Data Breaches – It Could Happen to YOU!

How Big is the Problem of Data Breaches in Education?

Nationally, 21 MILLION P-20 education records have been exposed in 829 reported data breaches between 2005 and early 2018.

On average, that is 1.6 MILLION person's records exposed every year or 4,421 per day, every day, for 13 years. Adding fuel to the fire, many organizations were repeat offenders – meaning they were not learning from their own mistakes or the mistakes of others.

No, it's Actually MUCH Worse than Reported

Sadly, the 15.9 MILLION number is probably conservative. Why? There are 2 big reasons:

1. Out of the 793 EDU data breaches, 30% reported the number of records exposed as "unknown." Based on some of the descriptions of these breaches, it is obvious the numbers of records could be in the thousands for each; but without specific data, their numbers aren't figured in.
2. As stated, these are only the REPORTED breaches. For every breach that the Clearinghouse is aware of, many more are swept under rugs.

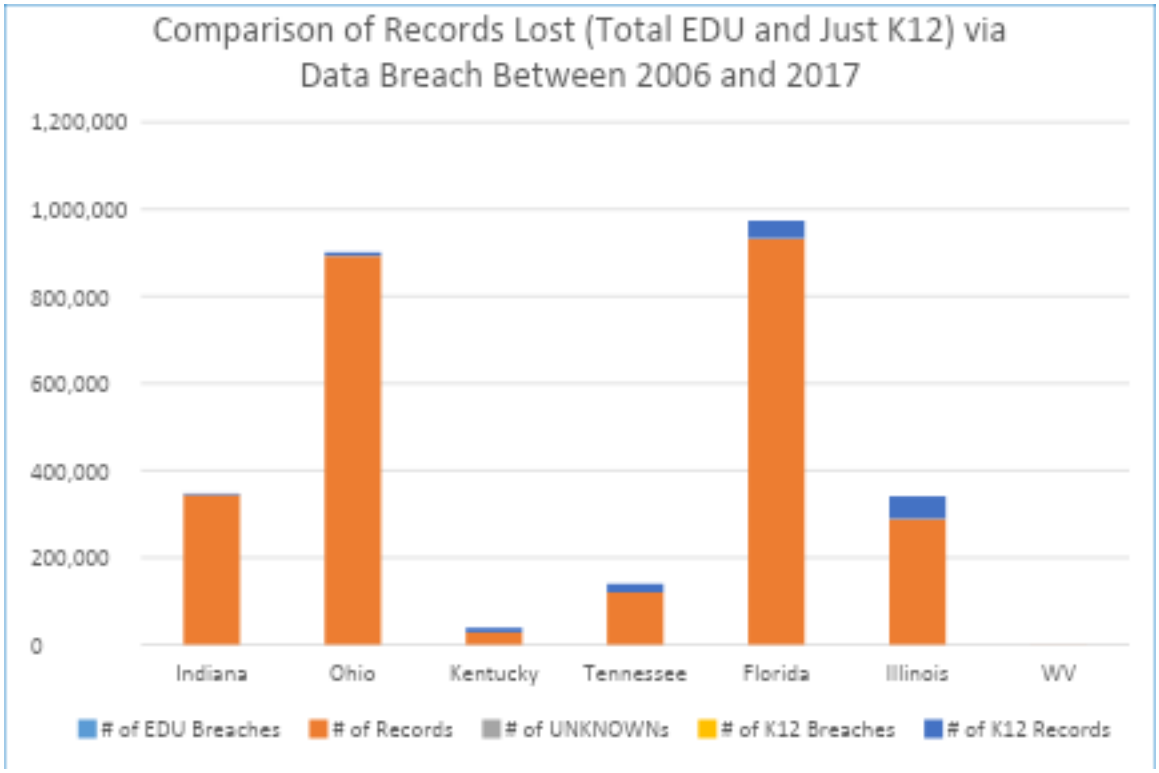
How is Kentucky Doing?

Since 2005, 35 data breaches have occurred all along the P-20 "educational pipeline" in Kentucky including the Kentucky Department of Education for a total of 28,564 exposed records. K12 is responsible for 10,620 exposed records.

State government is not immune. Despite new laws and improved processes, the Commonwealth Office of Technology states that 174 data breaches were reported to them by other state agencies during the period between October 2015 and September 2016.

Summary of Breaches to Education Organizations in Kentucky 2006-2017

DATE	ORGANIZATION	RECORDS
06/01/06	UK	1,300
06/22/06	UK	6,500
08/15/06	UK	630
08/15/06	UK	80
01/25/08	MuSU	260
05/17/08	UL	20
08/15/09	NKU	200
09/02/09	BCTC	100
09/23/09	EKU	5,045
10/21/09	K12 Public School District	676
06/02/10	UL	709
08/20/10	UK	2,027
12/15/11	K12 Public School District	UNKNOWN
01/31/15	K12 Public School District	1
03/08/15	K12 Public School District	75
03/10/15	KDE	1
04/14/15	K12 Public School District	345
04/16/15	K12 Public School District	16
05/02/15	K12 Public School District	1
07/15/15	KDE	1
09/10/15	K12 Public School District	2800
11/17/15	K12 Public School District	1
12/04/15	K12 Public School District	UNKNOWN
03/02/16	K12 Public School District	10
03/22/16	KSU	1,071
09/08/16	K12 Public School District	10
03/15/17	K12 Public School District	1
03/22/17	K12 Public School District	54
05/12/17	K12 Public School District	22
06/28/17	K12 Public School District	1
09/28/17	K12 Public School District	6,000
10/20/17	K12 Public School District	191
01/12/18	K12 Public School District	1
01/16/18	K12 Public School District	151
02/09/18	K12 Public School District	~264



How Can I Avoid a Data Breach?

1. Know YOURSELF and YOUR business
    - Know WHERE your data are - do a data system (files, databases, etc.) census
    - Know WHICH systems contain the top secret data and how data are transmitted
    - Know WHO is responsible for each system and WHO has access to each
    - Keep user accounts with access to your systems to a minimum. Disable or delete non-essential accounts

2. Protect your data
    - Keep Top Secret data off of USB drives, laptops, and mobile devices
    - Encryption is your friend because it makes PII useless and prevents breaches. However, you MUST have a strategy before implementing encryption across your enterprise
    - When it is time to delete top secret data, do it completely. Cross-cut shred paper and remember not just to delete files, but also to empty recycle bins and trash folders

- Do not email screen shots of top secret data

3. Training is KING when it comes to protecting data
    - Smart hackers hack PEOPLE, not technology.
    - Even though training is KING, technology is STILL your bullet-proof vest. It won't stop everything, but if the bullets are flying, wouldn't you rather walk around with a bullet-proof vest than not?
    - Make sure you have data and security policies and that folks are aware of them
    - Have a breach procedure in place; who do people call if they recognize a breach?

4. Improve your Passwords/Authentication
    - Have reasonably complex passwords or passphrases that expire – BUT:
    - Too much complexity in authentication breeds MORE attack vectors, like staff posting them on monitors. Make it as easy as possible to be successful with passwords
        - Longer is better than super-confusing
        - Use a unique password for each application or system
        - Try to use a password no one has ever thought of ("p@55W0rd" doesn't count!)
        - Be wary of password hints (we give them all away on Facebook, anyway)
        - Look at multifactor authentication (MFA) everywhere you can, even though it shifts some complexity to IT. ALL Admin accounts should already use MFA.

5. Understand that you WILL have a breach at some point
    - There's no such thing as 100% secure
    - Do folks in your district know whom to call?

Detailed Kentucky Education Organization Data Breaches

University of Kentucky, June 1, 2006 – Unintended Disclosure 1,300 Records

Personal information, including SSNs, for 1,300 current and former University of Kentucky employees was inadvertently made available on the UK website for 19 days.

University of Kentucky, June 22, 2006 – Portable Device 6,500 Records

The personal data of 6,500 current and former University of Kentucky students including classroom rosters names, grades and Social Security numbers was reported stolen following the theft of a professor's flash drive.

University of Kentucky, August 15, 2006 – Unintended Disclosure 630 Records

The names and SSNs of 630 University of Kentucky students were posted on the University's financial aid web site for 4 days.

University of Kentucky, August 15, 2006 – Unintended Disclosure 80 Records

About 80 University of Kentucky geography students were notified that their SSNs were inadvertently listed on an e-mail communication they all received telling them who their academic advisor would be for the coming year.

Murray State University, January 25, 2008 – Unintended Disclosure 260 Records

Names, Social Security numbers, dates of birth and other personal information of 260 Murray State University students and professors had been posted online in a publicly accessible report titled "2000-2001 State Admissions Report." The report, which was supposed to have been posted as a PDF, was instead posted in the original Excel format, with hidden columns or tabs containing confidential information. The information was pulled from the website and affected individuals were contacted shortly after Murray was notified of the breach.

University of Louisville, May 17, 2008 – Physical Loss 20 Records

Documents containing personal information, including Social Security numbers, student and employee identification numbers and salary information, for 20 current and recent University of Louisville student employees were copied and taken from the president's office, to its Internal Audit Office and Department of Public Safety. The university learned of the theft when salary information was shared anonymously with some employees in the office.

Northern Kentucky University, August 15, 2009 – Portable Device 200 Records

A Northern Kentucky University employee's laptop computer - which contained personal information about some current and former students -- was stolen from a restricted area. The personal information stored on the employee's computer included Social Security numbers of at least 200 current and former students.

Bluegrass Community and Technical College, September 2, 2009 – Hacking or Malware or Insider 100 Records

A file containing the personal information including Social Security numbers of nearly 100 students at the Bluegrass Community and Technical College was stolen.

Eastern Kentucky University, September 23, 2009 – Unintended Disclosure 5,000 Records

The names and Social Security numbers of about 5,000 Eastern Kentucky University faculty, staff and student workers were posted inadvertently on the Internet last September, where they were on display for a year.

K-12 District October 21, 2009 – Unintended Disclosure 676 Records

During open enrollment for insurance, a public school employee accidentally sent an email containing names and SSNs of 676 district staff, who hadn't yet completed the process, to nearly the entire district (about 1,800 folks). This was obviously an accident. The email was supposed to just be a reminder to the 676 folks to complete the process, and instead it has become a reminder of a completely different sort.

Email is such an easy form of communication and method of sharing that we often do not spend as much time as we should preparing our message. Always know what information is being shared, regardless of media.

University of Louisville, June 2, 2010 – Unintended Disclosure 708 Records

A University of Louisville database of 708 names, Social Security numbers and dialysis details was available on the Internet without password protection for nearly a year and a half. The Web site was disabled on May 17 when the university discovered the flaw. University officials said in a statement that accessing the database would not have been easy, and no direct links to the database were discovered. The information was available so long because the U of L doctor who set up the Web site thought the information was protected by a password and other precautions. U of L was finally notified when someone outside the university sent an e-mail about open access to the information. The Web site was shut down an hour later.

University of Kentucky, August 20, 2010 – Portable Device 2,027 Records

A laptop from the Department of Pediatrics Newborn Screening Program was stolen from a locked private office. Dates of birth, names and medical record numbers for 2,027 patients were on the password-protected laptop. Some patients also had Social Security numbers on the laptop.

K-12 District, December 15, 2011 – Unintended Disclosure 6,500 Records

Around 6,500 ACT Explore test results were accidentally mailed (on paper) to incorrect addresses. It's unknown how much top secret information was actually exposed in this example, but the parents were encouraged to shred the information they'd received. No SSNs were exposed, but the test results were certainly bad enough.

K-12 District, January 31, 2015 – Unintended Disclosure 1 Record

1 teacher's top secret personal data was exposed for an undetermined amount of time after copying the contents of local "My Documents" folder to OneDrive's "Shared with Everyone" folder where it was literally available to everyone in KETS. Records indicated that it had only been accessed by 1 other person, so it wasn't as bad as it could have been. Districts have been advised to ask staff to delete the "Shared with Everyone" folder because it is such a dangerous feature.

K-12 District, March 8, 2015 – Phishing, Hacking or Malware 75 Records

While working from home using a district-owned device, a pop-up window, purporting to be a local Internet provider warning of a virus, looked legitimate enough to convince a district employee to call the

provided phone number. She was further convinced to allow remote access to the computer. Second-thinking the decision, she called a district technician who advised her to disconnect and shut down the unit immediately. Upon inspection, district technicians discovered recently installed malware, and a determination of a security breach was made. Top secret data for 75 students was exposed.

Kentucky Department of Education, March 10, 2015 – Physical Loss or Theft 1 Record

Laptop with 1 staff person's timesheets on it stolen from residence.

K-12 District, April 14, 2015 – Unintended Disclosure 345 Records

Excel spreadsheet containing PII accidentally emailed to all 345 district employees

K-12 District, April 16, 2015 – Unintended Disclosure 16 Records

Personal information, including SSNs, for 16 candidates for the job of Superintendent in 2 districts was briefly exposed on a Kentucky association's website. Logs indicated that the personal information had not been accessed until it was discovered by a school employee

K-12 District, May 2, 2015 – Unintended Disclosure 1 Record

Military orders for 1 employee requesting leave were accidentally posted to an e-meeting website.

Kentucky Department of Education, July 15, 2015 – Physical Loss or Theft 1 Record

Laptop with top secret data for 1 employee on it stolen from car.

K-12 District, September 10, 2015 - Phishing, Hacking or Malware 2,800 Records

A phishing scheme ("Your PC is Infected! Call This Number NOW!) allowed access to a nutrition services computer at the district's High School, on which a database of the personal information for is stored. Without a reliable way to know how many person's top secret data was stolen, the district stepped up and assumed all 2,800 persons were affected.

K-12 District, November 17, 2015 – Unintended Disclosure 1 Record

A file with PI for a teacher whose account had been disabled was shared with everyone via OneDrive.

K-12 District, December 4, 2015 – Phishing, Hacking or Malware Unknown # of Records

An unknown number of district staff were tricked by a Phishing email into sharing PII and passwords.

K-12 District, March 2, 2016 – Physical Loss or Theft 10 Records

An employee took a personally-owned folder home, but removed the contents of the folder, which had PI for 10 persons in it. The contents of the folder could not be located.

Kentucky State University, March 22, 2016 – Phishing, Hacking or Malware 1,071 Records

Kentucky State University experienced a data breach on March 22 when an employee, responding to an email supposedly from the school's president, sent W-2s for employees and students to the attacker.

K-12 District, September 8, 2016 – Physical Loss or Theft 10 Records

Paper documents for 10 district staff were unprotected at a local Bank on a bank employee's desk. They were then accidentally taken from the bank by a customer who then apparently discovered them but left them at another business, where the owner of that business found them, and returned them to the bank.

K-12 District, March 15, 2017 – Unintended Disclosure 1 Record

A teacher accidentally posted 1 student's ARL/IEP notice to FaceBook, when attempting to send it to the student's parent.

K-12 District, March 22, 2017 – Unintended Disclosure 54 Records

54 former students' personal information, including SSNs, were exposed when a file was discovered on the district's website via a google search for a former student's name. It is unknown why the file, a report from the student information system, had been posted.

K-12 District, May 12, 2017 – Unintended Disclosure 22 Records

Cumulative student records, including names, addresses, and SSNs were accidentally placed in a trash container and improperly disposed of.

K-12 District, June 28, 2017 – Unintended Disclosure 1 Record

A contract containing name and SSN was submitted with a board agenda and posted online.

K-12 District, September 28, 2017 – Phishing, Hacking or Malware 6,000 Records

Staff email account containing emails with files having the SSNs for over 6,000 students and staff was compromised.

K-12 District, October 20, 2017 – Unintended Disclosure 191 Records

An email attachment was sent mistakenly to the in-district email distribution list. All employees having received this email are governed and trained by Acceptable Use Policy, HIPPA and FERPA guidelines. Action was immediately taken to recall and delete unread copies. Many were successful. Some were not. Employees have been notified of this incident.

K-12 District, January 12, 2018 – Insider Breach 1 Record

Video of staff suffering medical condition shared maliciously

K-12 District, January 16, 2018 – Phishing, Hacking or Malware 151 Records

A district staff apparently fell victim to a phish, allowing access to adult and student PII

K-12 District, February 9, 2018 – Phishing, Unintended Disclosure ~246 Records

Records containing name, HR and SSN data was posted briefly online with a board agenda.