck by inviting CISOs into emergency operations centers (EOCs) and reinforcing the importance of coordination and documentation, as well as the idea that managing technology is only one part of the response to a cyberattack. IHEs can involve CISOs in continuity planning and broader decision-making to nurture working relationships.

Friction point #3: New and/or overlooked risks. Roundtable participants mentioned a number of other growing concerns around cyberattacks, including:

- The advent of quantum computing and its potential downstream effects, such as the ability to unencrypt data.
- Dependency on a single AI platform that could one day be hacked or misused.
- Deferred maintenance, which can ignore existing vulnerabilities.
- Uncertainty about ways to measure the true price of cyberattacks at IHEs, beyond the cost of insurance premiums.
- Pressure to demonstrate the value of risk mitigation and prove that the absence of breaches is due to those mitigation efforts.
- Difficulty mapping IHE risk exposure, including likelihood, cost of events, and operational impact.

Case Study Workshop & Exercises

In this part of the event, attendees presented and discussed a variety of their own real-world experiences. They shared how various situations created different challenges for their enterprise risk teams and emergency management teams. These discussions are summarized here in a way that preserves confidentiality and respects anonymity.

The situations and challenges that the IHEs faced fell into four topical areas.

Ownership challenges

Some participants whose IHEs experienced cyberattacks reported difficulties identifying who was supposed to handle specific areas of the response and recovery efforts. Specifically, they experienced:

- Confusion about who "owns" the management of the event, which incident response teams to involve, and whether and when the school's CISO is supposed to lead or follow.
- Uncertainty about whether and when to activate the IHE's emergency operations center (EOC).
- Inconsistent decisions about the frequency of, platform for, or nature of communications and messaging to students or campus communities.
- Disagreement about how many people to involve in managing the incident and how to balance inclusion with decision-making speed.
- Lack of awareness about who has the authority to shut down specific campus-wide technologies or platforms.
- Unclear action plans for improvement, including lack of clarity about who has the authority to assign improvement tasks and what's permitted in terms of holding assignees accountable for completing those tasks.
- Failure to hold staff and faculty accountable for not completing cybersecurity training.

Incident management struggles

Several participants described execution-related challenges that ended up slowing down or overcomplicating their response or recovery efforts after a cyberattack, including:

- Lack of plans and/or tools needed to switch quickly to analog systems for processing payroll, monitoring building access, managing class attendance, and other necessities.
- Failure to anticipate or prepare for the downstream effects of shutting off certain platforms or features, such as keycard access, HVAC systems, water treatment, or wifi.
- Disagreement about whether cyberattacks should be classified as continuity incidents or emergency management incidents, which can change the nature of the response.
- Inconsistent expectations, disorganization, or lack of follow-through regarding when to contact third parties, such as insurance carriers, outside counsel, forensic services, recovery operations, etc.
- Reluctance to enforce policies requiring researchers to house their research data and information on protected school networks rather than on vulnerable private networks.
- Disorganized after-action reporting processes, including uncertainty about who is supposed to create the reports and who should receive the reports.

Stresses of concurrent or subsequent events

Many roundtable participants mentioned that cyberattacks rarely happened in a vacuum – other response or recovery activities were often also happening at the same time, which affected how teams triaged events and how long things took. In particular, participants said they struggled with:

- Resource constraints due to management of other incidents.

- Fraudulent activity, particularly with “ghost students” using fake or stolen identities to apply for student loans, or with hackers using student credentials to change the direct deposit accounts for financial aid refunds.
- Whether to establish stricter admissions and registration processes to thwart fraud.
- Anticipating and preparing for media coverage of the event, including phishing attempts that may occur due to publicity.

Legal and insurance concerns

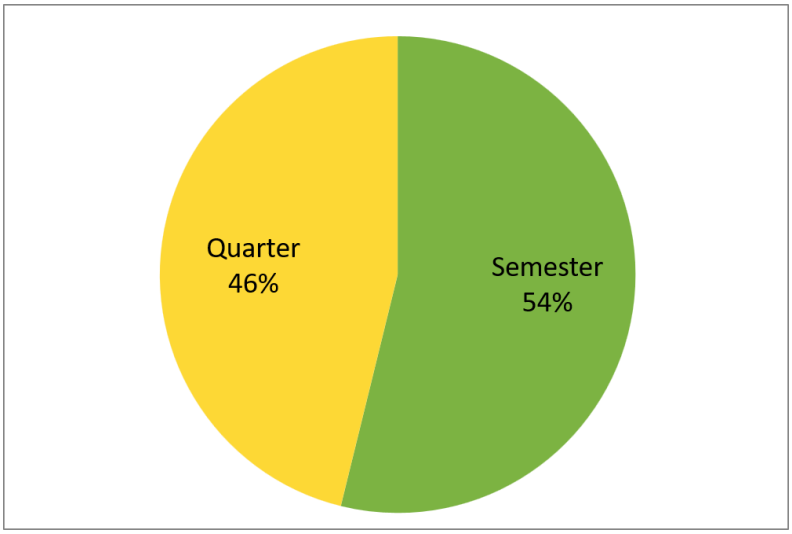
Although legal and insurance matters are a fundamental part of most cyberattack response and recovery efforts, participants experienced a variety of hurdles in this area, including:

- Contracts that were outdated, confusing, or hard to locate.
- Confusion about which laws, contracts, or requirements applied, or about who should interpret the laws, contracts, and other requirements around breach notification or cyberinsurance.
- Concerns about whether and how to use identity-verification programs to mitigate future risk.
- Uncertainty about who the IHE can or should indemnify.
- Mistaken assumptions about what cyber insurance pays for, which in turn affected subsequent decisions about whether to spend money on updating the IHE’s infrastructure or on more insurance.
- Mistaken assumptions about what constitutes legally privileged conversation at the IHE.

Canvas survey response data

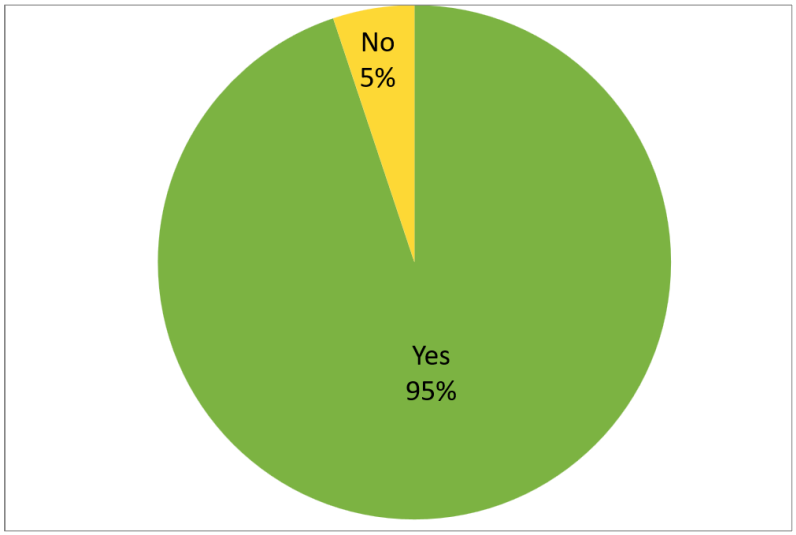
Earlier this year, the Disaster Resilient Universities (DRU) Network partnered with the University of Oregon – Safety and Risk Services to develop and administer the DRU 2026 National Higher Education Cybersecurity Survey. The DRU conducted the anonymous online survey of IHEs regarding their experience with and response to the May 2026 Canvas security incident. The 10-question survey ran from June 2 to June 16, 2026, and collected 42 responses. Survey funding support came from the University of Oregon and a financial gift from Deloitte Government and Public Services Practice to the DRU Network.

Is your institution on a semester or quarter academic calendar?



The survey results highlight the widespread disruption caused by the recent Canvas outage, with virtually all responding institutions reporting that they were directly impacted.

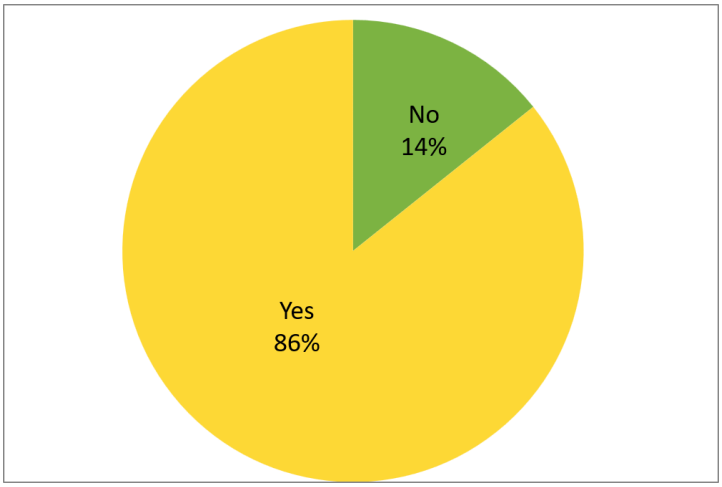
Was your institution impacted by the Canvas incident?



Leadership during the crisis primarily fell on Chief Information Officers (CIOs) and Chief Information Security Officers (CISOs), with IT and information security departments serving as the lead operational units.

Despite having established IT leadership—as evidenced by 86% of institutions maintaining a dedicated CISO—the incident exposed significant vulnerabilities in coordination between technical teams and the broader academic community during a critical operational period.

Does your institution have a CISO (Chief Information Security Officer)?

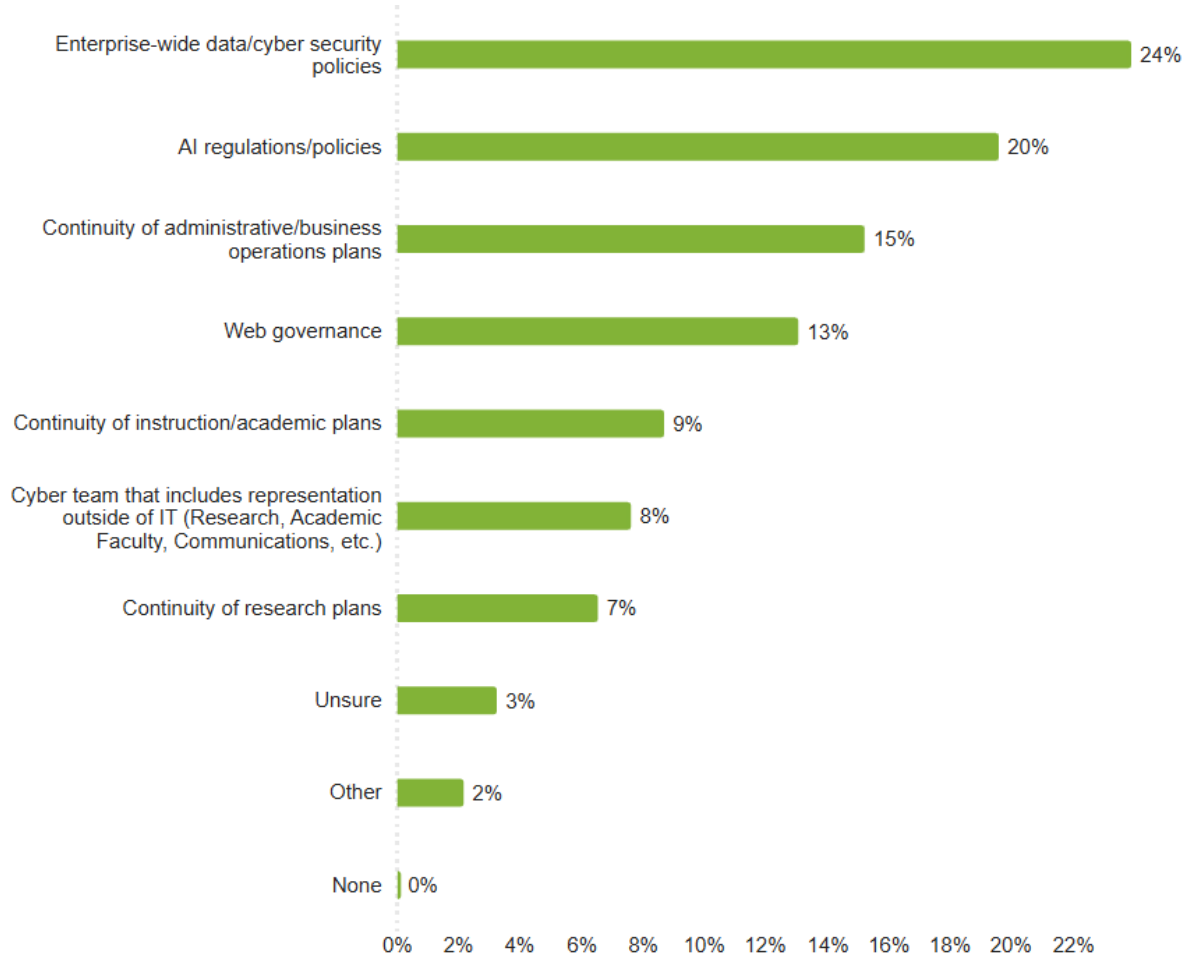


Respondents identified core challenges around pervasive communication breakdowns and a lack of formalized academic continuity planning. Internally, institutions struggled with:

- Disjointed public messaging
- Slow or non-existent updates to faculty and students
- A failure to integrate the response into existing campus Emergency Management systems (such as Emergency Operations Centers).

Externally, respondents expressed deep frustration with the vendor, Instructure, citing poor communication, limited transparency, and uncertainty regarding data recovery timelines. These issues compounded operational anxieties, particularly for accelerated programs and campuses facing immediate deadlines for final grading and exam scheduling.

Does your institution have any of the following components integrating cyber threat/response/security?

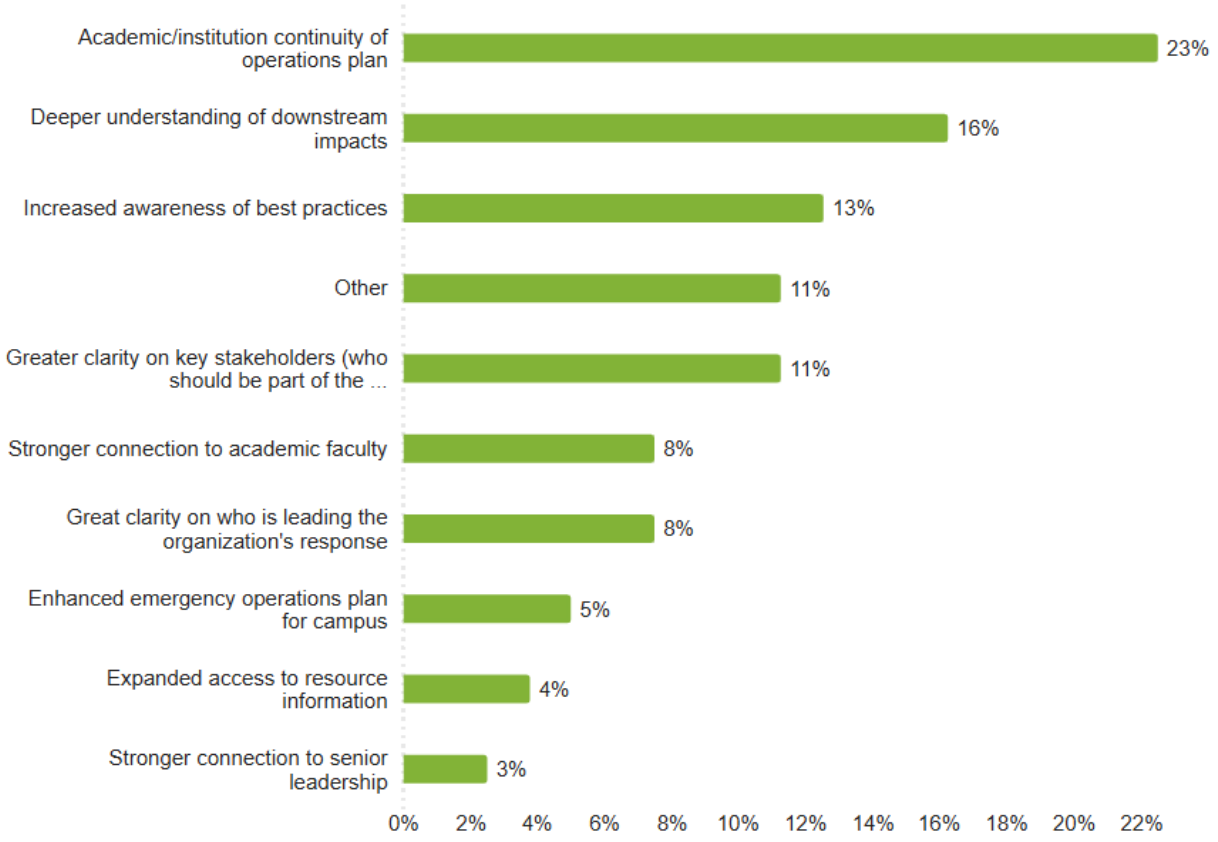


To strengthen future resilience against cybersecurity and system incidents, respondents strongly advocated for formalized operational frameworks and clearer organizational integration. The most requested resources to improve future responses were:

- Academic/institutional continuity of operations plans (23%)
- A deeper understanding of downstream impacts (16%)
- Increased awareness of best practices (13%)

Furthermore, qualitative feedback underscored an urgent need to treat cyber incidents with the same protocol as physical hazards, requiring a cultural shift in which IT professionals actively participate in established campus crisis management structures rather than managing outages in isolation.

Which three resources would most strengthen your institution's ability to provide an effective response to a cybersecurity incident?


Academic/institution continuity of operations plan
23%
Deeper understanding of downstream impacts
16%
Increased awareness of best practices
13%
Other
11%
Greater clarity on key stakeholders (who should be part of the ...
11%
Stronger connection to academic faculty
8%
Great clarity on who is leading the organization's response
8%
Enhanced emergency operations plan for campus
5%
Expanded access to resource information
4%
Stronger connection to senior leadership
3%
0%
2%
4%
6%
8%
10%
12%
14%
16%
18%
20%
22%