

# Information Security in Higher Education

Joanna Grama, JD

October 20, 2015  
OARnet CIO Meeting

# Agenda

- Information Security in Context
- REN-ISAC
- EDUCAUSE Cybersecurity Initiative
- EDUCAUSE Annual Conference



# Speaker Bio

## Joanna Grama

- Director of Cybersecurity and IT GRC Programs at EDUCAUSE
- Lawyer by training
- Credential hoarder by choice (CISSP, CIPT, CRISC)
- Admitted work-a-holic who becomes bored easily
- Social media addict (*@runforserenity*)
- (Reformed?) helicopter parent



# Information Security in Context

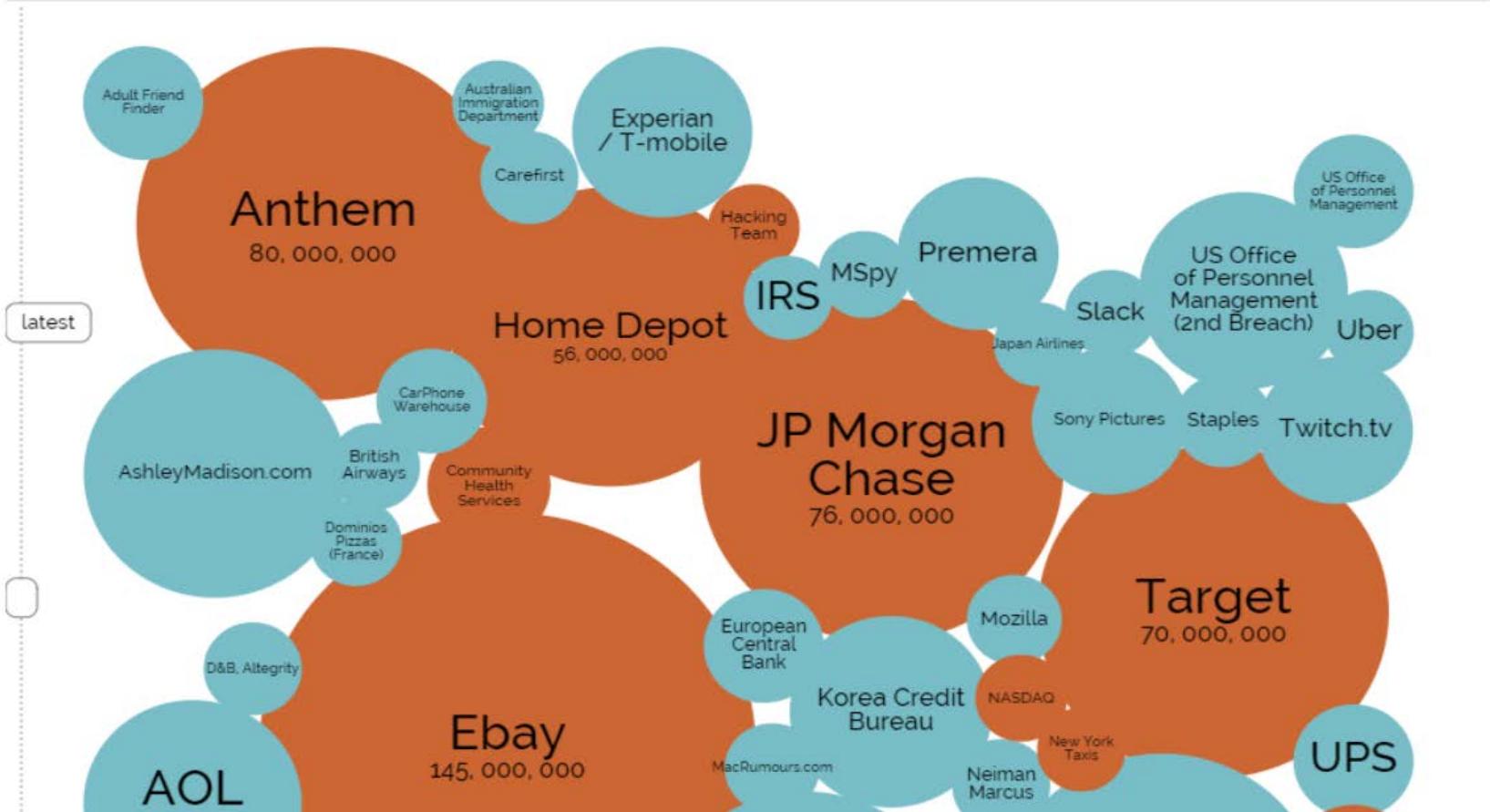
# It's Scary "Out There"

## World's Biggest Data Breaches

Selected losses greater than 30,000 records  
(updated 2nd October 2015)

 interesting story

YEAR      BUBBLE COLOUR      YEAR      METHOD OF LEAK      BUBBLE SIZE      NO OF RECORDS STOLEN      DATA SENSITIVITY       SHOW FILTER



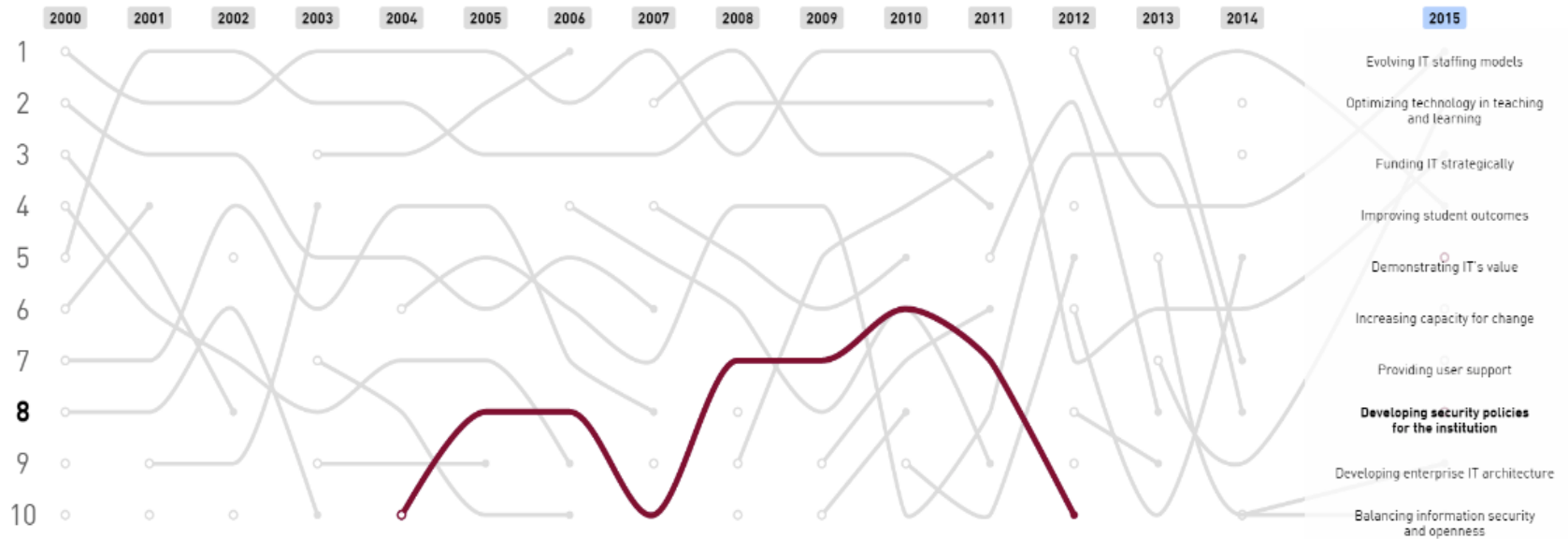
# Information Security is a Top 10 IT Issue

*Not Just Once in 2015...*

## TOP 10 IT ISSUES: 2000-2015

EDUCAUSE

This graphic tracks the rankings of the top 10 IT issues since 2000. Clicking or tapping a year along the top will show the top 10 IT issues for that year. Hovering over or tapping an issue will highlight the trend in importance for that issue across years.



Source: 2015 IT Issues Report

EDUCAUSE

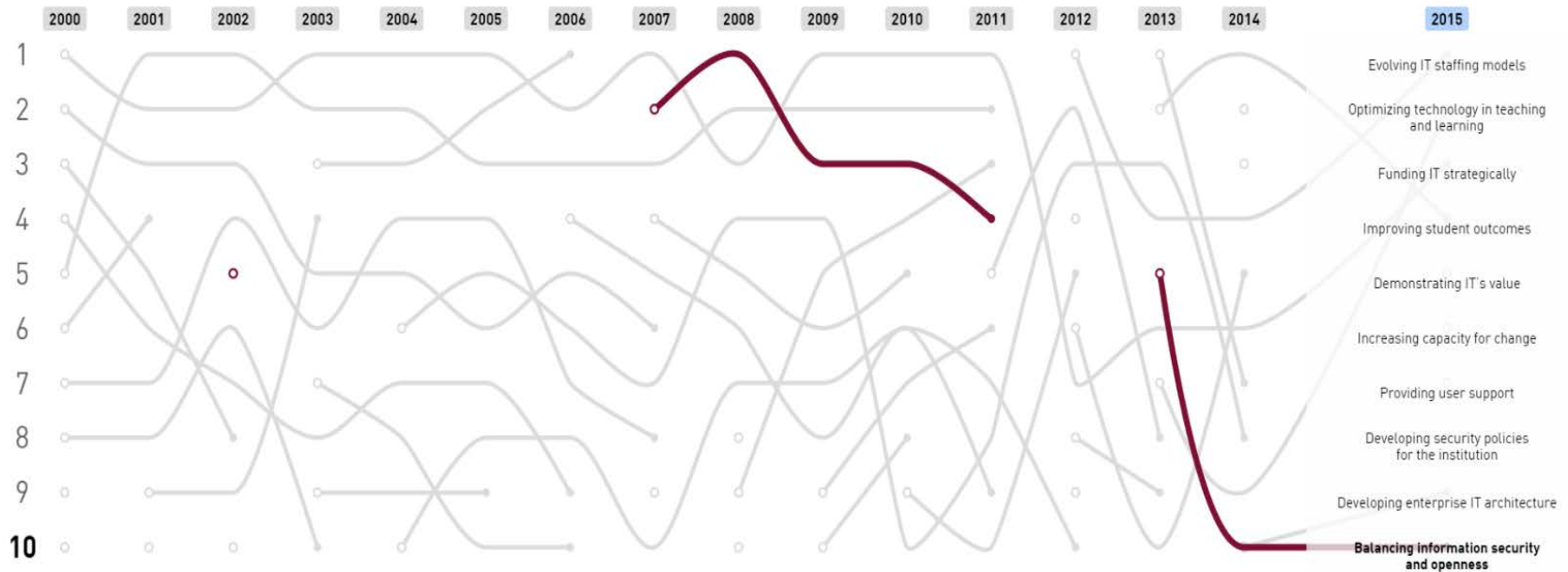
# Information Security is a Top 10 IT Issue

*But Twice.*

## TOP 10 IT ISSUES: 2000–2015

EDUCAUSE

This graphic tracks the rankings of the top 10 IT issues since 2000. Clicking or tapping a year along the top will show the top 10 IT issues for that year. Hovering over or tapping an issue will highlight the trend in importance for that issue across years.



[Source: 2015 IT Issues Report](#)

EDUCAUSE

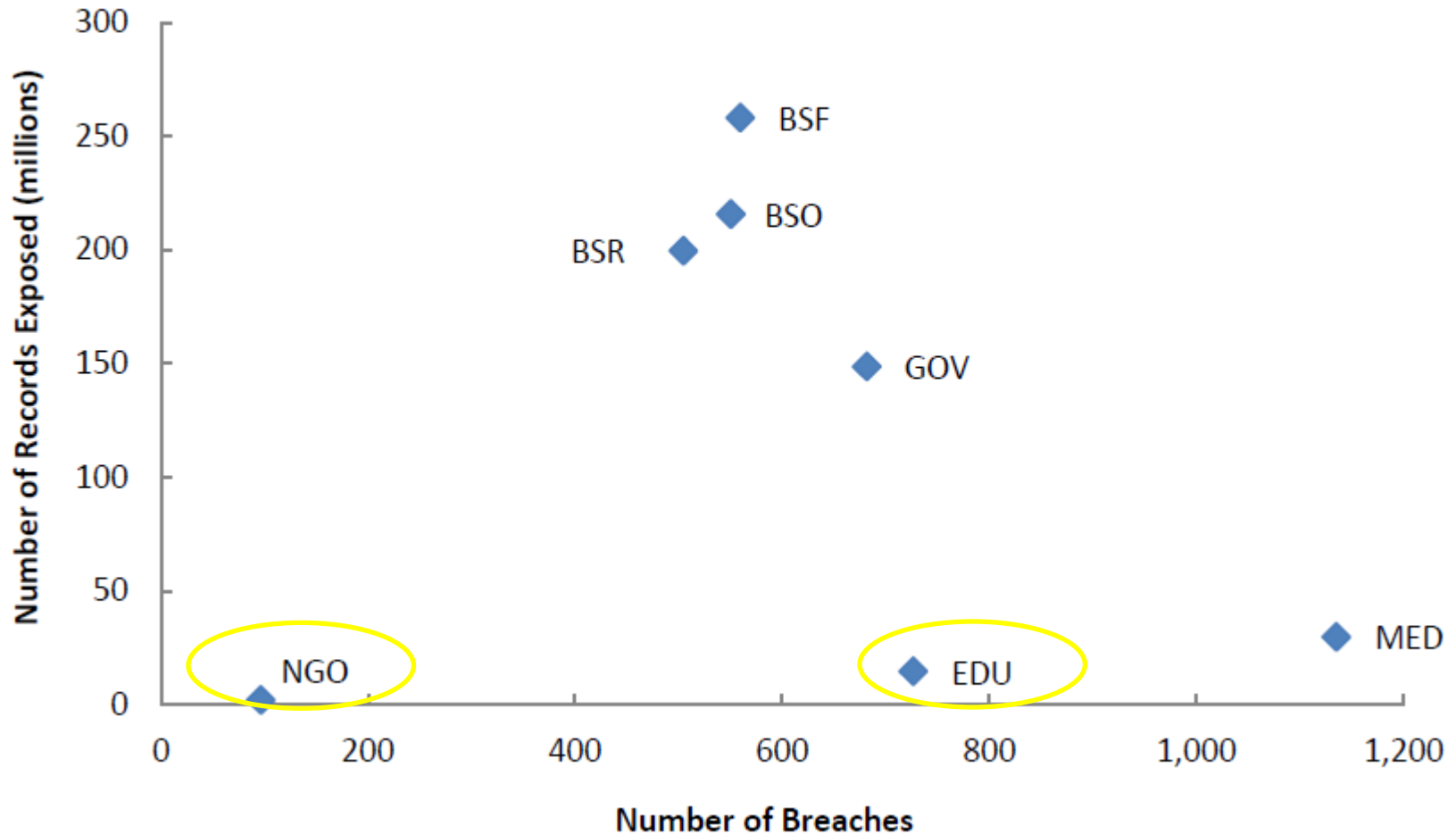
# Data Is The Target



- User credentials/passwords
- Personally identifiable information
  - Financial information
  - Health information
- Proprietary information/trade secrets
- Research data
- Information about how networks and IT resources work
- Confidential information that, if released, could cause personal embarrassment



# Data Breaches by Industry



Source: ECAR, *Just in Time Research: Data Breaches in Higher Education*, May 2014.

# Data Breaches in Higher Education

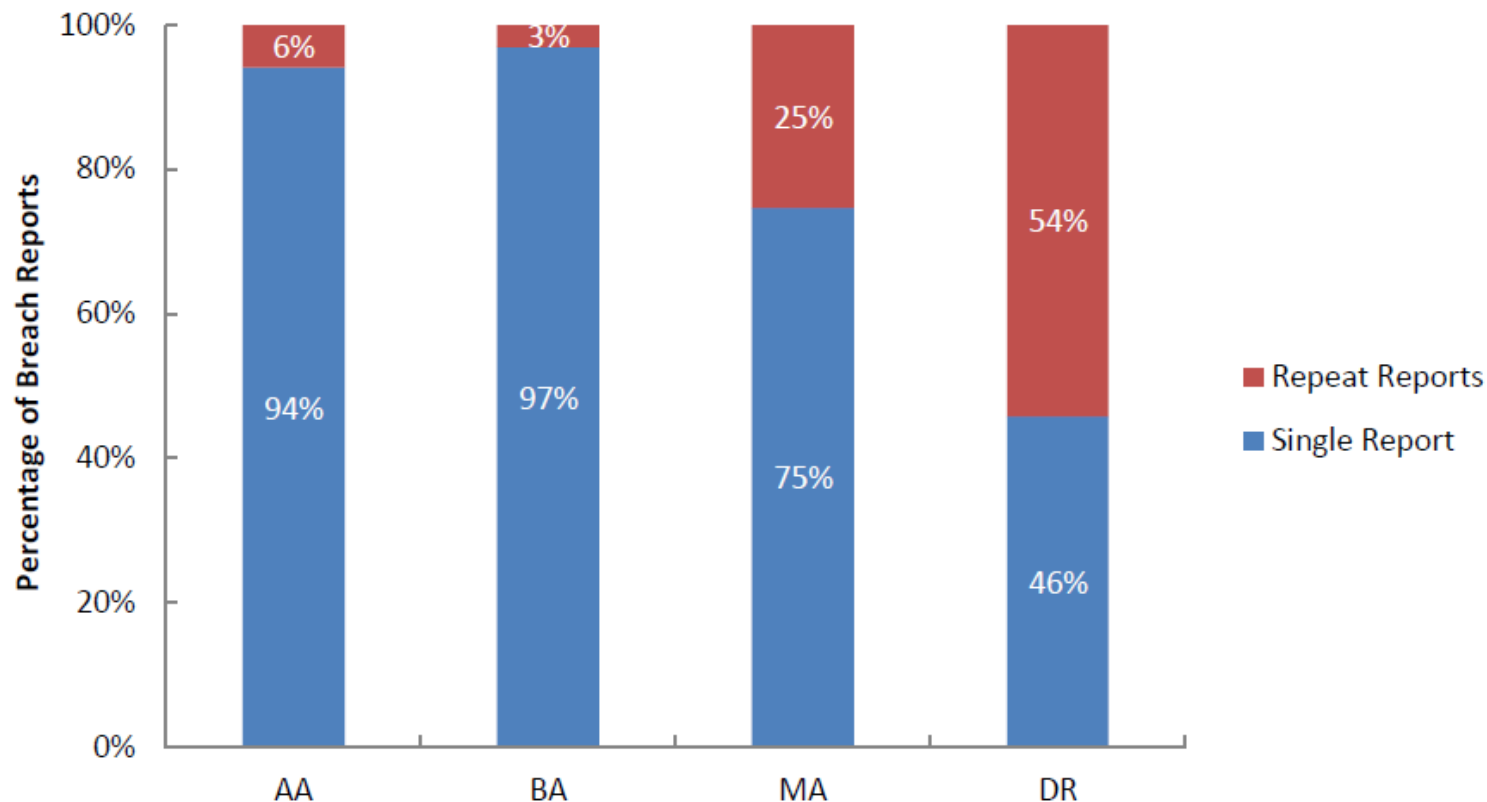


Figure 5. Proportion of single/repeat breach reports by Carnegie Classification in the PRC, 2005–2014 (ECAR data set, n = 324)

Source: ECAR, *Just in Time Research: Data Breaches in Higher Education*, May 2014.

# Data Breaches in Higher Education

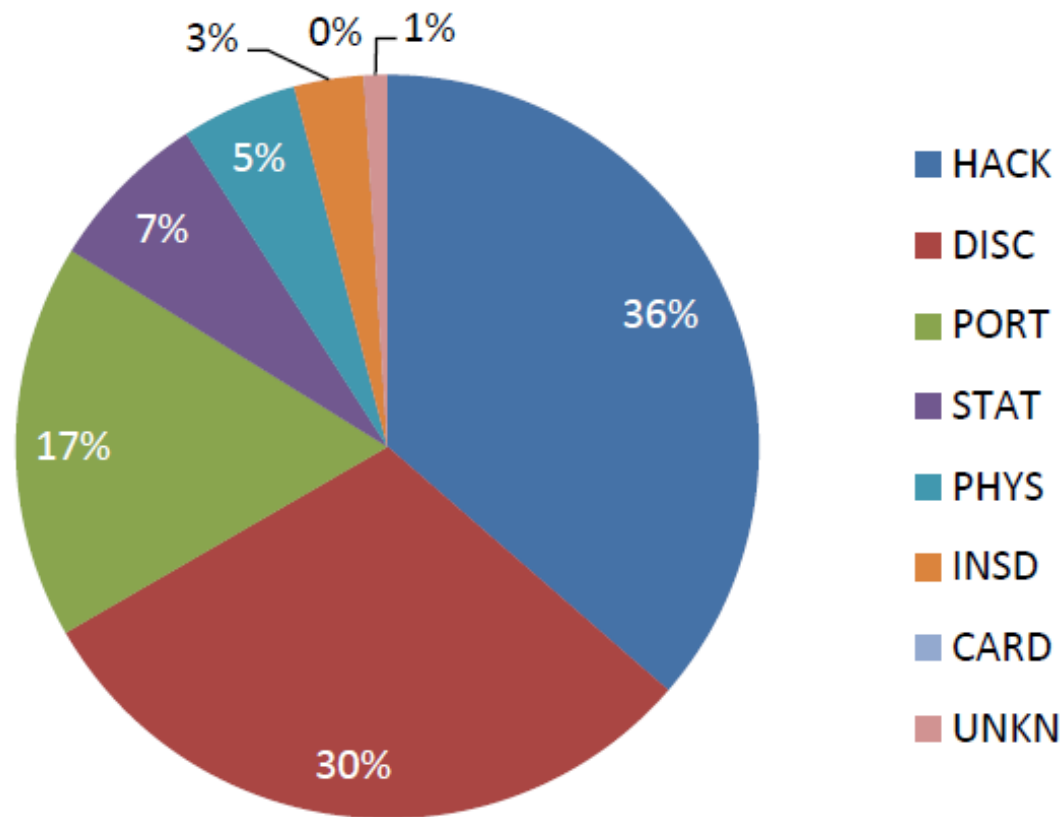
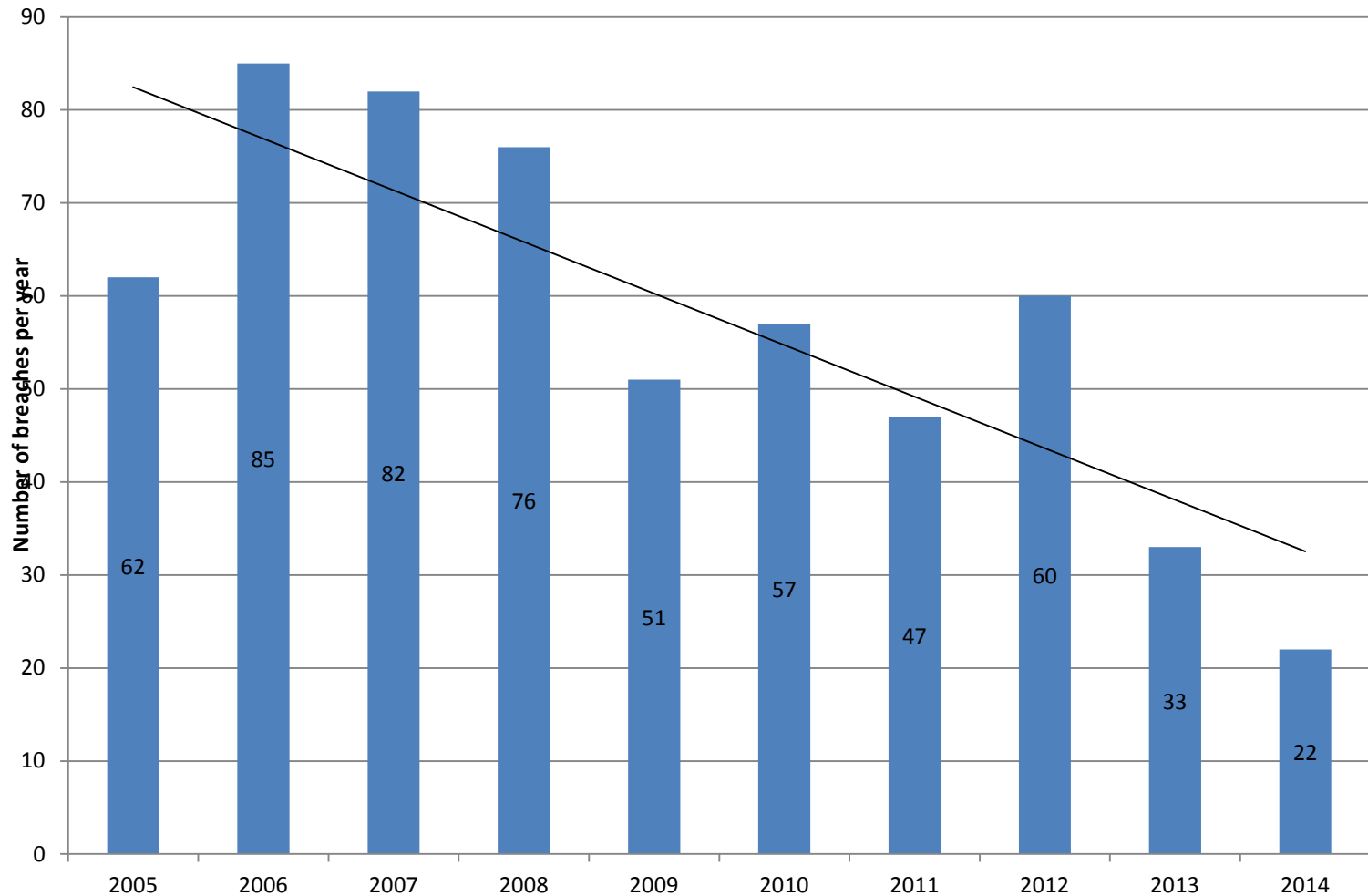


Figure 6. Types of data breaches in higher education, 2005–2013 (ECAR data set, n = 551)

Source: ECAR, *Just in Time Research: Data Breaches in Higher Education*, May 2014.

# Data Breaches in Higher Education



Source: EDUCAUSE Review, *This Magic Moment: Reflections on Cybersecurity*, September, 2015.

# Introduction to REN-ISAC



REN-ISAC  
Research and Education Networking Information  
Sharing and Analysis Center

<http://www.ren-isac.net/membership.html>

Kim Milford, Executive Director



## Mission

The REN-ISAC mission is to aid and promote cyber security operational protection and response within the higher education and research (R&E) communities.

The mission is conducted within the context of a private community of trusted representatives at member institutions, and in service to the R&E community at-large.

REN-ISAC serves as the R&E trusted partner for served networks, the formal ISAC community, and in other commercial, governmental, and private security information sharing relationships.

# REN-ISAC

---

## Ohio Higher Education Members

- OARnet
- Ashland University
- Case Western Reserve University
- Denison University
- Eastern Gateway Community College
- John Carroll University
- Kent State University
- Kenyon College
- Marshall University
- Miami University
- Oberlin College
- The Ohio State University
- Ohio University
- Owens Community College
- Sinclair Community College
- University of Akron
- University of Cincinnati
- Wittenberg University
- Xavier University
- Youngstown State University



## REN-ISAC Components

- Private Trust community
- CSIRT for .edu
- Sector ISAC
- R&D

# REN-ISAC

---


## Private Trust Community

- Membership is open to:
  - Colleges and universities
  - Teaching hospitals
  - R&E network providers
  - Government-funded research organizations
- Member representative eligibility:
  - Very specific job responsibility requirements: institution-wide operational protection and response (essentially the IT Security Office (or alike) security engineers, architects, and direct managers)
  - Tightly circumscribed to maintain a high level of trust and interaction among the representatives
- 2 tiers, differing in eligibility criteria, trust vetting, sensitivity classification, and the commitment-level of the institution

# REN-ISAC

---

## Private Trust Community

- Member participation is a cornerstone of REN-ISAC
  - Member contributions through participation:
    - Board
    - Technical Advisory Group
    - Microsoft Analysis Team
    - Membership Committee
    - Member Orientation and Engagement Committee
    - Technical webinars
    - Services development
    - Projects, e.g. sensor development
    - Special Interest Groups, e.g. SIEM, Forensics, Bro, etc.
- 

# REN-ISAC

---

## Private Trust Community

- Information products (e.g. Daily Watch, Advisories, and Alerts)
- Benefit from REN-ISAC relationships in broad security community
- Benefit from REN-ISAC / vendor security cooperation relationships
- Participate in technical educational security webinars
- Participate in REN-ISAC meetings, workshops and training
- Access to the 24x7 REN-ISAC Watch Desk
- Develop relationships with known and trusted peers

# REN-ISAC

---

## CSIRT for .edu

- Daily notifications, directly and privately to abuse contacts at .edu institutions concerning compromised or vulnerable systems, credentials, and other incident involvement
  - In service to all of US .EDU regardless of membership, and international members
  - Over 12,000 notifications per month
  - Over 1,800 institutions notified
- 24x7 Watch Desk
- Represent the sector in forums of private, commercial, and governmental CERT/CSIRTS

# REN-ISAC

---

## EDU Sector ISAC

- Trusted partner for the R&E community
- Member, National Council of ISACs
- Formal relationship with DHS/US-CERT
- Cross-sector information sharing
- Public alerts aimed at R&E security practitioners, CIOs and business officers

# REN-ISAC

## R&D

- CSIRT Tools
  - RINO (Ren-Isac NOtification system)
    - Receives, collates, and distributes notifications concerning observed compromised or vulnerable systems
  - RIHF (Ren-Isac Human Filter)
    - Process notifications based on data that requires operator vetting and interaction.
- RINO and RIHF aren't currently released open-source but we're hoping to get there.

# REN-ISAC

## Relationships

- APWG (Anti-Phishing Working Group)
- DHS/US-CERT and other national CERTS and CSIRTS
- EDUCAUSE
- Global Research NOC at IU
- Higher Education Information Security Council
- Internet2
- LE (various)
- National Council of ISACs
- NCFTA



# REN-ISAC

---

## Organization

- Hosted by Indiana University (fiscal and administrative agent)
- Eight full-time staff
- Governed by a Board formed from among the members (2/3) plus sponsoring and host organizations
- Relationship with the Higher Education Information Security Council (HEISC, similar in concept to a Sector Coordinating Council (SCC))

# REN-ISAC

## Fees

- FY2016 (July 2015 - June 2016) are unchanged from the rates established for FY2015
- Fees are calculated according to a modified Carnegie Classification (CC) model, based on the CC Basic2010 of U.S. colleges and universities. The 30+ CC classes are mapped to 4 REN-ISAC classes:

Very High Research	\$2,500
High Research	\$2,250
Large Master's and Doctoral/Research	\$1,500
All Other	\$1,250

# Introduction to the EDUCAUSE Cybersecurity Initiative

# EDUCAUSE Cybersecurity Initiative

- Lead by the Higher Education Information Security Council (HEISC); an EDUCAUSE and Internet2 partnership
- Working Groups
- Yearly Security Professionals Conference
- The *Information Security Guide* (practitioner resource)
- Mentoring Program
- Security Discussion List

*The Higher Education Information Security Council (HEISC) supports higher education institutions as they improve information security governance, compliance, data protection, and privacy programs. Learn about HEISC and its programs at*

[www.educause.edu/security](http://www.educause.edu/security)

# Working Groups

- Awareness and Training
- Governance, Risk, and Compliance
- Technologies, Operations and Practices
- Information Security Guide Editorial Board
- Security Conference Program Committee
- Higher Education Chief Privacy Officers

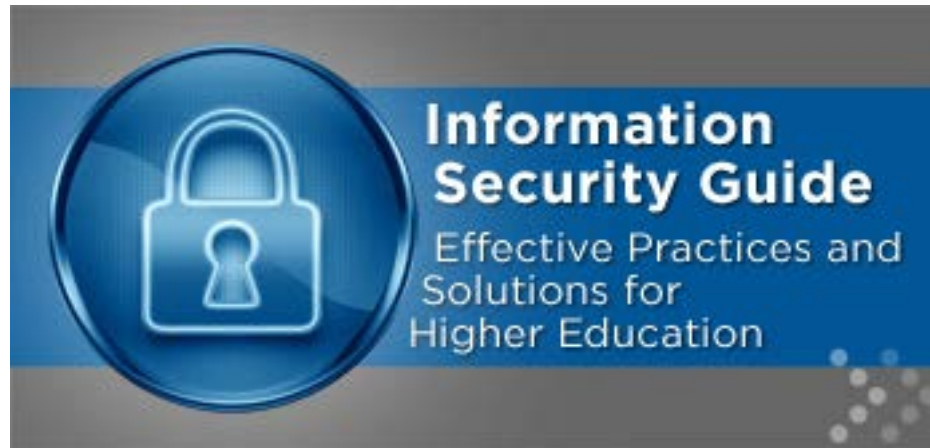
# Security Professionals Conference

- Established 2000
- Only conference for higher education information security practitioners
- April 18-20, 2016 in Seattle, WA
- *CFP open now!* Submit by 11/9/2015



# Information Security Guide




- Effective practices and solutions
- Created **by** higher ed security professionals **for** higher ed security professionals
- Based on ISO 27002



View the *Information Security Guide* at: <http://www.educause.edu/security/guide>

# InfoSec Program Assessment Tool

- Self-assessment tool
- Based on ISO 27002
- 104 questions
- Appropriate for institutional or unit use

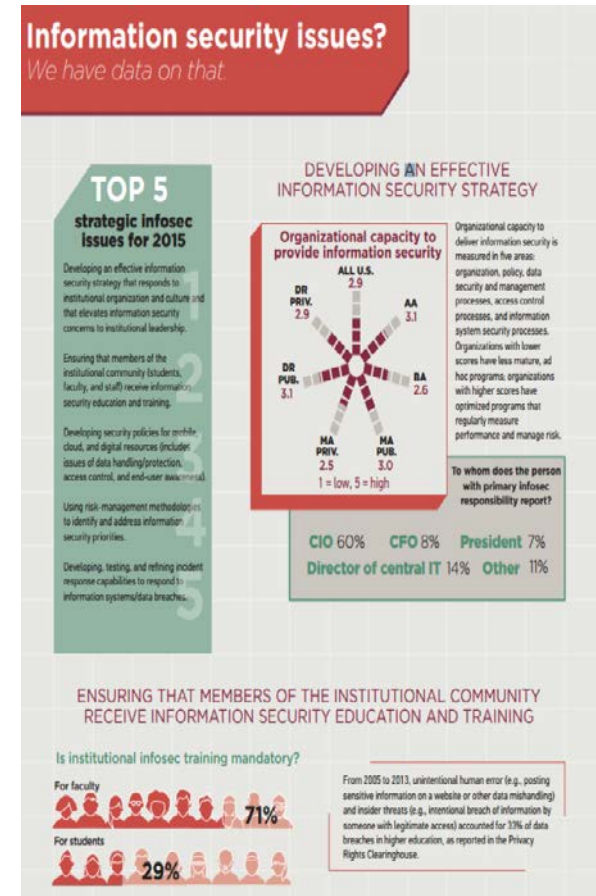
Security Policy (ISO 5)	Total Score for ISO 5->	0.00		
Does your institution have an information security policy that has been approved by management?	Not Performed	0		
Has it been published and communicated to all relevant parties?	Not Performed	0		
Does your institution review the policy at defined intervals to encompass significant change and monitor for compliance?	Not Performed	0		

View tool at: <http://www.educause.edu/library/resources/information-security-program-assessment-tool>



# InfoSec Research from EDUCAUSE

- Core Data Service
  - Core Data Reporting (M7)
  - Almanacs
  - CDS Spotlights
- ECAR
  - Infused throughout research
  - Infographics
- EDUCAUSE
  - Leader materials



## *Next Week!* Security & Privacy at the EDUCAUSE Annual Conference

- DHS Deputy Assistant Secretary Gregory Touhill speak about the Importance of a Cybersecurity Education.
- Briefing: Cyber threats facing colleges and universities today.

Learn more:

<http://www.educause.edu/blogs/vvogel/security-privacy-and-risk-sessions-educause-2015>

# Resource List

# Resource List

- Resources for Presidents and Senior Executives: Information Security (EDUCAUSE):  
<https://www.educause.edu/library/resources/resources-presidents-and-senior-executives>
- 2015 Top Information Security Strategic Issues (EDUCAUSE):  
<http://www.educause.edu/library/resources/2015-strategic-information-security-issues-infographic>
- REN-ISAC Public Alerts and Advisories: <http://www.ren-isac.net/alerts.html>
- Grama & Milford, *This Magic Moment: Reflections on Cybersecurity*: <http://er.educause.edu/articles/2015/9/this-magic-moment-reflections-on-cybersecurity>

# Questions?

Please ask questions so that I don't have to tell jokes or show embarrassing family pictures for these last few minutes.

Joanna Grama

[jgrama@educause.edu](mailto:jgrama@educause.edu)

[@runforserenity](https://www.instagram.com/runforserenity)

