EAB

IT Forum

Virtual Executive Roundtable

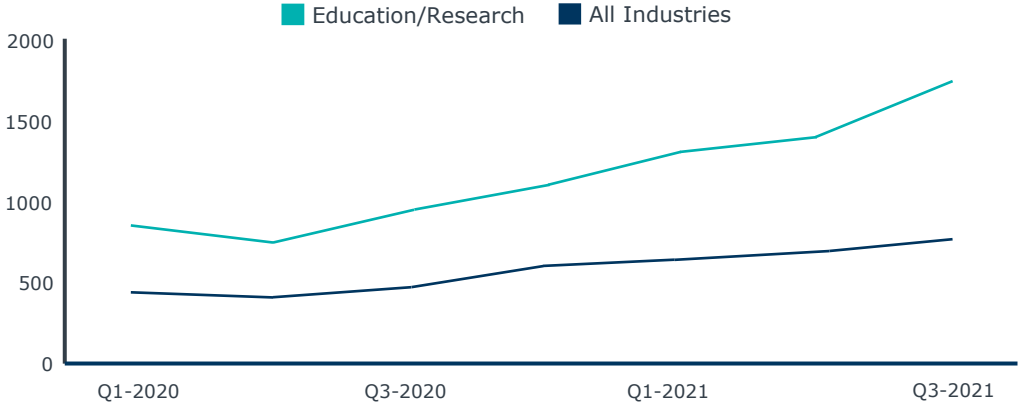
Enhancing IT's Cyber Risk Management Capabilities: Pinpointing High-Value Security Investments and Staffing Solutions in Higher Ed

We will start promptly at 10:03 AM EST once everyone has joined

Higher Ed a Particularly Appealing Target

No Industry Has Been Spared—but Ours Bears the Brunt

Weekly Average Attacks per Organization Globally



Education: the New Hotspot for Cyberattacks

3,936%
increase in security incidents in education from 2013 to 2020

200%
increase in attacks on education during peak of the pandemic (March and August 2020)

44%
of educational institutions in a survey of 499 IT leaders were hit by ransomware in 2020

Source: BlueVoyant, "Cybersecurity in Higher Education Review", *BlueVoyant*, 2021; Check Point Research, "Education sector sees 29% increase in attacks against organizations globally," *Check Point*, August 8, 2021; CheckPoint, Not for higher education: cybercriminals target academic & research institutions across the world," *CheckPoint*, 2020; Sophos, "The State of Ransomware in 2021", *Sophos*, July 2021; Verizon, "2014 Data Breach Investigations Report", *Verizon*, 2014; Verizon, "2021 Data Breach Investigations Report", *Verizon*, 2021; EAB interviews and analysis.

My, What Big Data You Have

Many Factors Make Higher Ed a Valuable (and Vulnerable) Target

High Volume of Valuable Data

Personal, financial, and medical information on par with banks, hospitals, etc. – without the same level of protection

Research & Intellectual Property

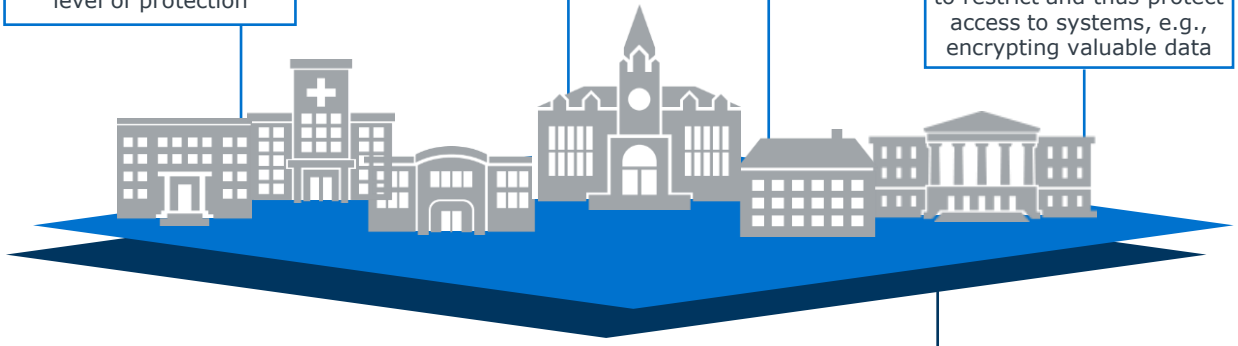
Research (especially government or industry-sponsored) is a profitable target for hackers

Digital Sprawl

Sprawl and lack of adherence to basic security measures, e.g., vendor security assessments

Open Academic Environment

Culture of academic freedom means reluctance to restrict and thus protect access to systems, e.g., encrypting valuable data



Pandemic Exacerbated Historical Weaknesses

- Increased network and system architecture complexity
- Increased number of unprotected devices accessing environment
- Increased vendor purchases and products

Resource Scarcity

Unable to compete in labor market or dedicate resources to posture at level comparable to similar private organizations

Source: EAB interviews and analysis.

Cyberattacks Cost So Much More Than a Ransom

Atlanta Shells Out $17M for a $52K Ransom (Which They Didn't Pay)

Approximate Costs

Restoring the city's computer networks	*$2.7 million*
New devices (e.g., laptops, smart phones)	*$1.1 million*
Immediate post-incident consulting services with eight different firms	*$1.5 million*
Legal fees:	
Law firm	*$485 per hour*
Law associates	*$300 per hour*
Upgrading security and software services	*$6 million*

Average Total Cost of a Single Data Breach in Education in 2020

$3.9M

Insurance Premiums Are Rising, Even Without Attack History

300%

Reported increase in insurance premiums and deductibles, with sub-limits on certain types of events like ransomware and co-insurance requirements, according to Katherine Mayer, AVP of information security at the University of Wisconsin

Source: IBM Security, "Cost of a Date Breach Report 2021", *IBM*, July 2021; J Jorstad, "Higher-Ed Cybersecurity Insurance: Are You in Good Hands?", *GovTech*, November 19,2021; S Deere, "Cost of City of Atlanta's cyber attack: $2.7 million — and rising," *The Atlanta Journal-Constitution*, October 1, 2019; EAB interviews and analysis.

A Shift in the Tide

> “A recent attack on a neighboring institution scared our board and senior leadership into action. We suddenly got a blank cheque to upgrade our security posture.”
>
> — Chief Information Officer
> *Private Research University*

Quick Recap of First Session from Last Month

PART 1 : DEVELOPING A SECURITY-FIRST CAMPUS CULTURE

I. Building Leadership Commitment to Enterprise-Wide Security

Tactic 1: Proactive Risk-Rated Escalation Paths (Vanderbilt University)

Tactic 2: Executive-Level Tabletop Exercises (Arizona State University)

Tactic 3: Cyber Enforcement Mandate from the Board (Virginia Tech University)

Tactic 4: Monthly Risk-Based System Quarantines (Rice University)

II. Improving End-User Engagement in Security

Tactic 5: Components of Effective Training

- Gamified Security Platform (Ohio State University)
- Department-Tailored Training (Arizona State University)
- Mandatory Training with Penalties for Non-Compliance (Barry University)
- Monthly Self-Phishing (Fairfield University)

If you missed this session, feel free to request the slide deck from your strategic leader, schedule a call with our experts, or have our experts facilitate a conversation with your boards and cabinets.

Today's Focus

PART 2: ENHANCING IT'S CYBER RISK MANAGEMENT CAPABILITIES

I. Case Studies of Leading Edge Technologies in Higher Ed

Tactic 1: User-Focused Security Enhancement Tools

- Password Managers
- Mobile ID and Wallet
- User Driven Sensitive Data Removal
- Unit Security Dashboard

Tactic 2: Proactive and Automated Security Management Tools for IT and InfoSec

- Cybersecurity Asset Management
- Extended Detection and Response Tools
- Risk-Based Microsegmentation

II. Practical Staffing Solutions to Address Talent Shortage

Tactic 3: Benefits Value Sell Document

Tactic 4: Apprenticeship Programs

Tactic 5: Distributed IT Responsibilities

Tactic 6: Shared SOC Among Universities

EAB

Case Studies of Leading Edge Technologies in Higher Ed

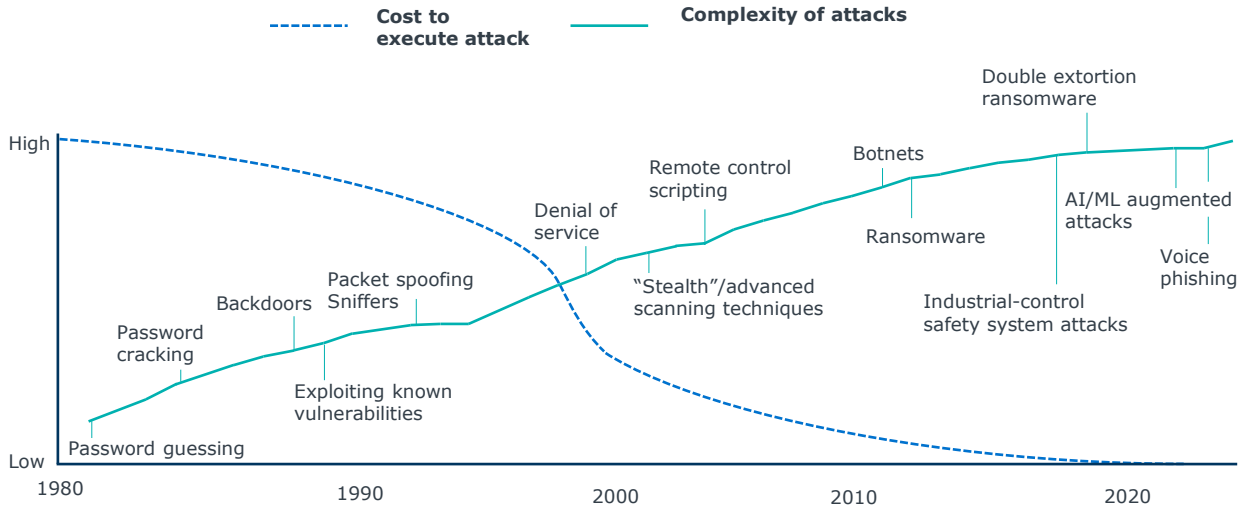
SECTION 1

- Tactic 1: User-Focused Security Enhancement Tools
- Tactic 2: Improved Security Management Tools for IT

A Struggle to Keep Up

Evolving Threats Require Stronger Defenses

Attacks Have Become Both More Sophisticated and Cheaper to Execute



Source: Boston Consulting Group, "The CEO's Guide to Cybersecurity", *BCG Executive Perspectives*, September 2021; EAB interviews and analysis.

The Right Tool for the Job

Private Institution Sees Value from XDR Just from Short Demo

XDR Demo and Implementation

CHALLENGE ▶ IMMEDIATE VALUE ▶ CONTINUOUS RESULTS ▶

Reeling from an attack

A small, private institution was undergoing a CrowdStrike Falcon pilot when it was targeted by a NetWalker ransomware attack amid COVID.

"[With such a small IT staff], we cannot have our eyes on everything all the time."

Minimizing Damage and Exposure

The pilot CrowdStrike Falcon XDR[1] services alerted the institution to the threat and began remediation workflows, resulting in:

30% **Impacted Infrastructure,** substantially less than expected and shielding the main ERP and SIS from contamination

64 **Devices** touched by malware

4 **Weeks** of recovery with the aid of CrowdStrike Falcon to conduct a forensic investigation and restore full operations

Ongoing and As Needed

Within first 18 months of use, security team has:

- Received an average of 2-3 notifications to investigate vulnerabilities per week
- Identified and resolved 2 major vulnerabilities
- Recouped time from monitoring logs for higher order tasks

1) XDR refers to Extended Detection & Response

Source: EAB interviews and analysis.

Our Focus Today

Case Studies of Emerging Technologies in Higher Ed

Two Aspects of Cybersecurity Technology We'll Discuss Today

For End-Users

Enhancing the Security Experience for Users

- User Driven Sensitive Data Removal
- Password Managers
- Mobile ID and Wallet
- Unit Security Dashboard

For IT and InfoSec Teams

Improving IT's Security Management

- Extended Detection and Response
- Cybersecurity Asset Management
- Risk-based Microsegmentation

Source: EAB interviews and analysis.

Empower Users with Tools to Purge Sensitive Data

User-Driven Sensitive Data Removal

Institutions introduce data loss prevention technologies that proactively scan devices for personal information (PI). IT then equips units with remediation steps to protect or remove the PI, ensuring the institution reduces potential exposure in cyberattacks

1 Identify high-risk units

Install automated data loss prevention software in high-risk units or roles more susceptible to attacks or more likely to have PI incorrectly stored.

2 Automate device scanning

While voluntary adoption and on-demand scans are steps in the right direction, we recommend automating the scanning to occur at least monthly

3 Recommend remediation actions

A representative from each college/division receives detailed reports provide guidance on how to destroy the files or redact the PII.

4 Generate buy-in from core users

For UND, the tool is deployed in every machine. But users have the option to run it. This optionality helped with getting approval from the faculty senate. For RIT, they were able to build consensus for automating the scans.

SPIRION OHIO UNIVERSITY RIT UND UNIVERSITY OF NORTH DAKOTA

Source: link to the pages. Ohio University, Athens County, Ohio; Rochester Institute of Technology, Rochester, NY; University of North Dakota, Grand Forks, ND; EAB interviews and analysis.

Reduce User Password Frustration

Stanford Provides 1-Yr Premium Password Manager for All, Including Students

Key Features of Stanford's Password Manager

Stanford University

DASHLANE

Manages Passwords Across Devices

Dashlane stores passwords and keeps them up-to-date across phones, computers, tablets and other devices, including personally owned devices

Supports Two-Factor Authentication

Offers 2FA for safeguarding the master password

Free of Charge For All Faculty, Staff, and Students

Anyone with an active stanford.edu account is provided with a premium account for a year

Business Accounts Provided for Faculty and Staff Groups

Allows groups to securely share passwords. Also provided free of charge.

Source: Stanford University, Stanford, California; EAB interviews and analysis.

Quick Poll 1

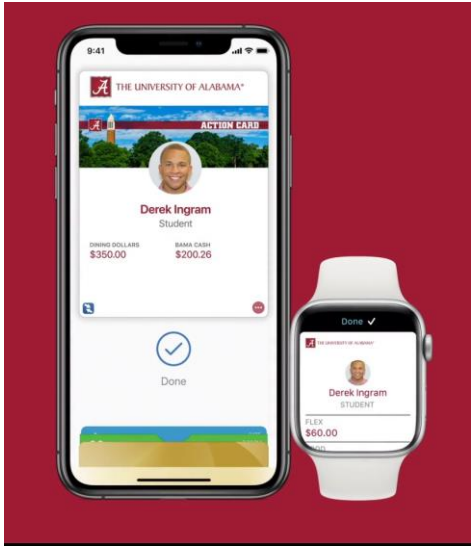
Do you currently offer password managers for users? (select all that apply)

a. For IT staff only
b. For staff in specific business units
c. For all staff
d. For all faculty
e. For all students
f. We don’t have this option

Make ID Authentication Easier for Users

Replacing ID Cards with More Secure and User-Friendly Alternatives

Action Card Incorporated in Phones and Watches



Program in Brief

THE UNIVERSITY OF ALABAMA

- Alabama's physical ACT Card replaced by mobile ID cards in iPhones, Apple Watches, and compatible Android devices
- Students, faculty, and staff can access buildings, purchase meals etc. simply with their Phones and Watches
- All new students (plus students who lost their physical IDs) since 2020 required to use mobile ID cards
- Project a collaboration between UA's IT, Access Control, Bookstore, Event Access, Dining Services along with Transact, Apple, and Google

Benefits of Mobile IDs

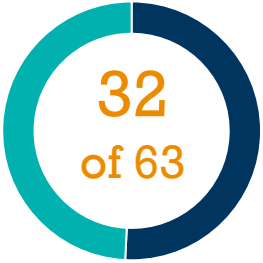
- Not easily lost or shared: 5,000 physical cards lost in 2017
- Contactless access: Users simply present their phone or watch to NFC-enabled devices
- Efficient transactions: No fumbling around looking for cards or swapping between cardholders
- Environmentally friendly: No plastic wastage
- Easy to replace: Users can download, freeze when lost, and reactivate mobile ID cards remotely
- Enables business continuity: Chip cards difficult to procure during supply chain constraints

Source: University of Alabama, Tuscaloosa, Alabama; EAB interviews and analysis.

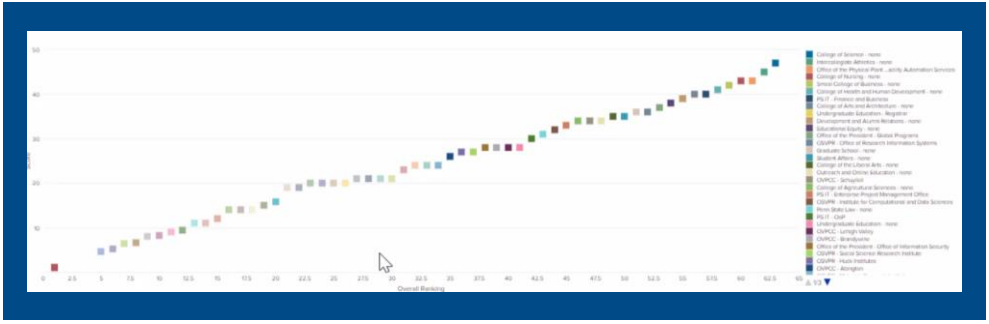
Putting Security Performance Data in Users' Hands

Penn State Unit-Level Dashboard Provides Visibility at All Times

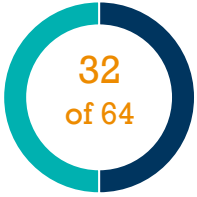
Overall Ranking



Comparison to Other Units' Overall Score and Ranking



Vulnerabilities
60% of overall score

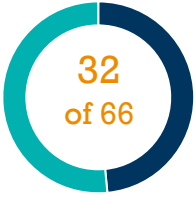


Immediate attention

Authorization To Operate
20% of overall score

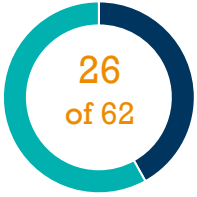
Good performance

Unsupported OSs
15% of overall score



Needs improvement

Compromised Acc.
5% of overall score



Needs improvement

Source: Pennsylvania State University, State College, PA; EAB interviews and analysis.

API Driven Asset Inventory

Axonius' Cybersecurity Asset Management Platform

Pennsylvania State University uses Axonius to get clear visibility on assets, both on-prem and cloud, across their distributed IT environment

PennState

Reduces Time to IT Asset Inventory

Correlates data from all sources to provide a continuous, up-to-date inventory of all unique assets

- Can be deployed on-prem, or private cloud, or an AWS-hosted SaaS solution.
- Once deployed, Axonius connects to solutions you're already using adaptors (over 400 pre-built integrations on the platform).
- Provides a unique list of devices, users, and cloud assets in the environment.

Discovers Coverage Gaps and Surfaces Risks

Enables security control validation by identifying problematic assets

- Identifies devices that are missing or malfunctioning security controls (via queries)
- Finds rogue devices and unwanted software or with missing vulnerability scans and patches
- Helps during incident response by indicating device coverage and context

Validates Policies and Automates Response

Security Policy Enforcement Center can be used to notify personnel, enrich data, and configure assets automatically

- Notifies the right teams when assets don't meet policies
- Creates incidents via ticketing system
- Can directly install missing agent on the device if credentials are supplied and machine is reachable on the network

Source: Pennsylvania State University, State College, PA; EAB interviews and analysis.

Quick Poll 2

What is your current approach to asset management?

a. We have created an asset management system in-house
b. We use a vendor-based solution
c. We are considering a solution for asset management
d. We don’t need an asset management solution

Microsegmentation Limiting Lateral Movement

UNIVERSITY OF Nebraska

Access Based on Who You Are and the Security Posture of Your Device

- Users categorized into seven groups, based on their level of exposure to sensitive data
- Posture of device assessed each time to check that it's adequately configured to access the network level appropriate for the role. If not, user downgraded to lower level of network access
- This model shifts more responsibility and control to the endpoint (i.e., linking access to not only identity but also device posture) which suits itself well to remote and hybrid environments

Network Access Requirements

Network Segment	Endpoint Class	User Group	Endpoint Posture	Authentication	Access
Noncompliant	Noncompliant Devices	Institution Identities	Documented Exception	User *-and-* Device *-or-* Device & v IoT	Internet
Untrusted	Unknown Devices	Guests, Conference Attendees, eduroam Peers, & IoT MPSK	No Requirements	User *-or-* Device v v IoT	Internet
Low Risk	Personal or Institutional Devices, Digital Signs, Printers, & other IoT	Institution Identities & IoT MPSK	BYO w/NAC Agent -or- Managed with Low Risk Controls	User *-and-* Device *-or-* Device & v IoT	Internet, Printers, IoT, & Low Risk Services
Medium Risk	Institutional Desktops, Laptops, & Mobile Devices	Institution Employees	BYO w/NAC Agent -or- Managed with Medium Risk Controls	User *-and-* Device &	Internet, Printers, IoT, Low & Medium Risk Services
High Risk	Institutional Desktops, Laptops, & Mobile Devices	Limited Institution Employees	Managed with High Risk Controls	User *-and-* Device &	Internet, Printers, IoT, All Risk Services
Research	Institutional Desktops, Laptops, Mobile Devices, & Required IoT	Limited Institution Employees & IoT MPSK	Managed with High Risk Controls	User *-and-* Device *-or-* Device & v IoT	Variable by Requirement
IT Infrastructure	Institutional Desktops, Laptops, & Mobile Devices	Limited Institution IT Employees	Managed with High Risk Controls	User *-and-* Device &	Internet, Printers, IoT, All Risk Services, Data Centers, & Network Infrastructure

Source: University of Nebraska, Lincoln, NE; EAB interviews and analysis.

EAB

Adopting Practical Staffing Solutions to Address Talent Shortages

SECTION 2

- Tactic 3: Benefits Value Sell Document
- Tactic 4: Student Apprenticeship Programs
- Tactic 5: Distributed Security Responsibilities
- Tactic 5: Shared SOC Among Universities

Cybersecurity Expertise in High Demand

While Higher Ed Struggles to Keep Up with the (Private Sector) Joneses

Higher Ed Is Not Alone in Talent Crunch…

94%

Increase in IT cybersecurity job postings since 2013, 3X faster than IT jobs overall

20%

Longer to fill cybersecurity roles compared to other IT roles

18 months

Average tenure of cybersecurity staff at J.P. Morgan and Raytheon

…But Certainly, at a (Pay) Disadvantage

Higher Ed Funding Structure Limits Ability to Raise Wages…

- Tightening budgets
- Inability to pass along costs to customers

…and Wage Increases Fraught with Ongoing Concerns

- Uncertain funding for recurring wage increases
- Existing staff discontent over wage compression

Severe labor competition will only intensify as US Bureau of Labor Statistics projects that demand for information security analysts will grow 31% from 2019 to 2029, compared to 4% in other industries

Source: "The Demand for Cybersecurity Skills Is Outstripping the Supply of Skilled Workers," IBM; "Top Cybersecurity Skills for 2021," Burning Glass; EAB interviews and analysis.

Quick Poll 3

How are you meeting the need for cybersecurity staff and skills? (Choose all that apply)

a. Making the case to leadership/HR for higher salaries
b. Leading with benefits/quality of life when recruiting
c. Developing internal candidates
d. Participating in consortial/system SOC
e. Contracting with commercial provider

What Job Seekers Want (Beyond Pay)

Higher Ed Offers Compelling Benefits and Perks That Candidates Value

Candidates Place Premium on Benefits Packages in Employment Decisions…

57%
rank benefits and perks as a top consideration for accepting job offer

76%
at least somewhat likely to accept a more robust benefits package for lower compensation

9%
pay increase needed to overcome preference for hybrid work option

…Particularly Benefits that Higher Ed Offers (and Private Sector Might Not)

% of employees valuing select benefits more than pay raises, 2015

37%	Vacation and paid time off
31%	Retirement plan and/or pensions
30%	Flexible schedule

Source: "Glassdoor Employment Confidence Survey (Q3 2015)", *Glassdoor*, October 12, 2015; "Glassdoor's 5 Job Trends to Watch in 2016", *Glassdoor*, January 12, 2016; WFH Research, Dec 2021; EAB interviews and analysis.

Quantifying Non-Monetary Benefits

CU Anschutz's Compensation Snapshot Showcases Total Value of Job Package

Your Total Compensation Snapshot[1]

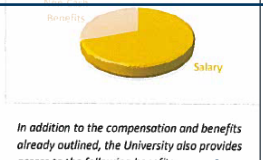
Name
EID:

ILLUSTRATION

University Paid Compensation (as of July 31, 2017 payroll)	
Cash Compensation	
Base Salary/Cash Compensation	***$115,419.00***
Health Benefits	
Medical Insurance	$11,454.00
Dental Insurance	$318.00
Annual Total	***$11,772.00***
Additional University Paid Benefits	
Basic Term Life Insurance, Accidental Death & Dismemberment, and Disability Coverage	$291.60
Fringe/Additional Benefits *(workers comp, unemployment, meditax, social security tax as applicable, etc)*	$237.76
Annual Total	***$529.36***
Retirement Benefits *Mandatory Programs – PERA or 401(a)*	
Annual Total of Retirement Contributions	***$22,861.68***
Paid Leave	
Paid Sick Leave	$6,658.79
Paid Vacation Leave	$9,768.44
Paid Holidays	$4,883.11
Annual Total	***$21,310.34***

Total of Cash Compensation	$115,419.00
Total of University Paid Non-Cash Benefits	$56,235.62
Total of Compensation from University	$171,654.62

TOTAL COMPENSATION



In addition to the compensation and benefits already outlined, the University also provides access to the following benefits:

- Immediate accrual of Paid Leave
- Eligibility for Health Benefits within 30 days
- Optional Employee and Dependent Term Life Insurance and Accidental Death & Dismemberment coverage*
- Voluntary Vision coverage*
- Voluntary Short Term/Long Term Disability*
- Health Savings Account sponsorship with pre-tax contributions**
- Dependent Care and Health Care Flexible Spending Accounts with pre-tax contributions*
- Employee and Dependent Tuition Waiver Benefit
- Voluntary Retirement Savings Plans
- *Be Colorado Move* program
- Discounted RTD Eco Pass
- State of Colorado Employee Discounts
- And much more…

*Benefit must be elected in annual open enrollment process
**Employee is eligible only if enrolled in a qualifying medical plan

Every effort was made to ensure the accuracy and clarity of these statements, however you are encouraged to review your information closely and direct any questions, concerns or discrepancies to Facilities Management HR.

University of Colorado Anschutz Medical Campus

Highlights Annual Salary
Presentation of annual salary reflects wage stability, and allows for more competitive comparison to private sector offerings

Easy-to-Understand Visuals
Pie chart compares value of benefits to salary

Quantified Individual and Total Benefits
Table spells out monetary value of individual benefits, total non-cash benefits, and overall compensation

1) Figures not representative of all employees

Source: University of Colorado Anschutz Medical Campus, Aurora, CO; EAB interviews and analysis.

Getting the Numbers Right

CU Boulder Calculator Shows Applicants Personalized Benefits Value

Excerpt of Total Compensation Calculator

University of Colorado Boulder

Gross Annual Salary		$50,000.00
Gross Monthly Pay:		
Base Monthly Salary:		$4,166.67
Hourly Equivalent:		$24.04
Health Benefits:		
Contribution to Health Premium:	*Family*	$1,435.00
Contribution to Dental Premium:	*Family*	$37.00
Total Annual Employer Benefit Contributions:		$17,664.00
Retirement:		
Employer contribution to retirement annually:		10%
Annual Employer Retirement Contribution:		$5,000.00
Leave Benefits:		
Days *of Annual Leave earned per year*	22	$4,230.77
Days *of Sick Leave earned per year*	15	$2,884.62
Days *Holiday Leave:*	10	$1,923.08
Total Annual Value of Leave Benefit Amounts:		$9,038.46

Beige cells prepopulated with benefits rates and calculation formulas

Applicants enter individual-specific salary and benefits information in gray cells

Tool quantifies value of leave time, in addition to more commonly quantified health and retirement benefits

Source: University of Colorado Boulder, Boulder, CO; EAB interviews and analysis.

Bringing Higher Ed-Focused Benefits to Life

OU Script Helps Interviewers Sell Most Relevant Perks to Candidates

Common Benefits Often Needing Clarification

- Pensions
- Paid holidays
- Paid sick leave
- Employee assistance

Unique Higher Ed Benefits to Emphasize to Candidates

- Tuition remission
- Stable schedules
- Sports tickets
- Seasonal leave

The UNIVERSITY of OKLAHOMA

Recruiting Employees for FM

(Information from Naviga and OU HR)

How To Sell Your Open Positions To Top Candidates

An interview is not only about the candidate selling their abilities to the employer, but also about the employer selling the opportunity to the candidate. Too many companies focus on evaluating the candidate and don't spend enough time talking about potential growth opportunities, perks, and benefits of working for their company.

According to the data from the MRINetwork Recruiter Sentiment Study, one of the main reasons companies continue to lose out on great candidates is because of their inability to sell open roles and career advancement opportunities.

There are four strategies that will help you sell your open position and avoid losing out on top candidates.

Start with an Appealing Job Description

Many companies scare job candidates away by having too long of a job description. The best way to enhance a job description is to incorporate exciting information about the company. For example, include the company's history and forecasted growth, culture, solutions offered, etc. Make sure to add key selling points about your company that will entice candidates to continue reading and apply for the opportunity.

OU's Facilities Benefits Sell Document

- Five-page document provides scripting points and guidance for interviewers explaining benefits to candidates
- Resource addresses commonly misunderstood or underappreciated benefits, including value of retirement benefits, tuition discount, and process to obtain discounted sporting tickets

Source: University of Oklahoma, Norman, OK; EAB interviews and analysis.

A Renewed Focus on a Long-Standing Solution

Apprenticeship Programs Have Proven ROI, Multiple Workforce Benefits

Recent Bipartisan Support for Expanding Apprenticeships Across Industries…

INSIDE HIGHER ED

Trump Administration Proposes New Apprenticeship Structure

Biden Administration to Take Steps to Bolster Registered Apprenticeships

US Department of Labor Awards More Than $130M in Grants to Support Registered Apprenticeship Programs

…Reflects High Program Returns for Participants and Employers

1.5x

Return on Investment

- Enhanced recruitment
- Reduced turnover and increased productivity relative to non-apprentice candidates
- Augmented candidate soft skills
- Improved workforce engagement

Source: "Fact Sheet: Biden Administration to Take Steps to Bolster Registered Apprenticeships," *The White House;* "Trump Administration Proposes New Apprenticeship Structure," *Inside Higher Ed;* "US Department of Labor Awards More Than $130M in Grants to Support Registered Apprenticeship Programs; Increase Employment Opportunities," *U.S. Department of Labor.* Facilities Forum interviews and analysis.

More than Just Help Desk Support

Setting Student Staff Up for Success

Cybersecurity Student Apprenticeship Program at Illinois State University

Illinois State University

Oversight

- **1 FTE Supervisor** with security expertise oversees 12 apprentices to:
  - Design and curate trainings
  - Oversee work conduct
- A dedicated FTE also supports **knowledge management and continuity** as students cycle in and out

Training

- **Module-based trainings** cover institutional security context, relevant tools, and specializations
- **Trainings delivered in tiers**, so students gain new responsibilities as they complete trainings
- Training **assessments in test environments** allows students to demonstrate readiness before system access

Responsibilities

- **Job titles aligned with private sector roles** create a pipeline to full-time employment with ISU
- With more advanced trainings, **students can conduct vulnerability assessments**, mange corrective work and incident response, and resolve compromised credentials or locked accounts

Related Resources

- Extending the Student IT Workforce
- Cybersecurity Apprenticeship Program (pg. 10)

Source: Illinois State University, Normal, IL; EAB interviews and analysis.

Expanding NICE-ly: Rice Trains Apprentices

Rice University Designs an Apprentice Program for Cybersecurity

Partner with HR to Build Program

RICE

HR Consultation Emphasizes Fairness, Commitment

CISO worked with HR to design a program that is fair, measurable, and potentially scalable to the entire university

NIST NICE Framework

Formal training and roles framework contributed to program design and is an advantage for cybersecurity over other potential fields for apprenticeship

Select Core Training Program

Training Portfolio

Training includes **Cybrary, SANS, Splunk,** and **Tenable** courses in both self-study and group formats

Learning While Doing

Roughly 20% time formal training and 80% on-the-job learning under security staff

Tier One Cybersecurity Apprentice

Tier One Employee

Regardless of previous position, the apprentice is classified and paid as tier one staff

Six Month Training Window

Following successful completion of training, candidate becomes an FTE in the cybersecurity group

CIO Backfills Candidate Position for Three Months

CIO is responsible for finding a replacement at the three month mark

Source: EAB interviews and analysis.

Recruit with Care

Realistic Messaging Reduces Pool but Raises Confidence in Candidates

Full time IT staff in good standing → *7 interested* → *4 applicants* → *1 apprentice*

Communication

- About 120 eligible employees
- Info sessions attract 30 staff

Consideration

- Pre-apply conversations show salary top concern

Application

- "Serious, legit candidates"
- All entry level

Hiring

- Same interview protocol as external posting
- Focus on aptitude rather than experience

Lessons Learned

- Messaging emphasizes entry-level nature of position, commitments to be required
- Cachet of cybersecurity not enough to overcome pay decrease
- Applicants mostly came from desktop support; little interest from "declining" roles (e.g., sys admin, DBA)
- Based on outcomes, may repeat and extend eligibility to rest of university

Source: EAB interviews and analysis.

Mitigating Risk with Mutual Commitments

With 3.5 Million Unfilled Cybersecurity Jobs in 2021…

How do higher education IT units retain homegrown talent?

"We realize there is turnover risk, but we're willing to accept that."

Marc Scarborough
CISO, Rice University

As Training at Rice Progresses, So Does Obligation

Day One

New Position Starts

- Seat moved to CISO reporting line
- Salary adjusted to apprentice level
- Core training begins

Three Months

No-Fault Period Ends

- Last chance for no-fault drop out
- If apprentice continues, old position no longer held open
- >50% of trainings should be completed

Six Months

Official, but Committed

- Becomes an FTE with appropriate compensation
- Committed to two-year tenure
- Early departure requires repayment of $4,000 training costs

Source: EAB interviews and analysis.

Distributing Security Responsibilities

Enlisting Supplemental Security Support Reduces Burden on Core Team

Cross-Train Central IT Staff

SHAW UNIVERSITY 1865

- All IT staff received both product-based and agnostic security training and discrete security tasks.
- For example, help desk staff members now triage security requests and supplement endpoint security tasks, such as patching devices, while a system admin conducts log analysis.

Security Trainings for IT Staff

General Topics

- SANS Institute trainings, such as SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling
- GIAC Global Industrial Cyber Security Professional (GICSP)
- GIAC Security Essentials (GSEC)

Product Trainings

- Splunk Training & Certification
- Cisco Certified Network Associate (CCNA) Vendor Certification
- AWS Security Essentials

Recruit Distributed IT Security Volunteers

- Form a Cybersecurity Services Working Group, comprised of volunteers from distributed IT staff and enthusiastic faculty and staff.
- The group can report to a security analyst who coordinates their work on 'low hanging fruit' tasks, such as a NIST gap analysis.

> "Security is often a tight-lipped team, by necessity. But our current talent shortage means we must find ways to engage students and volunteers with low-level tasks that can take the burden off more specialized staff, without compromising our security.

Sources: Shaw University, Raleigh, NC; EAB interviews and analysis.

Considering Scaled Services

Range of Options for Collaboration and Cost Containment

Spectrum of Organizational Options for Achieving Scale

Less Scale → *Greater Scale*

Shared Service Hubs
One or more shared service centers fulfill transactional work, focusing on serving one segment of customers

Campus-Wide Shared Service Center
A single shared service center fulfills all transactional work, maintaining customer focus

Centralization
Transactional work absorbed into the existing central administrative function

System Shared Services
Institutions within a university system create a shared service center to serve multiple campuses

Consortia
Multiple institutions, usually close in proximity and mission, partner together for select services

Outsourcing
Institutions contract an external party to provide services

Two Trends in Consolidation to Consider

1. Regional institutions considering shared service centers on campus or across systems
2. Institutions across segments looking for opportunities to partner with other institutions to share administrative processing

Source: EAB interviews and analysis.

Shared Security Operations Centers

OmniSOC is Higher Ed's First Shared Multi-State Institution SOC

What is the Omni Security Operations Center (OmniSOC)?

A **shared multi-state institution cybersecurity operations center for higher education** and research. OmniSOC was founded by five Big Ten Academic Alliance schools and is located at Indiana University, where it currently serves 12 member institutions.

OmniSOC

Key Features of OmniSOC

- 24 x 7 x 365 Critical, Actionable, High-Quality Alerts
- Processing and Creating Cyber Threat Intelligence
- Proactive Threat Hunting and Analyzing Security Events
- Supplemental Workforce and Consulting Support Upon Request
- Multi-State Institution Data Sharing Agreement for Researchers

>14.2B **Average number of security events per day** across all members

Benefits of Shared SOCs

Higher Ed-Specific

Shared SOCs designed for higher ed understand the environment better (e.g., how to navigate federated departments, the implications of an incident the week before graduation)

Staff Time and Training

Shared SOCs allow member cybersecurity staff to focus on what is most important. OmniSOC also offers shadowing and intern opportunities for member staff

Economies of Scale

Not only do shared SOC subscription fees pale in comparison to setting up an internal SOC, but members benefit from collective threat intelligence of all members

Source: Indiana University, Bloomington, IN; EAB interviews and analysis.

Applying Our Discussion to On-Campus Strategy

Choose the Top Three Tactics You're Likely to Adopt in the Next Two Years

Please place a **Star stamp** next to the three tactics you choose. To access the stamp, select View Options at the top of your Zoom screen, then click **Annotate > Stamp**

I. Case Studies of Leading Edge Technologies in Higher Ed

Tactic 1: User-Focused Security Enhancement Tools

- Password Managers
- Mobile ID and Wallet
- User Driven Sensitive Data Removal
- Unit Security Dashboard

Tactic 2: Proactive and Automated Security Management Tools for IT and InfoSec

- Cybersecurity Asset Management
- Extended Detection and Response Tools
- Risk-Based Microsegmentation

II. Practical Staffing Solutions to Address Talent Shortage

Tactic 3: Benefits Value Sell Document

Tactic 4: Apprenticeship Programs

Tactic 5: Distributed IT Responsibilities

Tactic 6: Shared SOC Among Universities

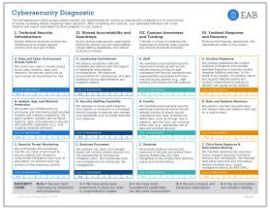
How EAB Can Help

Start by Conducting a Current State Assessment

1

Cybersecurity Diagnostic evaluates strengths and opportunities in an institution's cybersecurity posture and organization

- Contact your Strategic Leader to get access to the diagnostic or schedule a call with us to walk through the exercise



Communicate Security Imperatives to Boards and Cabinets

2

Cybersecurity Executive Briefing Deck helps leaders prepare for their next Board or Cabinet meeting

- Schedule a call with EAB experts to walk through the deck and/or schedule time for us to present to your board or cabinet

Practice Decision-Making with Tabletop Exercises

3

Security Incident Response Tabletop Exercises prepare leaders to navigate security incident crises

- Resource Center includes scenarios, exercise guidance, after-action report, etc.
- Use it to facilitate a session on your campus or ask our EAB experts to facilitate for you

Contact Us

Linnea Hengst
Strategic Leader
Research

LHengst@eab.com

Afia Tasneem
Director
Research

ATasneem@eab.com

Ron Yanosky
Director,
Research

RYanosky@eab.com

Connect with EAB @EAB @EAB @eab_