ECAR

Just in Time Research:
Data Breaches in Higher Education

This "Just in Time" research is in response to recent discussions on the EDUCAUSE Higher Education Information Security Council (HEISC) discussion list about data breaches in higher education. Using data from the Privacy Rights Clearinghouse, this research analyzes data breaches attributed to higher education. The results from this review will be used to inform EDUCAUSE research, programs, products, and services.

Hardly a day goes by without a media report about a data breach that exposes the personally identifiable information (PII) of individuals. While much of the news regarding data breaches focuses on the harm to affected individuals, data breaches also harm the organization experiencing the breach. Potential direct financial costs of a data breach include legal representation, fines (depending on the nature of the breach), and the expense of notifying affected individuals. Organizations also face losses in reputation and consumer confidence. Particularly important for higher education institutions are reputational consequences, which could result in a loss of alumni donations and even a reduction in the number of students choosing to apply to or attend the institution.

Since 2005, the Privacy Rights Clearinghouse (PRC) has worked to document how technology affects individual privacy and to educate consumers on how to protect their privacy.[1] The PRC also collects information on verifiable data breaches in the United States and the number of records containing PII exposed in those breaches.[2] As of April 25, 2014, the PRC Chronology of Data Breaches had documented 4,257 data breaches in the United States involving at least 867,217,832 records from all industry sectors, including but not limited to education.

The PRC database includes 727 breaches involving educational institutions that were made public in 2005–2014, involving more than 14 million breached records. The number of breaches includes breaches attributed to higher education institutions as well as trade schools, K–12 schools and school districts, and education-related nonprofit organizations.

Industry Sectors in PRC Data

BSF:	Businesses (Financial and Insurance Services)
BSR:	Businesses (Retail/Merchant)
BSO:	Businesses (Other)
EDU:	Educational Institutions (All)
GOV:	Government and Military
MED:	Healthcare
NGO:	Nonprofit Organizations

The PRC notes that the number of records exposed in the reported data breaches may actually be larger than the numbers they capture in their database. This is because the number of records exposed in many data breaches cannot be known.[3] Upon review of the PRC dataset, 73% of breaches attributed to the education sector included data about the number of

[1] See Privacy Rights Clearinghouse, https://www.privacyrights.org/.

[2] For more information on how the Privacy Rights Clearinghouse Chronology of Data Breaches is maintained, visit https://www.privacyrights.org/data-breach-FAQ.

[3] The PRC also notes that the number of records exposed does not equal the number of individuals affected by any reported breach. Some individuals may have multiple records exposed in any given breach.

records exposed per breach. While that leaves over a quarter of education's breaches with an unknown number of records, that is lower than for any other sector in the PRC data (see table 1). Due to this missing information, the total number of records affected by all breaches in the PRC database is likely two to three times larger than the currently reported total. This report focuses predominantly on the number of breach incidents reported, rather than the number of records exposed in those breaches, due to the large number of breaches with unknown records.

Table 1. Reported Breaches by Sector and Number of Records Exposed, 2005–2014 (PRC data set)

Industry Sector	Percentage of Reported Breaches with Known Records	Number of Reported Breaches	Average Number of Records Exposed per Breach
EDU	73%	727	27,509
GOV	63%	682	349,070
BSF	51%	560	1,420,533
NGO	45%	97	44,789
MED	43%	1,136	67,280
BSO	38%	551	1,041,668
BSR	38%	505	1,087,949

Education Has a Larger Number of Reported Breaches but Fewer Records Exposed

The number of breaches in an industry sector is not well correlated with the number of records exposed (see figure 1). Simply because a large number of breach reports stem from a particular sector does not mean that a commensurately larger number of records from that sector are exposed. Based on PRC data, education (K–20) as an industry has the second largest number of reported breaches (727) but the second *lowest* number of records exposed (14,524,954, or just over 1% of the total records reported). For breaches where the number of records is known, education has the lowest average number of records exposed per breach (27,509; see table 1).

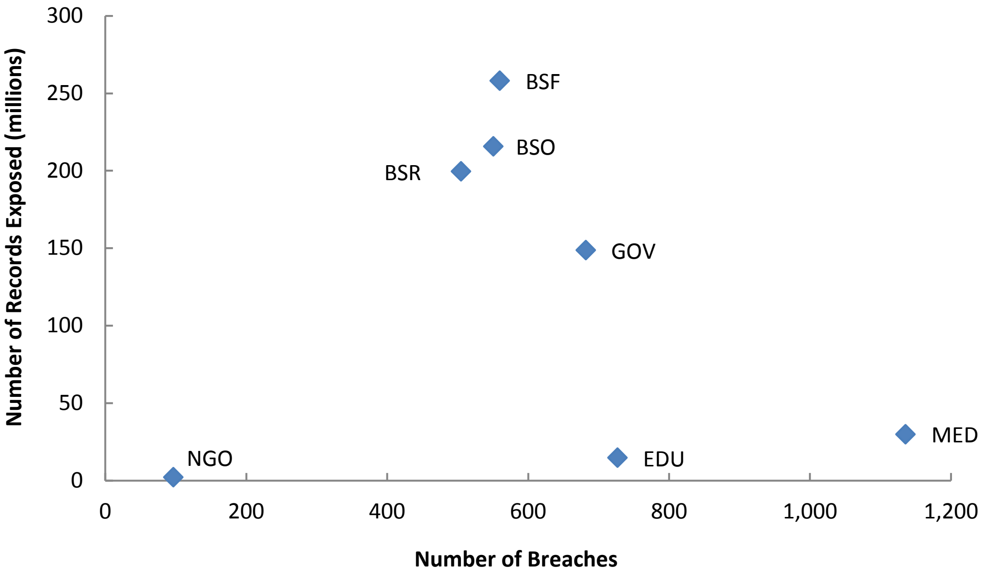

Figure 1. Number of records exposed vs. number of breaches reported, 2005–2014 (PRC data set)

The EDUCAUSE Center for Analysis and Research (ECAR) sorted the reported EDU breaches into a data set that consisted of higher education institutions only, resulting in a data set of 562 reported breaches at 324 unique institutions between 2005 and April 25, 2014. The data presented in this report are derived from the ECAR data set unless otherwise noted.

The Number of Reported Breaches Varies By Carnegie Class

Seventy-seven percent of the breaches attributed to educational institutions in the PRC Chronology of Data Breaches occurred at colleges and universities. From 2005 to 2013, there were 551 breach reports made by colleges and universities—a rate of just over one per week. While the data hint at a downward trend in the number of breaches reported over time, it is too early to tell whether this is a significant trend (figure 2).

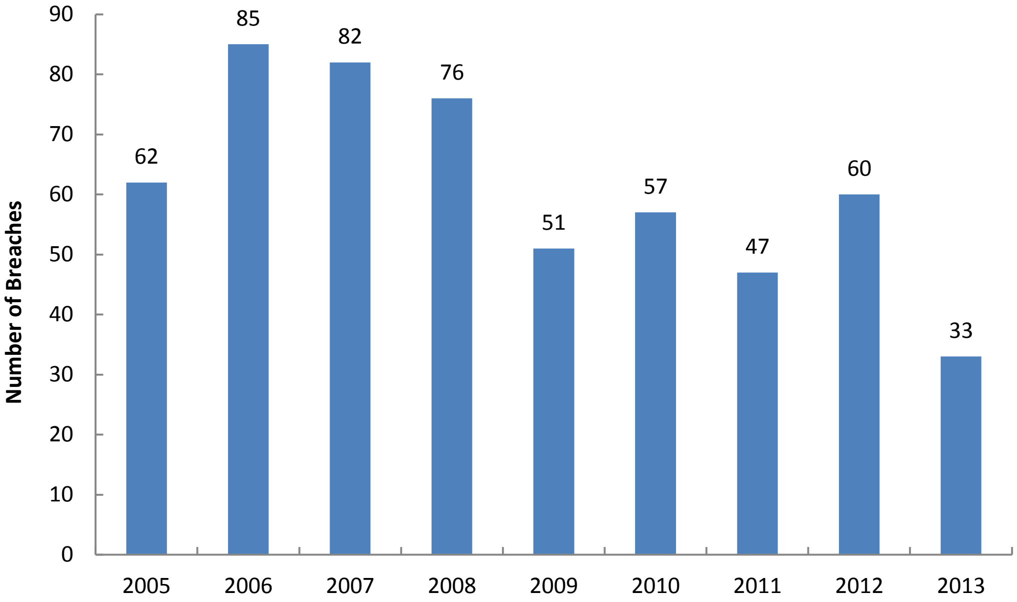

Figure 2. Number of higher education reported breaches per year, 2005–2013 (ECAR data set, n = 551)

Doctoral (DR) institutions are responsible for the majority of reported breaches, which is likely a function of scale (e.g., larger campuses, distributed environments, more complicated information systems, more records to manage, etc.; figure 3). Sixty-three percent of the PRC reported breaches are attributed to DR institutions, though they make up only 7% of all U.S. institutions. Twenty-one percent of the reported breaches are attributed to master's (MA) institutions, which make up 16% of all U.S. institutions. While they comprise the majority of U.S. higher education institutions, associate's (AA) and bachelor's (BA) institutions had fewer reported data breaches.

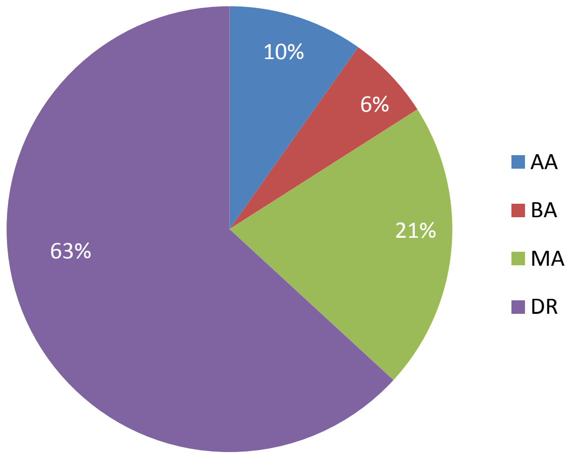

Figure 3. Breaches by Carnegie Classification, 2005–2013 (ECAR data set, n = 551)

One-Third of Institutions with Breaches Reported in the PRC Have More than One

Roughly 7% of all U.S. institutions have had a least one breach. From 2005 to 2014, most institutions (66%) listed in the PRC experienced only one reported breach. However, one-third of institutions with breaches have had more than one. Nineteen institutions (6%) have experienced five or more reported breaches. Using these numbers, just over 2% of all U.S. higher education institutions have experienced more than one breach (figure 4).

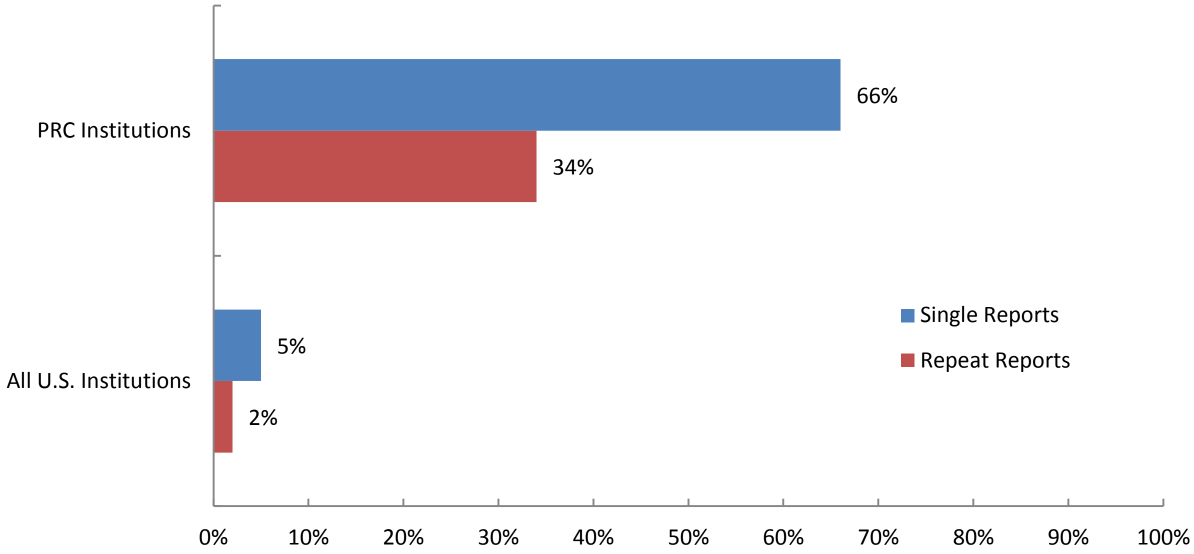

Figure 4. Single and repeat breach reports between the institutions listed in the PRC (n = 324) and all U.S. Institutions

DR and MA institutions are most likely to have experienced more than one breach reported in the PRC. Fifty-four percent of DR institutions with breaches—or one-quarter of all the DR institutions in the United States—have had more than one reported breach. Twenty-one MA institutions had more than one reported breach in the PRC. AA and BA institutions were significantly less likely to have more than one reported breach (figure 5).

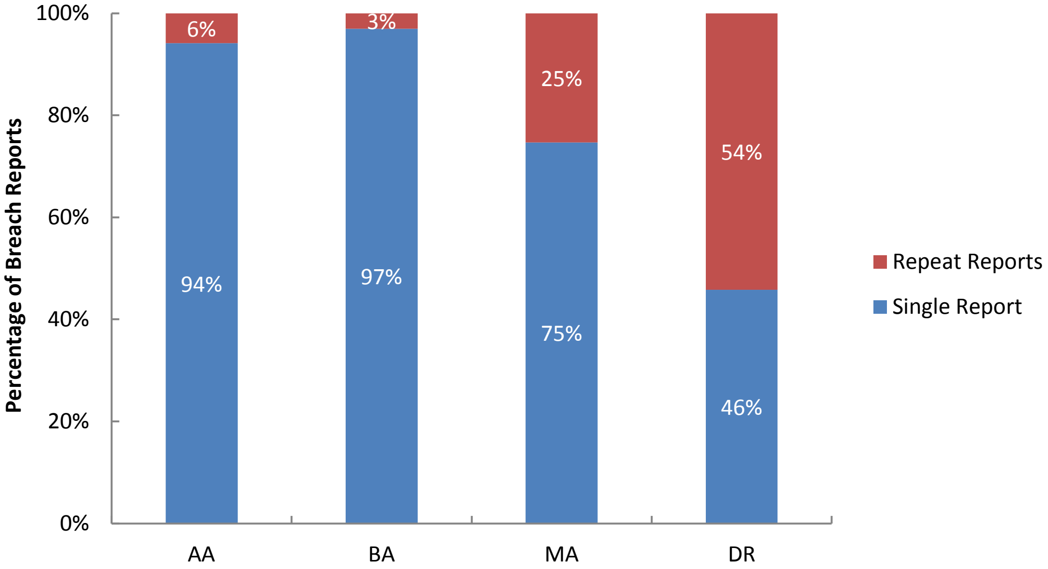

Figure 5. Proportion of single/repeat breach reports by Carnegie Classification in the PRC, 2005–2014 (ECAR data set, n = 324)

Unintended Disclosures and Hacking/Malware Are the Most Common Breaches in Higher Education

The PRC Chronology of Data Breaches classifies breaches into eight categories:

- **Payment Card Fraud (CARD):** Fraud involving debit and credit cards that is not accomplished via hacking.
- **Unintended disclosure (DISC):** Sensitive information posted publicly on a website, mishandled, or sent to the wrong party via e-mail, fax, or mail.
- **Hacking or malware (HACK):** Electronic entry by an outside party; data loss via malware and spyware.
- **Insider (INSD):** Intentional breach of information by someone with legitimate access (e.g., an employee or contractor).
- **Physical loss (PHYS):** Lost, discarded, or stolen nonelectronic records, such as paper documents.
- **Portable device (PORT):** Lost, discarded, or stolen portable devices (e.g., laptop, PDA, smartphone, portable memory device, CD, hard drive, data tape, etc.).
- **Stationary device (STAT):** Lost, discarded, or stolen stationary electronic device such as a computer or server not designed for mobility.
- **Unknown or other (UNKN):** Breaches that do not fit into the above categories or where a root cause has not been determined.[4]

[4] Privacy Rights Clearinghouse, Chronology of Data Breaches, Security Breaches 2005 to Present, Breach Legend, https://www.privacyrights.org/data-breach.

In higher education, the largest proportion of the reported breaches fall into the hacking/malware classification (36%). These are breaches where an outside party accessed records via direct entry, malware, or spyware. Thirty percent of the reported breaches were the result of unintended disclosure, where sensitive information was inadvertently made publicly available on a website or sent to an unintended recipient via e-mail or fax. Seventeen percent of the reported breaches were due to the loss of a portable device, such as a lost or stolen laptop or memory device (figure 6).

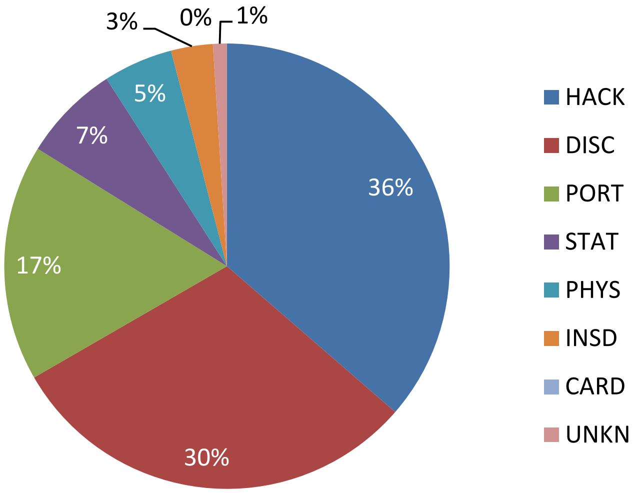

Figure 6. Types of data breaches in higher education, 2005–2013 (ECAR data set, n = 551)

Payment card fraud (CARD) is the least likely data breach classification seen among the reported breaches at higher education institutions. Only one breach, which occurred in 2012, was classified with this tag.

Conclusion

Education, and particularly higher education, is often singled out as having a large number of reported data breaches, and at first look, the PRC database appears to confirms that view. Look more closely at the data, however, and a different picture emerges. As an industry, education has some of the lowest counts of records exposed per breach incident—the number of reported breaches in the education industry does not mean more records containing personally identifiable information are being compromised.

Many speculate that higher education's culture of openness and transparency encourages breach reporting by institutions, even when such reporting is not legally necessary. This culture does not exist in other industry sectors, where breach reporting could damage an organization's ability to be competitive in that industry. In these instances, a breach may only be reported when it is required by a law or some other regulation, and even then, only when the breach circumstances clearly fall within the purview of the underlying regulation.

Higher education as a unique sector has long engaged in cooperative activities designed to improve the information security posture of all institutions. For instance, the Higher Education Information Security

Council (HEISC)[5] has created a number of materials that address information security practices in higher education. In particular, *The Information Security Guide: Effective Practices and Solutions for Higher Education*[6] includes an Incident Checklist and Data Incident Notification Toolkit, which can be used during the process of responding to incidents that require external notification. The guide also contains additional materials about risk management in higher education, as well as an information security program assessment tool.[7]

The EDUCAUSE Center for Analysis and Research (ECAR) provides research and analysis about information technology in higher education for IT professionals and higher education leaders. ECAR is higher education's only subscriber-driven research organization dedicated to understanding IT's role in colleges and universities. Learn more at educause.edu/ecar.

For more information about the Higher Education Information Security Council (HEISC) and the EDUCAUSE Cybersecurity Initiative, visit http://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-initiative.

Questions about this research should be directed to Joanna Grama (jgrama@educause.edu).

[5] Established by EDUCAUSE and Internet2 in July 2000, the Higher Education Information Security Council (HEISC) works to improve information security, data protection, and privacy programs across the higher education sector.

[6] "The Information Security Guide: Effective Practices and Solutions for Higher Education," https://wiki.internet2.edu/confluence/display/2014infosecurityguide/Home.

[7] Information Security Program Assessment Tool, available from http://www.educause.edu/library/resources/information-security-program-assessment-tool. More information about the current landscape of higher education risk factors, including data breaches, can be found in a forthcoming ECAR report of IT governance, risk, and compliance, available from http://www.educause.edu/library/resources/it-governance-risk-and-compliance-higher-education.