Make tough decisions easier.
When leaders want to make decisions faster, smarter, and with more confidence, Jenzabar Analytics is the easy answer.

Program Economics - How do we optimize offerings for today’s students?

Student Success - How do we get more students to completion?

Financial Health - Do our instructional methods achieve our mission?

Enrollment - How many students do we need to enroll next year?

Jenzabar Analytics is a portfolio of descriptive, diagnostic, and predictive analytics tools that give you the strategic insight you need to increase agility, improve performance, and identify new avenues for success. Learn more at jenzabar1.com/analyticsEDRev

Jenzabar One is a flexible, cloud-ready platform exclusive to higher education. Our powerful suite of technology products and services provides your campus with mobile-friendly solutions for both institutional and student success.

©2019 Jenzabar, Inc. All rights reserved. Jenzabar® is a registered trademark of Jenzabar, Inc. The Jenzabar logo is a trademark of Jenzabar, Inc.
The Human Nature of Cybersecurity
Jessica Barker
By understanding cognitive biases and shortcuts, we can better engage people to improve cybersecurity awareness, behavior, and culture.

Creating a Cybersecurity Strategy for Higher Education
Don Welch
Cyberattacks on higher education are increasingly frequent and damaging. Meeting the challenge, especially in higher education, requires strategic thinking, and that strategy must come from cybersecurity-specific strategic thinking.

Vince Kelten
Today’s designers of data analytics systems are using thirty-year-old mental models around scarcity of compute and are thus crippling their designs, not fully realizing how radically different 21st-century analytics has become.
COLUMNS

5 Homepage
[From the President]
Analytics, Interrupted
John O’Brien

8 Leadership
[Views from the Top]
The Internal Auditor as a Trusted Resource:
An Interview with Justin Noble
Justin Noble and John O’Brien

40 Connections
[Community College Insights]
Using AI to Help Students Learn “How to College”
Dawn Medley

42 E-Content
[All Things Digital]
Monica McCormick

44 New Horizons
[The Technologies Ahead]
Proactive Security versus Surveillance?
Tina Thorstenson

46 Viewpoints
[Today’s Hot Topics]
A Strategic Leader for Student Success:
An Argument for the Chief Academic Technology Officer
Helen Y. Chu and Bill Hogue

48 The Data
[Trending Numbers]
Spring Cleaning: Security and Privacy

Looking for more?

Information Security Guide: Effective Practices and Solutions for Higher Education

Elevating Cybersecurity on the Higher Education Leadership Agenda
By Tiffany Dosey Fishman, Cole Clark, and Joanna Lyn Grama

Security Matters, an EDUCAUSE Review blog:
“Everything related to information security, privacy, and risk in higher education”
https://er.educause.edu/columns/security-matters

The Yin and Yang of Security and Privacy
By Valerie M. Vogel and Joanna Lyn Grama

Volume 54, Number 2. EDUCAUSE Review (ISSN: 1527-6619) is published quarterly (4 issues per year) by EDUCAUSE, 282 Century Place, Suite 5000, Louisville, CO 80027. Subscriptions are available at $54 per year ($84 per year outside North America) and to all academic libraries (North America and international) at $54 per year. Single copies are available for $11 each. Periodicals postage paid at Boulder, CO, and additional mailing offices. POSTMASTER: send address changes to EDUCAUSE, 282 Century Place, Suite 5000, Louisville, CO 80027.

Publications Mail Agreement #40033384
Return Undeliverable Canadian Addresses to:
Station A, PO Box 54
Windsor, ON N9A 6J5
e-mail: info@educause.edu

Cover: Ann Cutting, © 2019
Self-Service DISPENSING KIOSKS

- Space-Saving
- Experience-Enhancing
- Forever-Flexibility

Break Down Barriers and Join 100+ Campuses In Making Laptops Anytime Automated Dispensing Kiosks Your Go-To Self-Service Solution for On-the-Go Students.

Dispense Wide Range of Dell, HP, Lenovo & Apple Laptops and 110V Portable Power Chargers and Accessories.


For More Info Go To: ChargersAnytime.com
A New Innovative Approach To Student Battery Access

OVER 2.5 MILLION ANNUAL CHECKOUTS AND GROWING
2,500,000

Trusted Technology Branded to Your Local Look-n-Feel

LAPTOPS ANYTIME
Automated Checkout Kiosks

1-877-836-3727 • LaptopsAnytime.com
Great tech support powers great education.

Fast, flexible support tools help you meet the diverse needs of your students and faculty. Transform your help desk with:

- Secure multi-platform support
- Remote support in 20 seconds or less
- Seamless integration into any workflow

Learn more at logmeinrescue.com/higher-ed
n March, I attended the American Council on Education (ACE) annual conference, with a primary audience of presidents, chancellors, provosts, deans, and other college and university leaders. It was impossible to miss the degree to which data and analytics had captured the attendees’ imagination. Clearly, when it comes to comprehending and confronting the most challenging issues in higher education in 2019, the effective use of data and analytics is an important, though not the only, part of the solution.

I was not surprised when ACE President Ted Mitchell brought up the topic of data and analytics in a panel on “digital transformation.” But I was surprised to see how often the thread appeared not only in sessions but also before and after sessions in discussions among colleagues about the wide-ranging role that data and analytics can play in areas from student success to race relations to food insecurity.

Anyone listening to these conversations of higher education leaders from around the world might walk away with the impression that there is a uniform sense of urgency about the need for increased use of data and analytics and might also be equally convinced that this work is moving forward briskly. However, EDUCAUSE research paints a different picture, suggesting that analytics progress is more stalled than striding forward. At our current deployment rate, we might even fall short of the EDUCAUSE prediction, made in 2016, that we will see mainstream adoption of business performance analytics and learning analytics by 2019–21. In fact, in the EDUCAUSE Review article “Moving the Red Queen Forward” (an apt reference to Alice in Wonderland and the Red Queen’s reference to a world where running quickly leaves you staying in the same place), Eden Dahlstrom cited the EDUCAUSE capability index for analytics—a collection of 32 data points embedded into the Core Data Service survey—to gauge the degree to which the work has matured.

In 2012, she noted, the composite maturity rating was 3.2 out of 5. In 2014, the composite rating “inched ahead” to 3.4, and it then remained flat for 2015. In 2016, the rating fell back to 3.3 before moving forward to 3.5 in 2018.

Why the lack of forward momentum? In his EDUCAUSE Review article “Changing Demographics and Digital Transformation,” Ted Mitchell pointed to ACE research: “In the 2017 ACE survey of US college and university presidents,

Continued on page 7
LOOK WHO’S USING EDUCAUSE ON CAMPUS

When your institution joins EDUCAUSE, everyone gets access to our vast collection of resources—from IT leaders to help desk staff to teaching and learning professionals—and everyone in between.

Learn more at educause.edu/join
Continued from page 5

only 12 percent regarded institutional research and information technology as important areas of strategic development going forward.”" This lack of buy-in from the top undoubtedly contributes to the lag we are experiencing. In this issue (Spring 2019) of EDUCAUSE Review, Vince Kellen convincingly tackles another possible reason for our hobbled progress: the need to rethink our fundamental models. There are certainly a range of explanations for the challenges involved. Even mainstream newspaper headlines about higher education funding problems and intense concerns about data privacy, data security, and data control point the way to issues that have become more concerning in the last few years.

The criticality of data and analytics features prominently in the 2019 EDUCAUSE Top 10 IT Issues report, with half of the Top 10 issues directly involving data.1 The work is tactical, technical, strategic, and sometimes political—and silos abound where real collaboration is needed. For example, “stakeholders must agree on data definitions and definitive, trusted sources. They must acknowledge the precedence of the institution over the department if the goal is to become a data-enabled institution.” And of course, “the most difficult work is cultural.” Talent development is also key to progress, and institutions that have already attracted or are committed to attracting employees with these collaborative skills will have the best chance of forward progress.

With the breadth and depth of the challenges to fully realizing the promise of using data and analytics, there is no simple answer to nudging the Red Queen forward. However, if one thing is clear, it’s the fact that collaboration is key. With this fact in mind, three higher education associations have joined forces to advance the application of data and analytics and to model the kind of team approach that will help these projects succeed. The National Association of College and University Business Officers (NACUBO), the Association for Institutional Research (AIR), and EDUCAUSE are working together to produce a draft statement on analytics, with the hope of re-energizing data and analytics work across all of our communities and campuses.

This statement promises (1) to make the case for using data and analytics, (2) to create a sense of urgency and opportunity, and (3) to point the way with recommendations. Data and analytics have proven traction when it comes to student success.2 Examples abound, including a recent one reported at the 2019 SXSW EDU conference: “UT Austin had a goal of increasing its four-year graduation rate from 52% in 2012 to 70%. Last year, it nearly reached that goal with a rate of 69.8%. New approaches to analyzing student data, such as predictive analytics, [were] key to that improvement, according to the university.”

Our focus with this joint analytics statement comes at a time when EDUCAUSE is also working hard to advance digital transformation (Dx). The two efforts are mutually supportive and perhaps even inextricably interdependent. Digital transformation involves moving from ad hoc to systematic technology innovation—powered by data and analytics. At EDUCAUSE, we hope that by working together with NACUBO and AIR, we can invigorate the Dx conversation while also reinvigorating the data and analytics conversation, bringing in more campus leaders and coming together to move the Red Queen decidedly forward. ■

Notes
3. Jamie Reeves and Leslie Pearlman, Digital Capabilities in Higher Education, 2016: Analytics, ECAR research report (Louisville, CO: EDUCAUSE, September 2017). While a few of the index prompts changed somewhat in 2018, we believe the equivalent composite rating would amount to 3.5/5.

John O’Brien (jobrien@educause.edu) is President and CEO of EDUCAUSE.

© 2019 John O’Brien. The text of this article is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License.
The Internal Auditor as a Trusted Resource: An Interview with Justin Noble

Justin Noble is a Certified Internal Auditor and is Assistant Chief Audit Executive for the Texas Tech University System, where he leads a staff of eight auditors in conducting compliance, operational, financial, and fraud reviews across the system’s four component institutions. In addition, he is the current President of the Association of College and University Auditors (ACUA), an international professional organization composed of audit, risk, and compliance professionals. Founded in 1958, ACUA serves more than 500 higher education institutions, including schools of all sizes, from community colleges to large university systems, and both public and private institutions. The association strives to assist its members in continually improving the internal operations and processes of the individual institutions they serve.

John O’Brien: How is auditing perceived by IT leaders? How do you want your profession to be perceived?
Justin Noble: Internal audit often suffers from a perception problem. Some leaders see internal auditors as glorified accountants who simply make sure the cash balances each day. Others stereotype internal auditors as boring, tedious, and inflexible number-crunchers who are nitpicky and out to find faults with people’s work. In this view, we are a “police force” that will catch you messing up and air your dirty laundry to anyone who will listen. Of course, high-functioning internal audit departments want none of these monikers to define them.

Internal audit, as defined by the Institute of Internal Auditors, “is an independent, objective assurance and consulting activity designed to add value and improve an organization’s operations.” There are many words in this definition that I believe are key to highlighting how internal audit departments should operate: independent, objective, designed, add value, and improve. Internal auditors want to partner with institutional leaders, including IT leaders, to bring an independent set of eyes to operations and ensure that everything is happening as expected and as designed. We want to assist technology leaders in understanding and managing their risks, controls, and governance processes. We want to walk alongside them to add value to whatever project or process we are evaluating in order to improve the overall objective under review. In short, internal auditors want to be a trusted resource: we want IT leaders to know that they can partner with us to be sure that operational, compliance, and governance risks are being managed.

O’Brien: What’s the difference between an internal audit, a co-sourced audit, and an external audit?
Noble: Internal auditors are on the institution’s payroll. We are campus staff members. Co-sourced and external auditors are vendors who are either procured or assigned, by outside entities, to review the institution. I tell people all the time that as an internal auditor, I have as my goal to never leave the institution worse off than it was to begin with. Why would I want to harm my employer and, in my own case, an institution from which I have received two degrees? I simply do not. That is not to say that I won’t adhere to my professional standards and outline the real issues, but I am not out to justify my salary through my audit work and public reports. By contrast, co-sourced or external auditors, like most other vendors, are pressured to validate the fees they charge and the results they bring. They do have an institution’s well-being at heart, but they also have a different set of pressures around the value they deliver.

O’Brien: How important are the relationships you develop prior to an auditing engagement?
Noble: Relationships are critical in all phases of an audit but even more so prior to the engagement. For any internal audit shop to be successful, an effective risk-gathering process must be employed. To effectively gather risk, internal auditors must have a trusted relationship with leadership to talk about strategies, process, programs, and forthcoming changes. If IT leaders do not trust their auditors—or if they feel that by talking to auditors, they could be disclosing information that will trigger an unwanted audit—they might decide not to reveal critical operational or system changes. By withholding this information, leaders are hampering a complete look at the organization’s risk profile and could send the auditors down a path of wasting critical time and resources. To mitigate this, leaders in both areas (audit
and technology) should be proactive in investing time to get to know each other and build a trust-based relationship outside of the normal audit process. There is simply no substitute for establishing a relationship prior to starting auditing engagements.

**O’Brien:** What else will help to achieve a successful auditing engagement?

**Noble:** While some might say this depends on the engagement itself, I would argue that all effective engagements have certain qualities. First, they are done in an independent and objective manner. This means that the audit team brought a fresh outlook not tainted by senior leadership or public perception. Regardless of what others think, the objective evidence obtained provides the story of how a certain process is working. Second, effective engagements align with risk. There is always something that could be reviewed, but if the work being performed has no bearing or consequence, then why do we care if it is working as designed or not? The most effective audits are ones in which the auditors can clearly articulate the risk being reviewed and mitigated. Third, successful engagements align with the broader set of stakeholders’ needs. Each area under review has stakeholders both inside the department and across campus. Effective audits understand the audience they are trying to inform and influence and seek to ensure that all stakeholders are considered throughout the engagement. Lastly, the results of effective auditing engagements can be supported and trusted. Management (whether technology leadership, campus leadership, or the institutional board) should be able to rely on the results to make decisions. While it is true that auditors are often asked for their opinion, this opinion should be based on the informed insight they have gained throughout their reviews. The most effective auditors are the ones who can intersect successful engagements with informed insights.

**O’Brien:** What are “audits from hell” like? How can they be avoided?

**Noble:** Audits from hell usually start from one of three places: misaligned objectives, ineffective communication, and/or mistrust. The internal auditor needs management’s buy-in to ensure that employees will be forthcoming with information and requests. If management distrusts or does not understand the objectives of the review, the engagement can quickly spiral into a mess. Additionally, if management seeks to “end run” the audit by telling employees how to answer questions or by telling them to intentionally give auditors “only what they ask for,” the communication between the teams will dissolve into distrust. Internal auditors are trained to recognize signs of distrust and untruthful communications and will seek even more information to ensure that other issues are not residing below the surface and that the information they have been provided is accurate. I believe that all of these problems—and the audit from hell—can be avoided by aligning objectives, communicating effectively, and trusting the other party.

**O’Brien:** How should IT leaders prepare for an audit?

**Noble:** An audit, by its nature, is disruptive. Believe me, we understand this. Auditors get audited too. IT leaders should prepare by engaging with the audit team early and often. They should be forthcoming about current issues or the status of an implementation. They should be honest about where things are already struggling or where a second set of eyes might be able to assist. Since most audit shops have a stakeholder visibility that IT leaders might not have, this could be a good opportunity for leaders to raise issues or concerns to a higher level. IT leaders should view internal auditors as a value-add, not a disruption. On the other hand, if a leader thinks an audit is being disruptive, he/she should be willing to speak up (respectfully, of course) to raise the concern. Most internal audit teams want to come alongside leaders and their teams to assist them in their risk-management activities.

**O’Brien:** How can building stronger governance systems help with risk and compliance?

**Noble:** Strong governance systems are essential to the effective management of risk and compliance. I dare say that every auditor could tell story after story in which the root cause of almost all issues, especially fraud issues, was ineffective governance. Building robust governance systems—that is, building stronger policies, processes, and informal and formal structures to assist the organization in achieving and protecting its goals—is essential for the organization to reliably manage its risks. Solid governance systems naturally produce risk-management practices, including compliance with our long lists of laws and regulations in higher education.

**O’Brien:** Where can we learn more?

**Noble:** ACUA provides in-person training twice a year, through our conferences, for members to gain both high-level and in-depth IT expertise. Additionally, ACUA offers listserv and webinar opportunities to complement more timely knowledge-sharing. Joining higher education audit experts with industry experts (e.g., EDUCAUSE members), the association focuses on training auditors for the specific environments they will face as higher education internal auditors.


Justin Noble (Justin.Noble@ttu.edu) is President of the Association of College and University Auditors (ACUA) and is Assistant Chief Audit Executive for the Texas Tech University System. John O’Brien (jobrien@educause.edu) is President and CEO of EDUCAUSE.

© 2019 Justin Noble and John O’Brien. The text of this article is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License.
THE HUMAN
NATURE OF CYBERSECURITY

By Jessica Barker
Looking to behavioral economics, psychology, sociology, neuroscience, and other fields, we can understand cognitive biases and how we can better engage people to improve cybersecurity awareness, behavior, and culture. Scientists in these fields have studied human perceptions and behavior: How do we think, and why do we behave the way we do? We need to take lessons from these disciplines and apply them to how we can best communicate about, and raise awareness of, cybersecurity. The problem is that we can raise awareness around an issue without positively influencing behaviors. Awareness of cybersecurity is high now and has been for a couple of years. But that doesn’t mean that people are behaving the way we would like regarding matters such as password authentication and social engineering attacks.

We need to consider ways that we can better communicate about cybersecurity. For me, this involves understanding how people think. When we are communicating messages to people, how are they receiving our messages, and how are they reacting? A lot of this involves understanding what is known in psychology as heuristics, or “shortcuts in the brain,” which have a significant influence over how people behave. These are ways of thinking, ways of making a decision, that we are not necessarily aware of. But to get through our day of making decisions, we all rely on these ways of thinking, these shortcuts in the brain. When it comes to raising awareness about cybersecurity, I believe that five of these heuristics are particularly relevant: social proof; the optimism bias; the psychology of fear; the stereotype threat; and self-efficacy.

Social Proof

When people don’t know how to act, they assume the behavior of others. Most of us are familiar with social proof, even if we might not know its name in the field of psychology. For example, TripAdvisor, Google reviews, Airbnb, and similar websites show what other people think about something. If you see that 90 people have given a service or product a four- or a five-star review, you’re more likely to give the service or product a try. That’s social proof, and it’s very powerful. Recent research has shown that when about 25 percent of a group start behaving in the same way, most of the other 75 percent of the people in that group will follow the behavior of the 25 percent. We think other people might know better.

The influence of social proof on behavior has been explored in many disciplines, including environmentalism and the attempt to tackle climate change. For example, some research has looked at hotels and the extent to which hotel guests will reuse their towels. Most people don’t reuse their towels; they want a new, fresh towel every day. This results in a large cost for the environment overall. Researchers investigated whether they could influence, by using social proof, the extent to which people reuse towels. In hotel bathrooms they put signs that said: “Most people in this hotel reuse their towel to help save the environment. Will you please do the same?” The researchers found that people who saw these signs were more likely to reuse their towel. Next, to see if they could make the social proof even more persuasive, researchers tried another sign that said: “The last person who stayed in this hotel room reused the towel. Will you do the same to help save the environment?” This was the most persuasive message of all. When we feel we can relate to someone, we are most influenced by social proof.

Yet the use of social proof has not been explored in the area of cybersecurity. Instead, we may be inadvertently using social proof against ourselves. Most of the messaging...
We need to consider ways that we can better communicate about cybersecurity. This involves understanding how people think.
around cybersecurity and behavior is very negative. When we tell people, “Here’s a list of really bad passwords that most people are using,” individuals think, “Everyone else has a bad password, so it can’t be that important for me to have a good one.”

How can we get social proof on the side of cybersecurity communications and awareness raising? One simple example is phishing simulation exercises. When an exercise is over, what message do you put out? Do you say that 30 percent clicked on the link (bad!), or do you say that 70 percent did not click on the link (good!). It is more effective to promote the number of people who did not click the link than the number who did. Next time, join your colleagues in being part of the majority. If we want to encourage people to practice more secure behaviors online, we need to start highlighting the positive behaviors of others.

The Optimism Bias

People underestimate the likelihood of bad things happening in their future and overestimate the likelihood of good things happening. Most people are optimistic. Research conducted by a team of neuroscientists over the last ten years found that about 80 percent of people are wired toward being optimistic. No matter what messages or what facts we give people, they remain optimistic.

For example, researchers conducted a study in which people were asked how likely they thought it was that they would get a disease such as cancer. When individuals replied that they thought they had a 10 percent chance of getting cancer throughout their lifetime, the researchers told them the facts: they had about a 30 percent chance of developing cancer. Nevertheless, the study participants were reluctant to let go of their optimism: the average response then was, “OK, maybe I have an 11 percent chance.”

In the area of cybersecurity, no matter what facts we give people and no matter how much we tell them where hacks have happened, how likely they are to be hacked, and the harmful influence a hack will have, people are going to retain their optimism. When cybersecurity professionals are faced with a nontechnical person who displays this kind of stubborn optimism, they usually respond with more facts. Someone might say: “Why would hackers want my data? That’s not something I need to worry about.” Cybersecurity professionals often respond by providing more statistics: how many cyberattacks occur, how much money they cost people, the negative impacts that can come from a cyberattack or data breach, and the extent to which the problem is increasing. Yet these statistics very rarely change people’s minds.

The good news here is that optimism makes people try harder. While using a tone that is more optimistic and more empowering, cybersecurity professionals can tell people: “The threat is real, but you can do a lot of things that are quite straightforward and that will bring the threat down to a great degree.” Even though optimism is generally more powerful than facts, when people feel that there is a point to changing their behavior, that they can actually make a difference in their level of cybersecurity, they are more likely to engage in the behaviors we recommend.

The Psychology of Fear

Fear has to be handled very carefully in order to motivate positive behavior change. The traditional cybersecurity approach has been deeply rooted in fear, uncertainty, and doubt. The bad news about this traditional approach—telling people something scary because we think it will lead to better behaviors—is that it simply doesn’t work. Research has been conducted analyzing six decades of what is known as fear appeals: using fear to try to change behavior. What these sixty years of the use of fear appeals have shown is that to use a scary message effectively, you
need to communicate that message very carefully. When people are confronted with something scary, such as a threat, they naturally appraise that threat and consider how real it is.

People need to understand that a threat is serious and that it applies to them before they will even consider some of the recommended behaviors to avoid it. Only then will they consider the behaviors and whether they are capable of enacting the recommendations. For example, when we’re told to use different and complicated passwords for each account, when we’re asked to turn on two-factor authentication, when we’re instructed not to click on suspicious-looking links, we think: How am I going to do that? And only if we feel able to do that will we engage with the actual danger. If we feel that those responses are beyond our reach, or that they wouldn’t make a difference, we ignore the threat.

Fear appeals can therefore be a very damaging way to spread the message about cybersecurity. A much more empowering way to communicate about cybersecurity is to highlight the positives that come from good cybersecurity. An example from the public health arena can help us understand why this is a better approach. A set of hospitals in New York State set out to address the issue of doctors and nurses who were not sanitizing their hands while they were on shift. The hospitals put in a system of surveillance to encourage doctors and nurses to use hand sanitizer and to wash their hands more regularly. The researchers found that when they told the doctors and nurses about the surveillance, compliance with hand sanitation rose 10 percent. They then installed, above every hand-sanitizer stand, an electronic sign that popped up with a smiley face and a message that said “good job” when doctors and nurses used the stand. Next the researchers added an electronic sign in the common area, tracked hand-sanitizing by shift, and introduced an element of gain: the shift with the highest amount of hand-sanitizing was rewarded. When they took this more positive approach, compliance increased by over 90 percent. These results were replicated in other hospitals.

People are drawn more to a positive message than to a negative message, motivated more by good feedback than by fear.

The Stereotype Threat
The burden of a stereotype makes people unintentionally confirm it. If individuals or groups enter a situation in which they know they are the subject of a stereotype, knowledge of that stereotype will be such a burden and
When it comes to cybersecurity, a stereotype that ferociously dominates this industry is that people are the weakest link, that humans are the problem.

As stated by Emma W, People-Centred Security Lead from the UK National Cyber Security Centre: “If security doesn’t work for people, it doesn’t work.” Instead of undermining people, let’s start spreading a more empowering message.

**Self-Efficacy**

A person’s increased belief in their ability to succeed in specific situations or to accomplish a task—that is, their self-efficacy—drives better behaviors. We know this from research that has been done not only around levels of empowerment and self-efficacy but also around levels of confidence in information security. This research has found that people who feel more confident about cybersecurity are more likely to pursue the behaviors we recommend, such as doing their updates, having a strong approach to passwords, using good cyber-hygiene. This comes from having a feeling of confidence and a feeling of being able. If we give people the encouragement and the tools they need, they will practice more secure behaviors. For example, implementing a “report a phish” button in your emails gives people a quick and easy way to report suspected phishing emails. They have a mechanism, a tool, with which they can engage in good cybersecurity.

This positive effect of self-efficacy is supported by the psychological research on how people respond to fear appeals. When we are discussing cybersecurity, we are inevitably talking about things that are scary: threats, crimes, and malicious behavior. People can often feel intimidated by the subject, and they cannot escape from the need to talk about something that evokes fear. This is why efficacy messages are so important. If cybersecurity professionals talk about something scary without providing a strong efficacy message, listeners will engage in controlling the emotional response to fear rather than in controlling the danger itself: “If fear appeals are disseminated without efficacy messages, or with a one-line recommendation, they run the risk of backfiring, since they may produce defensive responses in people with low-efficacy perceptions.”

Psychology research has shown the importance of empowering people and raising their sense of self-efficacy in order to positively change their behaviors. If we do not focus on efficacy by carefully communicating what people can do to better protect themselves online (e.g., use strong, unique passwords) and how they can do so (e.g., use a password manager), then we may find that our awareness-raising efforts will have a negative impact.

**Conclusion**

These five shortcuts in the brain, or ways of thinking, all relate to how we frame our messages. With a deeper understanding of psychology, behavioral economics, neuroscience and sociology, we can make our messages much more engaging and much more impactful. By
getting social proof on our side, harnessing optimism, spreading hope instead of fear, resisting stereotypes, and raising self-efficacy, we can be more effective in our cybersecurity awareness-raising, leading to more positive behavioral change and stronger cybersecurity cultures.

Notes

© 2019 Jessica Barker. The text of this article is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License.

Jessica Barker (jb@cygenta.co.uk) is Co-Founder and co-CEO of the cybersecurity consultancy Cygenta (www.cygenta.co.uk), where she follows her passion of positively influencing cybersecurity awareness, behaviors, and culture in organizations around the world. She has been named one of the top 20 most influential women in cybersecurity in the United Kingdom and in 2017 received one of the UK’s TechWomen50 awards.
CREATING A CYBERSECURITY STRATEGY FOR HIGHER EDUCATION

By Don Welch
Most of us don’t know how to create an effective cybersecurity strategy. I certainly didn’t. After many years of trying to fit cybersecurity strategy (square peg) into either an IT strategy or a business strategy approach (round holes), I realized that cybersecurity differs enough from both IT strategy and business strategy that the traditional approach won’t work.

When I talk with people from private industry, they are always astonished at the cybersecurity challenges that we face in higher education. Generally, they don’t realize that we face nation-state actors and that colleges and universities are essentially small cities with almost every kind of critical and sensitive data there is. Mixing in higher education’s core values of autonomy, privacy, and experimentation presents significant challenges in cybersecurity.

The first step in facing these challenges is developing and executing a workable strategy. Many approaches that people call strategies really are not. These include “risk-based security programs” or even “risk-based strategies.” Risk is just one component of a strategy. Focusing only on risk leads to tactical decisions. Other components include increased regulation and compliance standards. Meeting regulatory and compliance requirements should be a strategic goal, but again, this should not be the strategy itself.

Strategy Definitions
To get the most value from a strategy, we need to have the correct definition. Strategy started as a military term in the eighteenth century but has been in use as a concept since organized warfare began. Generally, strategy involves allocating a nation-state’s resources toward winning a war as opposed to winning a battle. In the late twentieth century, business began to adopt the term. Even though the environments are vastly different (of course), the concept does translate well to the business environment.

Below are three common definitions of strategy from a business perspective. Though all three are valid, they all are also incomplete. Therefore, I’ll combine them into a single definition that best fits cybersecurity. First, the most-recent Wikipedia definition of strategy is: “A high-level plan to achieve one or more goals under conditions of uncertainty.” This is a good start. Cybersecurity is the poster child for conditions of uncertainty. However, we need more from a strategy. Second, Henry Mintzberg calls strategy “a pattern in a stream of decisions.” This definition captures the concept that a strategy should drive alignment throughout an organization—a concept that is foundational to success, in my experience. Third, Business Dictionary defines strategy as “planning and marshalling resources for their most efficient and effective use.” This idea of allocation or prioritization of resources is a critical component. Thus, I combine all
three of these and define \textit{strategy} as follows: “A long-term plan that allocates resources and sets a framework for decision-making to achieve long-term goals under conditions of uncertainty.”

\textbf{Business Strategy}

Business strategies are slightly more straightforward than higher education strategies because almost every activity that a business performs can be traced back to dollars. An activity is either a cost or a revenue, and businesses aim to maximize profits. Colleges and universities are different. They must have more revenue than expenses, but in higher education, surplus dollars do not necessarily mean that an institution is performing better. The definition of success is stakeholder value, making the success of a college or university much more difficult to track.

Michael Treacy and Fred Wiersema talk about three types of business strategy: customer intimacy; product leadership; and operational excellence. Each offers a framework that is consistent with the definition of \textit{strategy} stated above. Businesses executing a \textit{customer intimacy} strategy focus their resources on the customer experience. Nordstrom was famous for this approach; a resurgence of this line of thought is evident in retail today. To compete with online shopping, many retail companies are focusing on a customer experience that online sellers can’t provide. Second, businesses that execute a \textit{product leadership} strategy are providing a product or service that is better for some segment of the market than that of any competitor. Apple under Steve Jobs is an example. Apple invested a great deal into R&D, and accounts of Jobs’s attention to detail and the focus of the Apple design teams illustrate the company’s slavish devotion to this strategy. As a result, those who believe the iPhone is the best smartphone will pay a premium. Finally, companies that focus on an \textit{operational excellence} strategy deliver products or services at prices lower than those of their competitors. Walmart is a classic example.
If you squint your eyes, you might be able to see how a cybersecurity strategy could be devised to fit one of these patterns. But doing so would not be intuitive.

**IT Strategy**

The Wikipedia definition of technology (IT) strategy is: “the overall plan which consists of objectives, principles and tactics relating to the use of technologies within a particular organization.” TechTarget states that IT strategy is a “comprehensive plan that outlines how technology should be used to meet IT and business goals.” The main concept to note is that IT strategy is not adversarial or competitive per se. In business strategy, by contrast, companies are striving to succeed over competitors. IT strategy must support the company strategies and deliver what the company needs.

Many IT strategies are simply tactical checklists of best practices. This represents an operational efficiency approach. IT strategies generally involve the prioritization of resources both within the organization and within the IT department. The long-term goals usually fall into two categories: those that enable a business goal, and those that free resources for business efforts. For example, a retail business may have a customer intimacy strategy. To execute this strategy, it may choose to collect and analyze data. The company may decide to increase the investment in information technology in order to increase the delivery and quality of information as a business goal. An example of a strategy to free resources would be IT consolidation that might trade a decrease in responsiveness for resources that can be spent elsewhere.

Risk must be part of the IT strategy. Risks include obvious ones such as disaster recovery and business continuity. Risk management involves determining how much risk the business can tolerate versus the costs required to address those risks. Availability is also a central tenant of cybersecurity. Confidentiality, integrity, and availability risks are the core of cybersecurity, so this is the obvious place where the IT strategy and the cybersecurity strategy overlap and must be aligned. However, making the cybersecurity strategy part of the IT strategy is a mistake. The two functions are too different to be fully integrated.

**Strategic Analysis**

Strategic analysis in business is usually organized into strengths, weaknesses, opportunity, and threats—aka SWOT analysis. SWOT analysis will work for cybersecurity, but it feels forced to me. There are three characteristics of cybersecurity that suggest a different approach. First, cybersecurity will always be a function of the organization’s strategy. Second, cybersecurity is reactive and not proactive. Finally, cybersecurity is asymmetrical.

Cybersecurity will always be a function of the organization’s strategy. The purpose of cybersecurity is to protect the information assets of the organization. An organization owns information assets so that it can accomplish its mission and give it an advantage over its competitors. According to Bill Stewart and his co-authors, two questions are the key to developing a strategy: (1) “How does cybersecurity enable the business?” and (2) “How does cyber risk affect the business?” Like IT strategy, a standalone
cybersecurity strategy would not make sense. The accusation "security for security's sake" would ring true. A cybersecurity strategy must complement the overall strategy as well as the IT strategy.

Cybersecurity is reactive and not proactive. Many experts have encouraged us to think proactively about cybersecurity and have called their strategic approaches proactive. Maybe it's semantics, but for me there is a difference between acting proactively in a tactical sense and having a proactive strategy. We can't seek out bad guys and arrest them or destroy their capability before they attack us. To me, a proactive strategy means acting before our adversaries do—either to beat them to a goal or to degrade their ability to obtain their goals. We can prepare for attacks before they happen, but we can't act until they occur. Our adversaries still pick the time, the place, and the method of attack.

Cybersecurity is asymmetrical. This is because our adversaries have options that we do not. We must operate within a legal framework that limits what we can do. Our goal is to defend our information. Our adversaries' goals are to steal or change our information or to stop us from having access to it. An analogy is a guerrilla war where the conventional forces are trying to defend territory and population while the guerrilla force is trying to gain political advantage by attacking the conventional force and civilian infrastructure.

Rather than considering SWOT, cybersecurity strategic analysis should look at threats and constraints. Essentially, the purpose of a cybersecurity program is to mitigate the threats it faces while operating within its constraints.

**Threats**

Whereas others might use the term risks, I'll use the term threats. This implies that there is a thinking and reactive adversary on the other side. We are looking at adversaries and what they might try to do to our college or university. We must know what it is that adversaries want to attack. What is valuable to them? How valuable is that information to them, and how much effort is required? The answers to those questions determine the likelihood that an attacker will go after that information. We must also look at the impact of a successful attack on our institution.

If our adversaries succeed, what will be the impact?

\[ \text{Threat} = \text{Impact} \times (\text{Value} \div \text{Effort}) \]

This formula is actually a qualitative analysis. Of course, we all would love to have data that could be used to quantify risk. However, when we rely too much on metrics to calculate risk in cybersecurity, we get precision but not accuracy. We get numbers that we can measure, calculate, and compare, but these numbers might lead us to the wrong conclusions. Take the number of compromises, for example. If the number of compromises per month is dropping by 5 percent, does this mean that our security is getting better? Or does it instead mean that our adversaries have adapted, and we aren't detecting compromises? Or does it mean that our adversaries have moved to different activities but will be back in the future? Also, the data that we gather is usually based on assumptions. Too many events in cybersecurity are "black swans"—unpredicted by previous events. Metrics can be useful and helpful, but they must be incorporated into reasoned qualitative judgment.

Table 1 shows another way to view this formula/analysis. To better illuminate the difference between the value to the attacker and the impact on the institution, look at credit cards. Attackers can make good money from stolen credit cards whether they sell the cards or use the cards themselves. Stealing credit cards is worth a lot of effort. But individuals are liable for only up to $50 if their credit card number is stolen. Likewise, a college or university storing credit card data that is stolen has no impact from the theft. The credit card providers are the ones who lose. The Payment Card Industry Data Security Standard (PCI-DSS) uses fines, the threat of increased process, or the revoking of card-processing privileges to create an impact on the institution, pushing colleges and

<table>
<thead>
<tr>
<th>Table 1. Threat Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Threat Category</strong></td>
</tr>
<tr>
<td>High</td>
</tr>
<tr>
<td>Moderate</td>
</tr>
<tr>
<td>Low</td>
</tr>
</tbody>
</table>
universities to expend the effort necessary to protect the cards.

A good cybersecurity strategy focuses on identifying the largest (high-impact) threats in order to garner the resources to protect the institution and defend against those threats.

**Constraints**

We all know what we’d do in a perfect world, with unlimited funding, complete cooperation, and as many talented staff as we need. Since we don’t live in a perfect world, the cybersecurity strategy must focus on those threats that have been identified to be the most serious (as noted above) while considering the numerous constraints limiting cybersecurity programs in higher education.

- **Funding.** This constraint is fairly straightforward. It concerns capital, operating expenses, and the amount and timing of money that can be spent.
- **Regulations and Laws.** The cybersecurity program must be compliant with regulations and laws. Resources expended for compliance are not available for other purposes.
- **Staff Time and Talent.** The capacity/capability of current staff and the ability to hire and retain talent are both limited. High turnover due to IT markets, the pay that can be offered, and the capacity of staff to learn new skills are all examples of restrictions around staff time and talent.
- **Business Overhead.** The individual culture of various groups in a college or university will determine how much can be accomplished through security controls. For example, understanding that the finance team will tolerate a lot of overhead whereas clinical physicians will tolerate very little is important. The process of assigning high-, medium-, or low-tolerance ratings for the various groups can provide better insight into an organization’s overall tolerance for security overhead.
- **Political Capital.** This constraint overlaps a bit with business overhead, but the emphasis here is on leadership and peer support. For example, if a college or university recently suffered a major security breach, the security team may have a good deal of political capital with senior leadership. In addition, knowing how much those in the rest of the institution trust the security team—that is, the level of peer support—is critical. I recommend making a list of the key leaders across the institution and categorizing them as “will support with a solid case,” “can win support,” or “tough sell.” Understanding political capital allows it to be spent in the most valuable ways and prevents the development of a cybersecurity strategy that won’t be supported.
- **Accountability.** This could be a subcategory of political capital, but I feel it deserves its own discussion in higher education. Being aware of the culture of accountability in an institution is critical to developing a successful cybersecurity strategy. If a strategy depends on shadow IT, but shadow IT is never disciplined for ignoring a central edict, the strategy is in trouble. Are there any real consequences to ignoring cybersecurity? The answer to that question will affect the cybersecurity strategy.
- **Calendar Time.** This constraint includes the dates that capabilities must be in place and the resources that are available.
Not everything in the cybersecurity strategy will be time-critical. This constraint is best analyzed in two parts: (1) identifying any and all limitations on time; (2) sequencing decisions to include calendar time considerations.

- Governance: If governance is imposed on cybersecurity, then it is a constraint. If governance can be created by the chief information security officer, then it is a component of the cybersecurity strategy. With a trusted security team, governance could be as lightweight as a reporting line. Most security teams in higher education don’t have that luxury, however. In this case, advisory committees, with their transparency and participation, are great ways to build trust and support. Heavier governance can involve an oversight committee, with many subcommittees and an executive committee. In a lower-trust environment, the oversight committee will make decisions and approve major projects. Heavier governance will be slower, more time-consuming, and more restrictive. On the other hand, the security team will have more support and will be able to impose more overhead, and the rest of the institution will be more accountable.

### Strategic Patterns and the Cybersecurity Strategic Matrix

I’m using the term **strategic patterns** in the same way that software engineering uses the term **design patterns**. Software design patterns themselves can’t be used to create an application; instead they serve as a component of the application design. Likewise, strategic patterns function as one part of the overall cybersecurity strategy.

Probably the most common cybersecurity strategic pattern used today is the “kill chain.” Another is “Defense in Depth,” which first came into favor in the 1990s. People-centric patterns were more popular a decade ago but are still important. Process-centric patterns are common and may be appropriate depending on the maturity of a cybersecurity program. Technology alone is unlikely to solve all our problems, but understanding what we need technology to do and its relationship with resources is a critical part of any cybersecurity strategy.

Much like fitting together the appropriate software design patterns to create an application design, fitting together the right strategic patterns can help create a cybersecurity strategy. A collection of cybersecurity strategic patterns forms the high-level strategy. Moving down a layer will involve people, process, and technology. A matrix is the natural way to capture this level of the strategic plan. Should people be emphasized over process? Which technology will be chosen? A cybersecurity strategic matrix can capture as well as analyze these decisions.

Table 2 shows a matrix with the five high-level cybersecurity strategic functions from the National Institute of Standards and Technology (NIST) Cybersecurity Framework—**identify**, **protect**, **detect**, **respond**, and **recover**—on the left side and with **people**, **process**, and **technology** across the top. This visual representation shows how the five functions are being addressed and the trade-offs that are being made. The five top-level functions could also be subdivided into more areas. For example, **protect** could be detailed as **access control**, **awareness and training**, **data security**, **information protection processes**, **maintenance**, and **protective technology**.

Based on the cybersecurity strategic patterns chosen, projects or initiatives can be inserted into the cells. These projects or initiatives represent the resources that are required. Doing this will necessarily prioritize the functions and how they will be addressed. For example, if the Kill Chain pattern is used, then the detect function(s) will probably be a top priority. A Defense-in-Depth pattern will require more effort in the **protect** function(s).

Next, efforts should be prioritized among People, Process, and Technology. For example, a startup that has a small, dedicated staff, that doesn’t have much money, and that must be highly productive will look first at solving issues with people. By contrast, organizations that are very mature can look to process first for success. Here is another example. The **identify** function includes asset management, which requires inventorying hardware, software, external systems, and data flows. These needs can be addressed by people, process, or technology but most likely by a combination of all three. People can provide inventory information. Process can issue an “authority to operate” and require documentation. Technology tools can perform automatic discovery of hardware and software. There are trade-offs in each of these approaches.

Each of the cells in the cybersecurity strategic matrix

### Table 2. Cybersecurity Strategy Coverage and Trade-Off Matrix

<table>
<thead>
<tr>
<th>Function</th>
<th>People</th>
<th>Process</th>
<th>Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protect</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Detect</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Respond</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recover</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
can also include submatrices. For example, the Detect/Technology cell could hold a matrix detailing Network, Payload, and Endpoint detection functions across Real-Time/Near-Real-Time and Post-Compromise technologies. Or the Protect/People cell could include a matrix dividing People into Users, IT Staff, and Security, with Mandatory and Optional functions. The idea is to make clear the tradeoffs involved in the allocation of resources.

Another way the cybersecurity strategic matrix can be helpful is in understanding emergent priorities and patterns. As tradeoffs are made in order to allocate resources within constraints, it may become obvious that the initial thoughts and plans simply aren’t practical. A better way to abstract resource allocation, or a different strategic pattern, may become clear. These insights will be important in communicating the cybersecurity strategy.

Communicating the Cybersecurity Strategy
The implementation of a successful cybersecurity strategy depends on a wide variety of stakeholders. For the strategy to be useful to others across the college or university, they must act in alignment with it. Yet communicating the cybersecurity strategy throughout an institution can be challenging. People in different roles need different levels of understanding. End-users will be the least sophisticated security-wise, whereas the security team must of course understand the details. In between are the system administrators, developers, academic leaders, and more. The cybersecurity strategy must be communicated in multiple ways tailored for everyone in the institutional audience.

Creating a cybersecurity strategy that serves as a framework for decision-making requires a concept simple enough that people can hold it in their head. What does this mean in practice? The strategy description must fit easily on one PowerPoint slide. There are two effective ways to do this. Both methods can be incorporated into a two- to five-minute presentation that will create a memory aide for the audience.

One way is to use the old standby of bullet lists, phrasing the text so that it captures the essence of the strategy. The range should be three to seven bullets, with five being optimal. A word or two followed by a phrase or sentence gives the viewer something to hold on to. For example: “Information Centric: Categorize and prioritize defending high-risk information.” It should be possible to explain the strategy in five minutes—not quite an elevator pitch, but not much more.

The other, perhaps better method is to use a diagram. The combination of a graphic and words is easier
for someone to remember than just text. This might be hard if you’re not an artistic person, but communication teams may be able to help. The risk is greater if the diagram doesn’t hit the mark, but the possibility of a winning home run is greater as well. Figure 1 is the illustration I use to communicate Penn State’s cybersecurity strategy.

These basic explanations might be the most important part of a cybersecurity strategy. Unfortunately, they are, like a poem, the hardest to get right. As the saying goes, a poor plan well-executed beats a great plan poorly executed. This simple, high-level explanation of the cybersecurity strategy will play a large part in determining how others across the institution do (or don’t) align.

Still, for those who want additional details and who have the tolerance to read or listen to more, further explanations are required. A “one-pager” is an option. This is a document that explains the strategy on one side (or both sides) of a piece of paper. Another option is a fifteen- to thirty-minute strategy briefing. This could consist of seven to fifteen slides that put more flesh on the bones of the strategy. The higher the picture-to-bullet ratio, the more effective this communication will be. I also suggest including a discussion of the threats and constraints. The more comfortable people are with the reasoning behind the strategy, the more enthusiastic they will be in implementing it.

Depending on the institution, a well-polished explanation of the cybersecurity strategy may not be required. The main benefit comes from the writing. Chances are that the detailed justifications will be helpful, at some point, for various initiatives.

I believe that effective communication is perhaps the most critical aspect in the entire process of creating a cybersecurity strategy. Feedback is thus essential. Words and concepts that make perfect sense to the security team, for instance, may be lost on some stakeholders or, worse, may evoke a bad reaction. Communication will need to be modified over time.

Conclusion
Thinking about cybersecurity from solely a risk-based perspective or as the risk part of an IT strategy will not result in the most efficient allocation of resources, nor will doing so align the institutional cybersecurity efforts. Cybersecurity demands a strategic approach because it is difficult, rapidly changing, and potentially devastating to a college or university. Cybersecurity differs from either IT or business operations because it is adversarial, reactive, and asymmetrical. Cybersecurity efforts must be closely aligned to the institution’s overall strategy and must complement its IT strategy. Failure to think and act strategically results in the inefficient use of resources and increases institutional risk.

The inputs to cybersecurity strategy are threats and constraints. The strategy must identify the institution’s information assets and the impact of a successful attack on them. Understanding the value to attackers provides insight into the likelihood of attacks and how much effort adversaries will expend to gain those assets. This analysis provides a risk-based prioritization for defending information. Institutions have limited resources to expend on cybersecurity. These resources include not only funding and staff but also intangibles like political capital and accountability. An effective strategy must address the most serious threats while staying within the constraints of the institution.

Cybersecurity strategy must be long-term, be effective under uncertainty, prioritize resources, and provide a framework for alignment throughout the institution. An effective plan can be developed by assembling cybersecurity strategic patterns. In addition, a matrix that matches the functions of the NIST Cybersecurity Framework to people, process, and technology can provide a visual representation of the strategy.
representation of the implementation of the cybersecurity strategy. Finally, sequencing the contents of this matrix can create a roadmap of projects, initiatives, and efforts to execute the strategy. Beyond offering a risk-based approach, the strategy will effectively allocate resources and align efforts.

Cybersecurity is not just an IT function; it is an institutional function. Thus, almost all members of the college/university community have a part to play and should act in alignment with the cybersecurity strategy. And since they can’t align with the strategy unless they understand and remember it, communicating the strategy is as important as devising the strategy itself.

Cyberattacks on colleges and universities are increasingly frequent and damaging. The cyberthreat to higher education overall is both significant and likely to grow for the foreseeable future. Meeting the challenge, especially in higher education, requires strategic thinking, and that strategy must come from cybersecurity-specific strategic thinking.

Notes

© 2019 Don Welch. The text of this article is licensed under the Creative Commons Attribution-NonCommercial 4.0 International License.
leadership skills are cleared for take off!

July 22-25, 2019 Salt Lake City, UT

Learning Technology Leadership Program
Management Program
Senior Directors Program
Leadership Program

Register by June 10 for early registration rates.

events.educause.edu/educause-institute
21ST-CENTURY ANALYTICS

NEW TECHNOLOGIES
In higher education administration, 21st-century data analytics has arrived. Signs of improvements are emerging sporadically, like flowers blooming in the desert.

BY VINCE KELLEN
Yet at most institutions, troubles abound. Political silos, held together by the maxim that hiding and hoarding information secures one’s position, prevent the consolidation of systems. Combatants use information technology as a proxy war, thus avoiding more difficult head-to-head conflict. Many staff in our IT organizations and end-user communities have not kept pace with the sudden advances in analytical approaches and tools and are often lacking basic skills in statistics and data management. New technologies go through careful and sometimes lengthy reviews before adoption while current approaches, delinquent as they may be, escape similar scrutiny. College and university leaders are loath to change their organizational structures to utilize data better, and given today’s technology, these structures now look downright anachronistic.

The refrain of objections repeats:

- We have so many ways to define data! (In reality, there aren’t that many.)
- Our data is of poor quality! (It can be fixed.)
- Legal regulations say we can’t! (These are commonly overstated; laws should be read carefully.)
- Our politics will prevent this! (That may be, but leaders can influence the culture.)
- What about privacy and security concerns? (Tools for managing these concerns are now more advanced.)
- We need outside experts to do this for us! (This is not always true.)
- We can’t integrate the data because our tools are too old! (Read on.)

One could argue that since the dawn of civilization, the adoption of new ways of doing things is slowed down in two ways: (1) the length of time required for the practice to be communicated from mind to mind, and (2) the length of time required for a single mind to accept that a new practice is worthwhile. With the communication technology available today, the first barrier is removed: practices can propagate prodigiously and swiftly. It’s the second impediment to adoption—mental inertia—that remains a concern. We all look at the world through a certain framing or lens (mental model), based on our background. New data and new logic must fit into these frames before we can adjust them and adopt a new practice.

One area of mental models stubbornness involves managing basic data. In most IT organizations today, staff are moving data between systems using “flat files”—text files containing rows of data, spreadsheets, and replicas of databases (database dumps)—just like our forebears did in 1989. The basics of the batch file import and export have not changed much, if at all. Worse still, in many IT organizations, data movement is a cottage industry that exists in piecemeal form sprinkled across, if not beyond, the central IT organization and is usually loosely regulated and often not systematically improved. For me, this is infuriating. Even though many organizations have adopted all sorts of
new technologies and approaches, vendors and IT organizations alike persist in flat file tangles.

In the area of structured analytics, the Kimball-style data warehouse, with fact tables and dimensions and with star or snowflake permutations, still reigns supreme. The concept of extract, transform, and load (ETL) is alive and well and permeates people’s thoughts and language. Data at rest needs to be extracted from the ground, lifted out, and transformed, like a manufacturing process, in often convoluted operations that fold, bend, and otherwise spittle upon the data and then finally load the data, like a railcar of goods, into the retail shop floor, which in this case is the Kimball model, arranged like empty shelves awaiting information goods to appear. Report writers and data visualizers then, again, rummage through the Kimball model in the data warehouse, combining data using a series of joins and, very frequently, making copies of the data in order to facilitate additional data transformation and analytics methods or to be combined with data not in the data warehouse. The current manufacturing process needs improvement.

The lack of processing speed within the computing environments has been a strong force shaping the evolution of our data management practices. Slow disk drives dictate a certain response from operating and database system software developers, involving things like indexes, transaction logs, and caches. Data warehouse designers respond by forcing the surface design of the solution to respect these limitations. The result is that data warehouses, once built, still require significant translation or add-ons to meet specific analysis needs. The historic, up until now, scarcity of compute performance that has not kept pace with the growth in data has profoundly shaped not just the nature of IT systems but the common thought processes of everyone involved. Designers of solutions today are using thirty-year-old mental models around scarcity of compute and are thus crippling their designs, not fully realizing how radically different 21st-century analytics has become.

The New Technologies

The past evolutionary pressure—that is, the performance constraints in older data analytics systems design—is fading. New technologies are significantly bending the cost-benefit curve and letting organizations process more data in ways that are better, faster, and cheaper than before. While some data, especially scientific data, continues to get arbitrarily dense and hence exponentially bigger, most, if not all, of the structured and unstructured data in college and university operations today lies safely within the comfort zones of the available technology. Five technologies in particular are enabling this transformation.

Technology #1: Improvements in Scale-Out, Low-Cost, Near-Real-Time Streaming

While usually associated with Internet of Things (IoT) applications, streaming technologies are now poised to take over the synchronization of data for analytics. These technologies include, but are not limited to, Apache’s Kafka, NIFI, and Storm and Amazon’s Kinesis (including Kinesis Data Firehouse). These tools support real-time and near-real-time use cases and can expand using horizontal scaling approaches that are the norm today to quickly handle big data movement at (usually) extremely low cost. When data moves to streaming, the real-time nature of the tools harder the environment because errors get rooted out quickly. When data is replaced nightly once a month, the IT organization gets twelve chances a year to fix it. When data is streaming hundreds of times a day, the IT organization fixes it many times a day. These streaming approaches also enable real-time analytics to be working as data moves through the stream even before the data lands to rest in a data store.

Technology #2: High-Speed, In-Memory Analytics

These tools (e.g., SAP HANA) sport scale-out, parallel designs that make mincemeat out of billion-row data sets. These environments also heavily compress the data, maximizing use of higher-speed memory. Very large data sets can be analyzed in these environments, which resemble supercomputers. In-memory analytics costs have dropped significantly in the last decade and are, in some cases, starting to replace high-speed disk drives as cheaper alternatives.

Technology #3: Low-Cost, Big Data Environments

Tools like Apache Hadoop, Amazon Redshift, and Google’s serverless BigQuery let organizations store petabytes of data cost-effectively. The high-speed, in-memory tools referred to above can now federate their queries with these environments, providing organizations with a two-tier approach. Tier 1 is very fast but more expensive. Tier 2 is very big and slower but super cheap. Petabytes of data can be modeled in one, synoptic architecture.

Technology #4: Artificial Neural Network Resurgence

After enduring an impossibly long and cold winter of a couple decades, artificial intelligence (AI) has undergone a renaissance, partly enabled by improvements in computer memory and hardware such as CPUs—for example, application-specific integrated circuits (ASICs), field-programmable gate arrays (FPGAs), and tensor processing units (TPUs)—but also due to software improvements represented by the various forms of new neural networks available today. These neural network techniques are now ubiquitous in the area of social media and e-commerce.

Technology #5: Hyperscale Cloud Providers

These cloud providers, dominated by Amazon Web Services (AWS) but with Microsoft Azure and Google Cloud Platform following close behind, are enabling all of these technologies to be run in very dynamic and elastic environments. Analytics data processing can ebb and flow in a pattern of big bursts punctuated by dry spells, and the resource consumption and pricing can also ebb and flow.

The New Rules

These five technologies, which are subverting the dominant paradigm of data and analytics, are begging for a new set of rules. The following six rules are an inversion, of sorts, of the old rules.

Rule #1: Everything Is a Verb.

In working with my analytics teams over the last few years, I have found that the old focus on nouns and their relationships to each other (e.g., entity-relationship modeling, among other approaches) is much less important. Relational modeling originally grew out of the need to divorce logical hierarchies (relationships) from physical data structures, providing great flexibility. In time, relational modeling also had to genuflect before the performance altar, and today, most data warehouse designers cut out of this cloth cannot stop themselves from trying to conserve performance and hence adjust their designs. Also, with master data management methods now fairly well adopted, teams I have...
worked with have made significant progress in ensuring we understand and accurately model key nouns (entities).

With the five technologies listed above, we can now put verbs first. For each noun, we work out all the events that can change or utilize the noun. Each of those events comes from one or more source systems in tiny batches—a stream—of data creations, updates, or deletions. Rather than try to make sure we have all the additional fields that describe the noun perfectly conformed, we instead work on making sure all streams of changes regarding the noun are suitably captured. In short, we are replicating a transaction log that describes all updates. We call this a **replayable log**, meaning that we have the time history of changes captured in the stream of events. We treat the events in this log as idempotent, allowing duplicate messages to be detected and dealt with safely within the analytics environment. This lets us ingest data very rapidly and very inexpensively with greater resiliency in case of any system failures. This method of designing the data to allow some duplicate data with after-the-fact resolution is called an **eventual consistency data integrity model** and enables the very low-cost, high-speed data integration capabilities.

All these events, or verbs, get placed into one very long table. Specifically, the table is one that has a variable record length, with different uses of columns, but all placed in one big, fat, wide table. While this is raising the hair on the back of the neck of old-school data warehousing folks, this sort of design is actually quite old, going back to very early mainframe days of computing, and works well in today’s modern systems. For example, although the developer sees a single wide table, in-memory columnar database tools store that activity log in an entirely different internal structure. These large activity tables then serve as our data lake in a very simple, very big, and often very wide data structure. This simplicity enables all sorts of extensibility since it relaxes so many rules of data design. In addition, the streaming technologies let us more easily ingest data, IoT style, from a variety of differing systems. We use this activity table as the base structure upon which we build all our other analytic views.

**Rule #2: Express Maximum Semantic Complexity.**

In the old way of doing things, analytics developers will often include only data that matches the need required. We do the opposite. We try to bring in all the data that we can find in any given stream, **whether we think we will use the data or not**. An analogy is home construction, where it is much easier to put in electrical cabling before the walls go up, not after. For example, in one of our analytic domains, we are bringing in over 5,000 unique fields of activity data but surfacing only about 800 in our initial analytic views. The rest will be surfaced over time.

A second aspect of this rule is that we also bring in data at the lowest level of granularity possible. While this can often explode the number of rows of data within our models, the new technologies come to our aid with all sorts of tiering between high-cost and low-cost storage and several automatic compression methods.

Bringing in as many attributes as possible and all data at the lowest level of granularity also ensures that we will be able to answer any question that may be asked. The only questions that can’t be answered are those for which there is no data or for which the source system did not capture data at that level of granularity.

We have found that this in-memory, parallel columnar analytics environment also means that we do not have to handcraft the pre-aggregation of data. All of our models can rely on the lowest level of detail at all times. If we do any pre-aggregation work in our designs, it is for the convenience of the analysts. Sometimes a pre-aggregated number is much easier to work with in visualization tools. Thus, we aggregate data for convenience only, not for speed.

**Rule #3: Build Provisionally.**

This rule is the hardest for data warehouse developers to swallow. Historically, these developers build fact tables and dimensions that must stand the test of time, and they do. But these models also end up requiring additional data structures, placed on top, to support analysts who often have many different ad hoc issues requiring their attention. Analytics has more than a whiff of ephemerality and needs to change based on ever-evolving business needs. Our designs must capture that ephemerality in a deeper way.

In our environment at UC San Diego, we have a replayable log in the activity tables serving as a data lake, which by itself is not really usable. We must build something on top of the data lake—something that can serve for the duration of time needed but that can also be considered ephemeral and adaptive. We have used the term **curated view** to capture two opposing intents here. The first intent is to ensure that a curated view of the data is appropriate for a specific, perhaps narrow, but also evolving use case. We call this type of view an **analytics vignette**. The second
The old rules for normalizing databases can be thrown away. But this is not a free-for-all environment. Quite the contrary. A new, strict set of construction rules replaces the old set.

Curated views can be redundant and overlapping. Several curated views can be combined and built on top of one another. Our curated view designs typically have three or four levels of hierarchy so that we can reuse code (SQL for us) when constructing curated views. Thus, what the user sees is a single, flat file with often a few hundred attributes (columns) that they can easily use. We take any joining of different tables away from the analysis. All our curated views are designed with all needed joins made.

I have been focused on structured data, but our data lake may carry with it lots of unstructured data—that is, data not adequately described in terms of attributes and relationships. This unstructured data will be continually seeking structure, chiefly through advanced algorithms including AI and machine learning. As the unstructured data grows exponentially, so will the need to structure it. Hence, over time, structure will be added, and our data lake is designed to accommodate that.

Although this may sound hideously wasteful of computational resources, the five technologies listed above have made this approach eminently feasible and cost-effective. Because our curated views are built on top of highly reusable components and are themselves reusable in other curated views, we can have as...
much model overlap or outright redundancy as our analysts need while still keeping the views quickly changeable. We can easily create new curated views borrowing promiscuously from the collection of other views. By merging the data lake (the activity logs) and the curated views in one environment, we can ingest very complex and unstructured data in the activity tables right away and then incrementally add structure to the data and include that structure in existing or new curated views.

**Rule #4: Design for the Speed of Thought.**

Why the need for speed, especially when many decisions in business are not made with real-time or near-real-time data? A faster-moving environment is cheaper to manage and more pleasing to the analyst. Designing with speed from the start is far less costly than trying to add it back in later. Managing a real-time, incremental data integration architecture is also less expensive than managing an old-school batch-oriented one. Speed is important for analysts, data developers, and data scientists. A fast environment lets analysts work at the speed of thought with subsecond responses for all clicks in an analytics tool, regardless of whether the task is to aggregate a single column across 500 million rows or to drill into 500 rows of fine detail. A fast environment lets data scientists build and deploy models that much faster.

Designing for the speed of thought also requires moving as much of the complexity as possible to the infrastructure. For example, in our analytic environment at UC San Diego, we can take difficult filtering logic (sometimes complex Boolean and set logic) that would normally be expressed in the front-end visualization tool and convert it into reusable bundles in the back-end, relieving the analyst of that work. Our curated views will contain what look like redundant fields and will include permutations of a single field side by side (e.g., last name and first name combined into one field, in that order, as well as first name and last name, in that order). Although a downstream analyst can easily do that simple manipulation, we found that providing these small details within the analytics environment increases analysts’ usage and throughput.

The overall analytics environment also needs to handle a variety of tools that good analysts typically use and that can also support real-time, daily business activities. This “bring set and explode it, often to enormous sizes. Why? In a nutshell, we are trading off a larger data structure for a simpler algorithm. For example, in a typical large university, a class schedule for all courses offered can fit into a decently sized spreadsheet. Exploding that data set to show also each room’s usage for

**Data must be freed from silos and transcend traditional hierarchies, making data hoarders a thing of the past. In this new world, information is no longer power.**

each minute of the day, for every day in a year for twenty years, results in 2.3 billion rows. Why would anyone do such a thing? Because visualizing an “exploded” data set is trivial and allows the analyst an incredible level of granularity with either a visual or an analytics algorithm. This allows easy historical analysis and quick answers to numerous questions without requiring effortful programming. Is the university more or less efficient in class utilization over time? In which time slots can additional classes be added? How do physical classroom factors such as the quality of the building and the classroom affect student performance in classes over the twenty years? What are the long-term correlations with facility utilization and energy and other utility costs? These questions can be answered with little to no additional data-preparation work.

The old rules for normalizing databases can be thrown away. But this is not a free-for-all environment. Quite the contrary. A new, strict set of construction rules replaces the old set. For example, the new methods for handling activity tables and curated views are as rigorous as any of the old rules for dimensional modeling. It’s just that the new methods involve an inverted set of assumptions regarding space, size, and performance. We don’t care about the growth or explosion of data. We embrace it.

**Rule #5: Waste Is Good.**

Even though the “waste is good” rule is implied or directly called out in the prior four rules, it is worthwhile touching on it further. Developers who make the transition from traditional environments to the new environment all spend at least a few months struggling to accept what was so ingrained in them: the need to conserve computing resources. This is where younger and perhaps less experienced developers and data scientists may have an advantage.

All this supposed waste enables agile, flexible, super-fast, and super-rich analytics environments at a lower price that was unheard of ten years ago. In this environment we routinely take what would be a parsimonious data activity in production settings. In the near future, many organizations will need to be able to manage dozens or hundreds of AI or machine learning models, all running real-time, acting on the stream of data as it flows in. These models need to be placed into service and taken out of service much more dynamically and frequently than in analytics of yore.

These new analytics models will be handling personalized alerting and nudging of people, as well as initiating system-to-system communication that will control human and system activities in an autonomic manner. This analytics environment must be capable of delivering timely information that fits within the cognitive time frame of the task at hand for each person and each intelligent computing system.

**Rule #6: Democratize the Data.**

Data democratization means providing equal access to everyone, leveling the playing field between parts of the organization so that all parties can get access to and use the data. Today’s economy is an information one, filled with information workers—and information workers need information. If key staff members in your organization end up in an environment not suitable for their intellectual skills, they will opt to
leave. So, when we consider access to data more broadly, we’re not talking only about the data itself. We’re also recognizing the information-oriented nature of today’s work and recognizing the complexity of organizations.

Organizations that invest in decentralized decision-making and that make the necessary investments in technology and organizational practices perform much better than their peers that don’t do so. Data must be freed from silos and transcend traditional hierarchies, making data hoarders a thing of the past. In this new world, information is no longer power. Information sharing is power. While anecdote and intuition can be potent influences on decision makers, this “faith-based” reasoning gets replaced with “fact-based” reasoning that accommodates more diverse thinking and perspectives than in the past. People who are lower in the organization and are empowered by data can now begin to correct errant anecdotes promoted by powerful people.

Organizations will need to establish a new culture to achieve this data democratization. That culture is going to require executive support—an executive mandate, perhaps—as well as a bottom-up push. But the shift to data democratization can be somewhat subtle. Organizational leaders can tell staff that information sharing is power and that information management is a team sport. People don’t own data; rather, they steward it. Data democratization can also be furthered through practices such as the following:

- Develop team-based processes for fixing data quality at the source. These processes put data consumers in tighter collaboration with data producers and place responsibility for data quality in the community.
- Reduce between-team rivalries by eliminating mission overlap and redundant activities where possible. Conflict over information is often caused by groups with highly overlapping missions, activities, and populations served. In this model, each duplicative unit has something to gain by competing with or trash-talking its peer unit.
- Work bottom-up, top-down, and sideways in the organization with messaging and community building.
- Ensure that “getting the culture right” is an executive concern and that leaders are promoting fact-based reasoning.

The traditional two-dimensional hierarchical model of organizations no longer accurately represents how information is managed within colleges and universities and how staff activities generate value. The new rules require organizations with more organic, molecular structures that can alter themselves in order to improve nearest-neighbor communication whenever and wherever that communication is needed. All notions of a hierarchy disappear as individuals find the colleagues they need to communicate with on a regular basis, independent of the organizational structure. Two structures are at play here: the structure that exists on paper and the structure that exists in reality, based on information flows. The latter is a three-dimensional, molecular protein folding.
Managers will need to move away from a mental model in which they own and control resources, toward a model in which they are primarily facilitators and guides on the side for those they lead.

Data democratization turns individual accountability on its head. In complex processes that involve multiple units, success and failure become a team affair. All team players (organizational units) must share information in order to adjust themselves as needed. Of all the new rules, this one is most flammable. The privacy, political, and organizational untangling that may be required to enable data democratization can be overwhelming.

**Impact on IT Organizations**

The implications here are manifold. IT teams will need to be organized very differently, around the following activities:

- Data movement design
- Data movement orchestration and monitoring
- Data architecture and data design
- Data science modeling
- Data science orchestration and monitoring
- Data security and privacy
- Data democratization community development and management

These skills, which are a repackaging of older skills but now wrapped around dynamic cloud technologies, form a sort of data science design and operations group. With software as a service growing by leaps and bounds, many IT organizations do not develop software. Instead, with a coterie of various systems in the cloud originating data, a new “Dev Ops” or “Data and Data Science Ops” team is being born. While the rigor learned from older methods like Kimball- or Inmon-style data warehouse is always useful, the specific design patterns and assumptions of older methods, especially if they are deeply ingrained in an IT worker, are not. Concepts like ETL, operational data stores (ODS), staging tables, and fact tables and dimensions have been formed around systems with more significant performance limitations and are not directly applicable or needed in new environments.

**Elevate Your Career.**

Be the bridge that connects your institution to the wealth of EDUCAUSE member benefits, so you can:

- Become an indispensable resource to your colleagues
- Increase your visibility with leaders across campus
- Grow your peer network

Explore the EDUCAUSE Ambassador Program.

educau.se/ambnetwork
Managing 21st-century AI and machine learning algorithms requires an operational environment that is very different from conventional analytics. Machine learning models are like tires: organizations will have many in service, and the models will require ongoing data operational monitoring and evaluation to identify anomalous output and responses, as well as to determine how fast or slow the models may be responding to the data. IT teams will need the right platforms for holding models on a “runway” for development and testing, for letting the model “take off” in production, and then for bringing models out of service while introducing new models seamlessly. This is not your grandparent’s data analytics environment.

These new technologies also raise more legal and ethical concerns. Privacy laws and policies are growing rapidly and differentially across multiple regions of the globe. New AI and machine learning approaches can introduce new forms of benefits and legal liabilities not previously imagined. While data democratization is both important and helpful, ensuring a highly secure environment takes on greater importance too. The tension between serving students and serving our communities needs to be balanced against institutional risk and personal privacy concerns. Fortunately, higher education is not alone. Our peers in the health care world have been grappling with security, privacy, and ethics issues and can offer good models and guidance. Research into quantitative techniques for ensuring privacy while still publishing (or using) data is advancing, and solutions for using these advanced methods (e.g., $k$-anonymity and differential privacy) are finding their way into products, with more advances in technical controls coming.

The impact outside of the IT organization is likely to be even more significant. Organizational structures that are more flexible and organic in nature are difficult for traditional, control-oriented managers to accept. As information flows more freely to people lower in the organization, power appears to shift away from traditional managers. That is probably as it should be. Colleges and universities are information- and knowledge-generating entities. Information workers in higher education can’t be held captive; highly skilled information workers can and will leave for environments friendlier to their talents. Managers will need to move away from a mental model in which they own and control resources, toward a model in which they are primarily facilitators and guides on the side for those they lead.

How higher education institutions portion out accountability will need to be re-examined as well. Institutional success will be increasingly guided by fascinating forms of fast and advanced analytics brought to bear to help reduce operating costs while making an impact on the institutional missions. A shared-information environment requires a shared-risk/reward environment that can promote excellent team play. This can make managing accountability more difficult, since simplistic, top-down reviews need to be blended into more complicated assessments of multi-unit system dynamics with a more diffuse accountability structure. This is also an inversion of the traditional accountability mindset that focuses on specific individuals and leaders. On the surface, this seems harder for managers to do, but one thing that is uniquely human is our ability, as a species, to manage a much larger and more complex set of social linkages. People can and do learn how to operate in more socially complex and dynamic environments. Many followers are up to the challenge. Are leaders?

Summarizing, the new technologies and new rules bring with them different concepts. Table 1 summarizes the key differences between the old approach and the new.

Other implications abound. We need to enumerate them, and we need to ponder them. But we don’t have the luxury of time. 21st-century analytics is here, and it is radically different. New technologies call for new rules. Those of us in higher education should learn and adopt these rules. Only with new data and analytics mental models can we discover and take advantage of new possibilities.

Table 1. Old versus New Concepts

<table>
<thead>
<tr>
<th>Old Concepts</th>
<th>New Concepts</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Permanence</td>
<td>1. Ephemerality</td>
</tr>
<tr>
<td>2. Design for system performance constraints</td>
<td>2. Design for speed-of-thought</td>
</tr>
<tr>
<td>3. Periodic batch data movement or ETL</td>
<td>3. Incremental, streaming real-time data movement</td>
</tr>
<tr>
<td>5. Separate models for live, near-line, and archival tiers</td>
<td>5. Single synoptic models across tiers</td>
</tr>
<tr>
<td>6. Dimensional modeling</td>
<td>6. Multiple modeling techniques</td>
</tr>
<tr>
<td>7. Data Ops</td>
<td>7. Data Science Ops</td>
</tr>
<tr>
<td>10. Top-down data control</td>
<td>10. Bottom-up data democratization</td>
</tr>
<tr>
<td>11. Hierarchical organizational models</td>
<td>11. Network/molecular organizational models</td>
</tr>
<tr>
<td>12. Individual accountability</td>
<td>12. Team accountability</td>
</tr>
</tbody>
</table>

Notes

© 2019 Vince Kellen. The text of this article is licensed under the Creative Commons Attribution-NoDerivatives 4.0 International License.

Vince Kellen (vkellen@ucsd.edu) is CIO at the University of California, San Diego (UCSD), a member of UCSD’s Chancellor’s Cabinet, and Vice Chancellor and CFO of the UCSD senior management team.
Using AI to Help Students Learn “How to College”

From before our students even set foot on—or return to—our campuses, we are helping them learn “how to college.” In doing so, we are setting them on the path to graduation and to success far beyond our college or university.

Wayne State University, much like the city in which it is located, is undergoing a transformation. In six years, the Detroit-based university has increased its graduation rate from 24 percent to 46 percent. That makes Wayne State one of the fastest-improving higher education institutions in the country. I have been fortunate to be a part of this team since 2016, when I was hired as Wayne State’s associate vice president for enrollment management. Over the last few years, we have learned much about how to address the problems holding our students back. Across so many of our initiatives, one common lesson stands out. This is also a thread that, unfortunately, binds many US public colleges and universities together in their struggle to make good on the promise of higher education.

What is this lesson/thread/problem? We don’t teach students “how to college.”

At Wayne State, 90 percent of our students come from within 30 miles of our campus. More than one-third of last year’s freshman applications were from first-generation students. About 40 percent of our students are minorities. In many ways, we are a microcosm of higher education’s evolving demographics. Nearly 40 percent of students in the United States are now over the age of 25. More than a quarter of students are parents, and nearly 60 percent of students must juggle their education with work obligations. About half of the students at Wayne State are children of parents who never earned a bachelor’s degree. Most of these students arrive on campus ready and capable to succeed in the classroom, but they are not prepared for the unexpected challenges of the college/university landscape.

Clearly, we must teach students how to better navigate...
college as a system. Consider the following common scenarios:

- A teenager, the first in her family to be accepted into a college, grows frustrated with the byzantine financial aid process and simply gives up before her first day of class.
- A sophomore struggles to find an affordable place to live off-campus.
- A working mother repeatedly skips class because she is unable to find short-term care for her children.

As higher education institutions across the country become more and more diverse, students are increasingly facing these kinds of barriers. Institutions have the solutions to help students with many of these challenges, but they have trouble communicating those answers to students, many of whom may be too embarrassed—or may not even know how—to seek help. At Wayne State, we knew we had to find new and better ways to reach more students in need.

In April 2018, we began experimenting with a conversational artificial intelligence (AI) tool—also known as a “chatbot.” The chatbot, developed by AdmitHub, helps prospective students successfully apply to and enroll in a college or university by answering their questions through text and mobile messaging. Marrying AI with a conversational tone, our chatbot—named “W the Warrior,” after our mascot—helped boost enrollment by 14.6 percent, including an 18 percent increase in first-generation students and a 13 percent increase in Pell-eligible students.

“W the Warrior” is not a passive assistant. When records indicate that a student has yet to submit an important document (e.g., a high school transcript), the chatbot will message the student, offering both a reminder and further assistance. When students approach the chatbot asking for help, W assists them by providing not only answers but also guided questions. Machine learning allows W to provide better answers to students’ questions as more students interact with it.

The questions that students ask W range from simple queries about important deadlines to more complicated inquiries about financial aid. We quickly learned that students were willing to ask W many questions that they were often too embarrassed to ask campus staff. This facet of the chatbot is what particularly excites us about its ability to help a fast-growing cohort at Wayne State: our returning students. These students have many questions that would never occur to their younger peers. To reach these students, in 2018 we launched the Warrior Way Back program, which offers those former students with an outstanding balance of less than $1,500 the opportunity to re-enroll and “learn” away their debt as a way to finally earn a degree. Basically, returning students can reduce their past-due balances by one-third for each semester they are enrolled—until the debt is eliminated.

To put this into context, nearly 700,000 people in the Detroit area have some college/university credits but no degree. That number includes more than 12,000 students who left Wayne State empty-handed. For many of these students, graduation was just around the corner, but financial hardship—sometimes totaling as little as a few hundred dollars—prevented them from reaching the finish line. Too many students are cruelly locked out of completing their education in this way. The Warrior Way Back program is an attempt to rectify this problem.

Of course, financial assistance is not the only support these students need to succeed once they have returned to Wayne State. Upon re-enrolling, students have access to a variety of services and resources designed to guide them toward graduation. Many of these services did not exist during their initial time at Wayne State. As an example, the AI chatbot can help them find out how and where to find childcare services. When these students are told to submit an assignment through a learning management system, W can explain what an LMS is and how to access it.

These are not questions that any returning student should feel embarrassed or afraid to ask. The chatbot allows them to ask these important questions without fear of being judged. In addition, returning students can ask questions no matter the time of day. Many of these students have questions for W during the evening, after campus offices have closed for the day. We are thus now in the middle of launching a version of the chatbot that will be available—anytime and anywhere—through Facebook Messenger.

Even with this AI assistance, in-person guidance and nudges are as vital as ever. But the chatbot has given us more time to focus on these important interactions. W quickly takes care of initial advising questions related to institutional navigation and financial aid, leaving staff with the hours they need to build relationships with students. This dynamic has allowed us to welcome more Pell-eligible, low-income, and first-generation students to campus. It has also allowed us to focus on finding deeper answers to more complicated questions.

At Wayne State, we have discovered that there is no silver bullet to helping our students learn “how to college.” But we now know about several solutions that can work in tandem to help our students succeed. Success is not just about how students learn in the classroom. It’s also about how students interact with the institution. Our students love communicating with staff through the chatbot. Some even send W fan-mail. “I know you’re not real,” one student wrote. “But you’re amazing.”

Dawn Medley (dawn.medley@wayne.edu) is Associate Vice-President of Enrollment Management at Wayne State University.

© 2019 Dawn Medley. The text of this article is licensed under the Creative Commons Attribution-4.0 International License.

We are in an era of significant change in the United States and Canada for publishing open-access (OA) scholarly monographs. Since most monographs are published by university presses, and most copies are purchased by research libraries, this article focuses on that community. The bulk of OA titles are older or out-of-print works, many funded by the Mellon/NEH Humanities Open Book (HOB) program, which enabled free access to backlist scholarly works. Under that program, about 2,500 books from 28 publishers are now OA. Meanwhile, new OA-only book publishers are, together with traditional scholarly presses and libraries, exploring innovative business models and technologies.

Precise numbers of new OA books are hard to calculate. In a 2017 survey, the Association of American University Presses found that 18 of 61 reporting members (out of 140 total member presses) had published new OA books. A few examples include MIT Press, which published its first OA book in 1995 and continues today with MIT Press Open. The University of Michigan Press and Library launched Digital Culture Books in 2006 and now publish new OA books on their library-supported platform, Fulcrum. Athabasca University Press was the first (2007) OA publisher in Canada, with a current list of more than 140 titles. In 2017 the University of California Press began the Luminos OA book program, which now includes more than 60 titles. Other recent examples include Lever Press (2014), Concordia University Press (2016), and the University of Cincinnati Press (2017). In addition, many other publishers have released an occasional OA title, often by posting a free downloadable PDF on their websites.

Beyond the multiple options for creating and disseminating open-access books in new forms, OA monograph publishing projects are driven by the value of releasing scholarship in forms that are free and available to anyone.

Costs and Funding Models

A scholarly monograph is required for tenure and promotion in the humanities and qualitative social sciences. Monographs are also the foundation of most university press lists. Yet OA book publishing has trailed OA journals, for reasons that include the slow emergence of e-books, the high proportion of relatively small nonprofit publishers in the scholarly book business (with little to no capital to invest in new ventures), and, perhaps most fundamentally, the different business models for books.

Though it may seem obvious, it’s worth stating that whereas journals benefit from the advance payment of either licensing revenue or, for many OA journals, article processing charges, each monograph is an individual investment by its publisher. In the traditional model, each title should sell enough copies to cover the costs of acquiring, editing, producing, marketing, and distributing it. Thus, OA monograph publishing has required an estimate of costs upfront.

A number of approaches to establishing costs have been tried. Among the first was Knowledge Unlatched (KU), established in 2012 by publisher Francis Pinter. Publishers proposed new humanities and social sciences books to be made OA if enough libraries crowd-funded them. Presses each established per-title costs to be covered, averaging from $10,000 to $15,000. In its first two rounds (2014–2015), KU “unlatched” over 100 new titles from more than 75 scholarly publishers, with 380 libraries and consortia around the world paying about $50 per title. The books were offered via HathiTrust Digital Library and OAPEN (Open Access Publishing in European Networks). The KU model demonstrated a willingness among libraries internationally to support the costs of OA monograph publishing and among traditional publishers to offer part of their lists free to readers, provided basic expenses could be met. KU changed hands in 2016 and is now a for-profit OA service provider, so it is unclear how the project will continue.

Another new funding model for OA monographs is TOME (Toward an Open Monograph Ecosystem), launched in 2017 through a collaboration among the Association of American Universities (AAU), the Association of Research Libraries (ARL), and the Association of University Presses (AUPresses). One goal was to address a free-rider problem: faculty at virtually all research universities and colleges must publish scholarly books for tenure and promotion, but there are only about 125 university presses in the United States. In addition, the monograph market is shrinking, as library budgets are increasingly devoted to journals. Under TOME, participating institutions provide $15,000 grants to support monographs written by their faculty. Publishers may apply these grants to eligible books, approved through the usual editorial and
peer-review processes, and release OA editions. As of July 2018, 14 institutions and 61 presses are participating, with approximately 20 titles accepted. TOME must grow if the free-rider issue is to be solved.

Luminos, mentioned above, also charges $15,000 per title, to be raised by the publisher, the author or the author’s institution, and libraries. Yet strong evidence suggests that these amounts are insufficient to sustain OA monograph publishing at scale. A 2015 study from Indiana University Press and the University of Michigan Press estimated per-monograph costs to be approximately $257,000. In 2016, Ithaka S+R examined first-copy costs (including acquisitions, manuscript editing, production, design, and marketing but not printing, binding, and shipping) to produce 382 titles from 20 presses. They calculated an average per title of $28,747 for basic costs (staff time and direct costs) and $39,892 for full costs (including press-level overheads).4

A new study is testing whether those costs could be lowered. The University of North Carolina Press is undertaking a Sustainable History Monograph Pilot. It will test a web-based workflow to produce digital-native books to be distributed on OA platforms. Based on usage analytics, publishers may decide whether to invest further in design and production to offer a book in a traditional cost-recovery model. Collaborating partners will test this model with 100–150 history titles over three years.

OA Platforms
The large OA aggregations include titles scanned from print and original ebooks, whose origins are both publishers and libraries, including participants in the HOB program and KU. These providers (e.g., HathiTrust, OAPEN, JSTOR, and Project Muse) have different emphases, with some focusing on preservation and others on format innovation. Creators of OA monographs may rely on one or more of these platforms to disseminate their work.

In addition, several publishers, in collaboration with scholars, libraries, and technologists, have developed distinctive platforms for their own OA offerings, utilizing open-source software. Notable examples include PubPub from MIT; Fulcrum, from the University of Michigan; and Manifold, from the University of Minnesota and CUNY Graduate Center. These tools are available now, and development continues. Each has distinct features and advantages, enabling potential users to select the option that best serves their purposes. Such development, much of it funded by the Mellon Foundation, creates crucial new infrastructure for nonprofit and small publishers.

The Value of OA publishing
Beyond the multiple options for creating and disseminating OA books in new forms, OA monograph publishing is driven by the value of releasing scholarship in forms that are free and available to anyone.

Robin Truth Goodman, professor and associate chair of English at Florida State University and author of Promissory

Notes, the first title to be released by OA publisher Lever Press in 2018, points out a potential tension in publishing specialized scholarship:

The author’s interest is to circulate her ideas as widely as possible, whereas academic presses want to keep their heads above water. So the academic presses tend to price books more highly than scholars and students would want to pay… or delay publication of a paperback to encourage university libraries to buy the hardcovers. For a scholar, this means that books are unavailable for classroom use, or that scholars whose main interests are not in the field would be unlikely to pick the book up. . . . Lever was getting around such concerns by offering immediate access, both in electronic and paperback form.5

Charles Watkinson, associate university librarian for publishing and director of the University of Michigan Press, notes that OA scholarship not only supports that global reach but also generates creativity and interdisciplinary work. Frank Smith, director of books at JSTOR, reports usage data indicating truly global access: JSTOR’s 5,000 titles have received millions of uses (chapter downloads and views), evenly distributed across geographic locations and institutions worldwide. Brett Bobley, CIO and director of the Office of Digital Humanities at the NEH, cites the example of Cornell University Press, which learned that within about two years, its 77 OA books had received 100,000 chapter downloads and 200,000 views on JSTOR and MUSE from people in 152 different countries and had been downloaded 29,000 times on Amazon.6

In an era when the average scholarly monograph sells only a few hundred copies, this usage—in both numbers and geography—suggests that the audience for these works is far larger than the market for them. The cost studies and technical innovations underway are particularly significant, emerging as they do from the nonprofit publishing sector. If colleges and universities truly wish to make a global impact, investing in open-access monograph publishing is one promising way forward. ■

Notes
5. Email to the author, February 14, 2019.

Monica McCormick is Associate University Librarian for Publishing, Preservation, Research and Digital Access at the University of Delaware Library, Museums and Press.

© 2019 Monica McCormick. The text of this article is licensed under the Creative Commons Attribution 4.0 International License.
Security versus surveillance—what’s the difference? And how can we—IT staff and leaders—engage the campus community in a security and privacy discussion that supports different points of view on technology choices so that we can take advantage of the opportunities to secure the campus environment and protect privacy? New technologies offer new capabilities, but they also have the potential to create controversy on campus. How can we ensure that security and privacy reinforce, rather than wrestle against, each other? We have the ability, now more than ever, to be extremely proactive to ensure that our students, faculty, and staff have amazing—and secure—learning, education, and research services. Are we doing enough to protect our community, or are there opportunities to do more?

When we reflect on the primary goals of higher education, student success is undoubtedly a key pillar. In fact, some might even go so far as to say it defines the very reason for the college/university’s existence. Enabling student success includes leveraging technology to build robust communities, provide high-quality services that deliver a top-notch learning experience, and protect our students during their time at our institution in a way that meets today’s rapidly evolving security and privacy expectations.

What’s stopping us from rapidly delivering increasingly relevant services to meet our institutional goals? I’d like to challenge our line of thinking and have us consider whether it’s time for a course correction. Are we envisioning alignment between privacy and security (rather than a collision course), proactively addressing threats entering our domain (rather than passively standing by or, worse yet, surveilling), and leveraging technology to integrate for a seamless and safe experience? If we aren’t quite sure the answer is yes, let’s explore for a moment how we might go about this differently.

With significant technology advancements in recent years, we have increasing capacities to collect and store data at rates nearly unthinkable only a few short years ago. In fact, Statista predicts that by the end of 2019, we will have 26.66 billion internet-connected devices across the globe. These solutions, combined with the power of our enterprise service capabilities, afford greater opportunities to streamline and simplify the education and research experience, moving well beyond wayfinding to collaboration with friends and to event suggestions provided via a voice-enabled campus technology, all while offering increasingly improved services to protect our students so that they can focus on their education.

Why aren’t we leveraging these capabilities to deploy services more quickly? For one thing, there is more than a little work involved in bringing these solutions in, as we push the boundaries of today’s service capabilities while at the same time ensure that each new initiative doesn’t upset the delicate balance of operational activities or risk acceptance. But let’s envision a world where we speed up our deployments, taking us from where we are now to third, fourth, or ultimately fifth gear. Let’s lean in to the technical advances of the last decade and incorporate intelligent observation to ensure we aren’t simply moving to a data-collection model that may serve more to surveil our communities than to actively protect them.

How could we improve? First, all of our teams should be focused on delivering services that meet both
In a world that is increasingly defined by data and information, those of us in higher education information technology must question our assumptions about security and privacy as we move forward. Above all else, we must listen to our students, faculty, and staff and foster a community of raving fans.

- **Building trust in our community** means that we are transparent in the services we provide and how we leverage the data. In a world where there is a tendency to collect more data than we need, keep it for longer than we should, and react to security breaches rather than proactively combatting the threat, it is increasingly important for us to communicate early and often. Managing data responsibly requires that we clearly articulate the uses for data collection and that we store data only as long as it is needed to provide a service.

- **Designing with privacy in mind** consists of considering the protection of personal data during each step of the development, design, selection, and use of IT services and systems. Creating this culture within our organizations is essential.

- **Embedding security in our development initiatives** requires that proactive security is a fundamental principle for which each of us—not just one individual or one small team—is responsible.

- **Integrating and automating** removes manual processes and frees up staff for higher-value work.

- **Moving quickly** by creating a vibrant Development/Security/Operations (DEV/SEC/OPS) culture with a bias toward action helps us lean in to the agile mindset.

At ASU we proactively seek opportunities to embed these concepts into our design principles. We embed security analysts and architects with cloud development teams, investing in security tools to aid development efforts and organically producing increasingly security-focused development. The result is rapid deployment of new application features with significantly more robust security from the start. ASU has taken a similar approach to meet transparency and privacy concerns: the security office has instituted a governance structure in conjunction with the provost’s office to elevate privacy discussions and decision-making involving stakeholders and executive leaders from across university departments and units. This action has resulted in a collaborative and high-functioning ASU privacy team. Continuing with our theme of being deeply embedded, ASU has a long-standing culture of empowering staff to buy enterprise solutions where well-established commercial solutions exist, thus freeing up staff time to focus on creative efforts to build innovative solutions to meet the various needs of our community. In a specific use case related to the constant barrage of cyberthreats, for example, we’ve constructed a set of fully automated email, firewall, and identity solutions that leverage robust threat intelligence to take immediate action to protect the university from external attacks, again freeing up staff to focus on higher-value initiatives.

Let us challenge ourselves and our IT teams to tackle this paradigm shift, building trust through meaningful transparency, thinking about privacy first, embedding proactive security in everything we do, integrating systems to remove repetitive tasks, and removing barriers that keep us from moving quickly. Let’s dream big and take time to imagine the “art of the possible.”

In a world that is increasingly defined by data and information, those of us in higher education information technology must question our assumptions about security and privacy as we move forward. Above all else, we must listen to our students, faculty, and staff and foster a community of raving fans.

**Note**


---

**Tina Thorstenson** is Deputy CIO for IT Governance, Policy, and Information Security at Arizona State University and also continues to serve as Chief Information Security Officer, a position she assumed in September 2009.
A Strategic Leader for Student Success: An Argument for the Chief Academic Technology Officer

Academic technology is changing. Instruction is becoming more of a team sport: instructional faculty want support from professionals who are fully versed in technology, video production, disciplinary content, and the evidence-based pedagogical practices documented in the scholarship of teaching and learning. Active learning classrooms and faculty development efforts can help increase passing grades, learning, comprehension, and content retention for all students—and disproportionately so for students from underrepresented groups.

The explosion of new academic technology facilities (e.g., innovation labs, makerspaces, data-visualization labs, and studio classrooms with learning glass or light boards), as well as third-party services (e.g., educational video-streaming services, applications that can be integrated into the LMS, and systems that offer API access to data), demand the oversight and management of knowledgeable academic technology staff.

These changes in academic technology are potential solutions to improving student success. Data analytics, early warning, intervention, and advising systems promise to ameliorate DFW (D/F/Withdrawal) rates and attrition. Course planning software for administrators and for students can help identify and resolve course sequencing or scheduling issues, shorten curricular pathways, and increase access to gateway courses—all of which should contribute to improved time-to-degree and graduation rates. The fusion of data management, data visualization, research computing, and digital scholarship with digital pedagogy prepares students intellectually, technologically, and practically. Offering hands-on experience in cutting-edge technology could be the differentiating factor in post-graduation job searches.

At many institutions, the evolution of online education—from adult education to MOOCs to hybrid and exclusively online mainstream degree programs—brings together the work of extension and distance education units with courses for matriculated students. To support accessibility efforts that increase inclusivity and equitable access for all students, we need technical expertise embedded whenever and wherever we create instructional and scholarly content. College affordability initiatives such as the adoption of open educational resources (OER) require digital publishing platforms and secure and collaborative ancillary materials platforms, as well as expertise in technology, security, academic publishing, and copyright. Legislation and a national spotlight on affordability only add to the pressure to ramp up academic technology infrastructure and services in support of student success.

All these developments in academic technology demand an institutional academic technology strategy—one that, arguably, a Chief Academic Technology Officer (CATO) can best articulate, socialize, and invest in. Over a decade ago, Michael J. Albright and John Nworie advocated for the establishment of “a senior academic technology officer to serve as a visionary, leader, director, planner, facilitator, collaborator, catalyst, advocate, change manager, and evangelist to coordinate all applications of instructional technology in meeting the institution’s academic goals.” Ten years later, the Big Ten Academic Alliance (BTAA) Learning Technology Leadership (LTL) group recognized the emergence of these roles as uniquely positioned at “the intersection of learning and technology.” Simultaneously, the Center for Higher Education Chief Information Officer Studies (CHECS) released its inaugural CATO survey, reporting that the portfolio of the CATO includes, predictably, hardware- and software-based facilities and platforms such as the LMS, classrooms, media services, enterprise academic software, research computing, labs, and help desks. In addition, CATO portfolios are branching out to include other specializations such as online/distance education, teaching centers, and libraries, along with people-intensive services such as instructional design and faculty development, all of which require fluency with the academic culture and a pedagogical formation.

The CHECS survey delved into the demographics, pipeline, reporting structure, and aspirations of CATOs. Of the respondents to the CATO survey, 44% identified as female, compared with 24% of CIOs and 30% of higher education presidents. While CIOs out-earn CATOs by approximately $20,000, female CATOs earned an average of $10,000 more than their male counterparts. When asked about their career aspirations, CATOs represent an incredibly stable workforce: 51% want to remain in their current position or serve as a CATO at another institution.
Many CATOs are internal hires, offering a deep understanding of institutional culture. Comparing data from the CATO survey and the CHECS CIO survey shows that both CATOs and CIOs have spent about fifteen years in higher education information technology. Interestingly, CIOs have spent about seven years in IT departments outside of higher education, while CATOs report roughly the same amount of time within higher education but outside of information technology. Finally, 95% of CATOs hold advanced degrees (54% master’s degrees, 41% doctoral degrees), compared with 81% of CIOs and 70% of CISOs (chief information security officers). Of these degrees earned by CATOs, 29% are in education, 20% in technology, and 12% in the humanities.¹

These datapoints ask more questions than they answer, but they are questions worth further exploration. Over the fifteen years of CHECS research reports, the majority of CIOs indicated that their ideal reporting relationship was to the president/CEO; in reality, only 34% of CIOs report to the CEO, and another 34% report to the CFO. Only 8% of CIOs stated that reporting to the provost was ideal, whereas 46% of CATOs indicated that their ideal reporting relationship was to the provost or chief academic officer.² So if the CATO is more closely aligned with the provost’s portfolio, are we seeing the emergence of a new “table” where academic decisions should be made? Who else should be sitting at this table? Research, teaching and learning, libraries, the registrar, academic affairs, student success, graduate schools, and the academic senate all have unique contributions to make to a new kind of partnership critical to student success.

We do not advocate for any particular reporting structure: no one size will fit all. On the other hand, we do argue for the establishment of a CATO to provide expert insight and direction to a changing academic technology landscape. Reflecting on the emergence of C-level positions—first CIOs, then CISOs, and more recently, CPOs (chief privacy officers)—we posit that the “chief” title is indicative of a level of complexity in operations and a need for strategic investment. The proliferation of CIO positions followed the explosion of the World Wide Web and the emergence of multi-million-dollar investments in networking and administrative systems. Higher education required a CIO to manage these investments on behalf of the institution. The rapid growth and risk of cybersecurity incidents demand the creation of CISO positions. CPOs—both in higher education and in industry—are tasked with complying with and managing the associated risk of the increasingly complex legal and technical landscape.

The educational technology industry has grown up quietly in the shadows of cybersecurity and has emerged as a distinct technology sector in its own right. We are familiar with the LMS and digital publishing markets, but the ed tech market also comprises small and medium-sized companies whose innovative practices challenge us to rethink our policies, traditions, and practices. It is time to establish the CATO position—an officer with a deep understanding of academic culture and a collaborative approach—to help meet the research, scholarly, and instructional needs of faculty and students while working closely with CIOs, CISOs, CPOs, and the institutions to ensure privacy, security, and accessibility.

The role of the CATO is to “provide strategic leadership and direction for academic technology applications, initiatives, and support services across the broad spectrum of instructional technology functions; provide leadership in planning and policy related to curriculum development, e-learning, and other instructional technology initiatives that facilitate achievement of the institution’s strategic goals; and build partnerships among campus academic support units to work collaboratively toward achievement of institutional goals that can be addressed through instructional technology.”³ The CATO solves academic, research, curricular, and pedagogical problems—at scale—through the strategic application of technology.

The goal of creating the CATO position—and defining a career path for academic technology professionals—is about developing a structural framework for deep collaborations among academic campus partners to support the strategic role of academic technology in the research and instructional mission. It is about advocating for the future of higher education: what these positions and partnerships can accomplish on our campuses and nationwide; how we can preserve the core research and instructional mission in a rapidly changing digital landscape; and how we can lead and significantly improve student success.

Notes
5. Ibid.

Helen Y. Chu (helenc@uoregon.edu) is Associate Dean of Libraries and Chief Academic Technology Officer at the University of Oregon. Bill Hogue (wfhogue@gmail.com) is Executive Coach in the MOR Leadership Programs and retired CIO, University of South Carolina.

© 2019 Helen Y. Chu and Bill Hogue
Spring Cleaning: Security and Privacy

Spring is traditionally a time for cleaning and organizing. Information security and privacy practices need as much upkeep as (or more upkeep than) storage sheds and closets. In fact, in the EDUCAUSE 2019 Top 10 IT Issues research, Information Security Strategy was #1 and Privacy was #3. Find out how higher education institutions view and treat these critical topics.

INFORMATION SECURITY STRATEGY

What it means: Developing a risk-based security strategy that effectively detects, responds to, and prevents security threats and challenges

What are the biggest threats?

79% Exposure of confidential or sensitive information

- 31% Email viruses, ransomware, or other malware
- 29% Unauthorized or accidental modification of data
- 27% Unauthorized, malicious network or system access
- 16% Loss of availability or sabotage of systems

Are institutions offering training?

- 85% Mandatory information security training for faculty or any staff
- 49% Mandatory information security training for students

What’s the leadership and spending landscape?

- 41% Institutions with a dedicated person whose primary responsibility is information security
- 3.6% Central IT spending on information security as a percentage of total central IT spending

Source: EDUCAUSE Information Security Almanac 2019
PRIVACY

What it means: Safeguarding institutional constituents’ privacy rights and maintaining accountability for protecting all types of restricted data

How do stakeholders view privacy practices?
In conducting student success studies, privacy rights are respected:

- 94% Strongly agree or agree
- 5% Neutral
- 1% Strongly disagree or disagree

Source: AIR/NASPA/EDUCAUSE data

What are the most common mandatory training topics for students?

- Usage policies (AUP) 36%
- Security policies 23%
- Self-defense (e.g., phishing) 23%
- Privacy policies 21%

How are institutions employing identity and access management?

- 75% Institutions that are tracking, planning for, or have partially deployed nonbiometric multifactor authentication (MFA)
- 17% Institutions that have fully deployed nonbiometric MFA

Source: EDUCAUSE Information Security Almanac 2019
## A Shared Commitment

Our goal of advancing the future of higher education is shared by our corporate Platinum Partners. We thank them for their unparalleled support.

<table>
<thead>
<tr>
<th>Company</th>
<th>Contact</th>
<th>Website</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blackbaud, Bronze Partner</td>
<td>1-800-443-9441</td>
<td><a href="http://www.blackbaud.com/highered">www.blackbaud.com/highered</a></td>
<td>15</td>
</tr>
<tr>
<td>Computer Comforts, Silver Partner</td>
<td>1-281-535-2288</td>
<td><a href="http://www.computercomforts.com">www.computercomforts.com</a></td>
<td>21</td>
</tr>
<tr>
<td>Jenzabar, Platinum Partner</td>
<td>1-800-393-0028</td>
<td><a href="http://www.jenzabar.com">www.jenzabar.com</a></td>
<td>Inside front cover</td>
</tr>
<tr>
<td>LaptopsAnytime</td>
<td>1-877-836-3727</td>
<td><a href="http://www.laptopsanytime.com">www.laptopsanytime.com</a></td>
<td>3</td>
</tr>
<tr>
<td>Laserfiche, Gold Partner</td>
<td>1-800-985-8533</td>
<td><a href="http://www.laserfiche.com">www.laserfiche.com</a></td>
<td>Inside back cover</td>
</tr>
<tr>
<td>LogMeIn, Gold Partner</td>
<td>1-866-631-9713</td>
<td><a href="http://www.logmeinrescue.com">www.logmeinrescue.com</a></td>
<td>4</td>
</tr>
<tr>
<td>Nelnet Business Solutions, Bronze Partner</td>
<td>1-888-867-7018</td>
<td><a href="http://www.campuscommerce.com">www.campuscommerce.com</a></td>
<td>Back cover</td>
</tr>
<tr>
<td>SMARTdesks, Bronze Partner</td>
<td>1-800-770-7042</td>
<td><a href="http://www.smartdesks.com">www.smartdesks.com</a></td>
<td>17</td>
</tr>
</tbody>
</table>

-educause.edu/corporate-partners
Share ideas.
Grow professionally.
Discover solutions.

Registration opens in June, so plan to join the best thinking in higher education IT!
Strengthening Higher Education Together

EDUCAUSE thanks our 2019 Corporate Partners for playing a meaningful role in helping higher education deliver on its mission!

We also thank 375+ additional corporations that support our community. educause.edu/corporate-partners
Trusted Content Services Platform for Higher Education

- Accelerate process automation across campus, from HR and Contract Management, to Student Services and Research Administration
- Integrates with SIS, ERP, CRM, HR and Homegrown systems
- See ROI in as few as 8 minutes

To learn more, visit info.laserfiche.com/TopTen2019
Payment technology for a smarter campus

“A great client experience is one that provides a combination of self-service technology with human expertise and empathy. That’s what makes us different in the marketplace.

It all starts with our people. That’s where we turn passion for the business into best-in-class customer service. Because that’s what a partner does — and that’s what a partner deserves.”

— MATT SPETHMAN, DIRECTOR OF CLIENT EXPERIENCE

Experience Smarter

CampusCommerce.com/ExperienceSmart