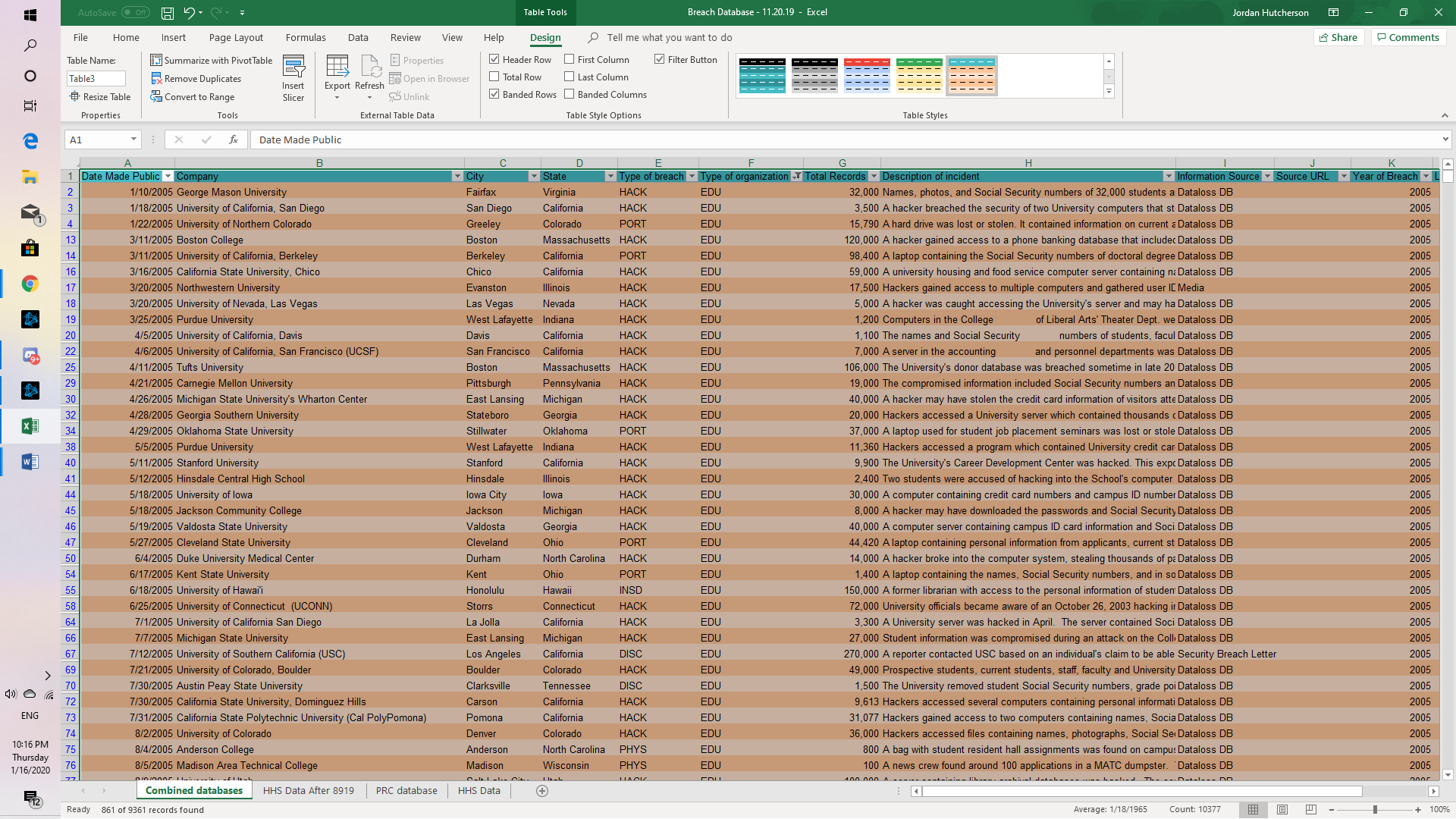
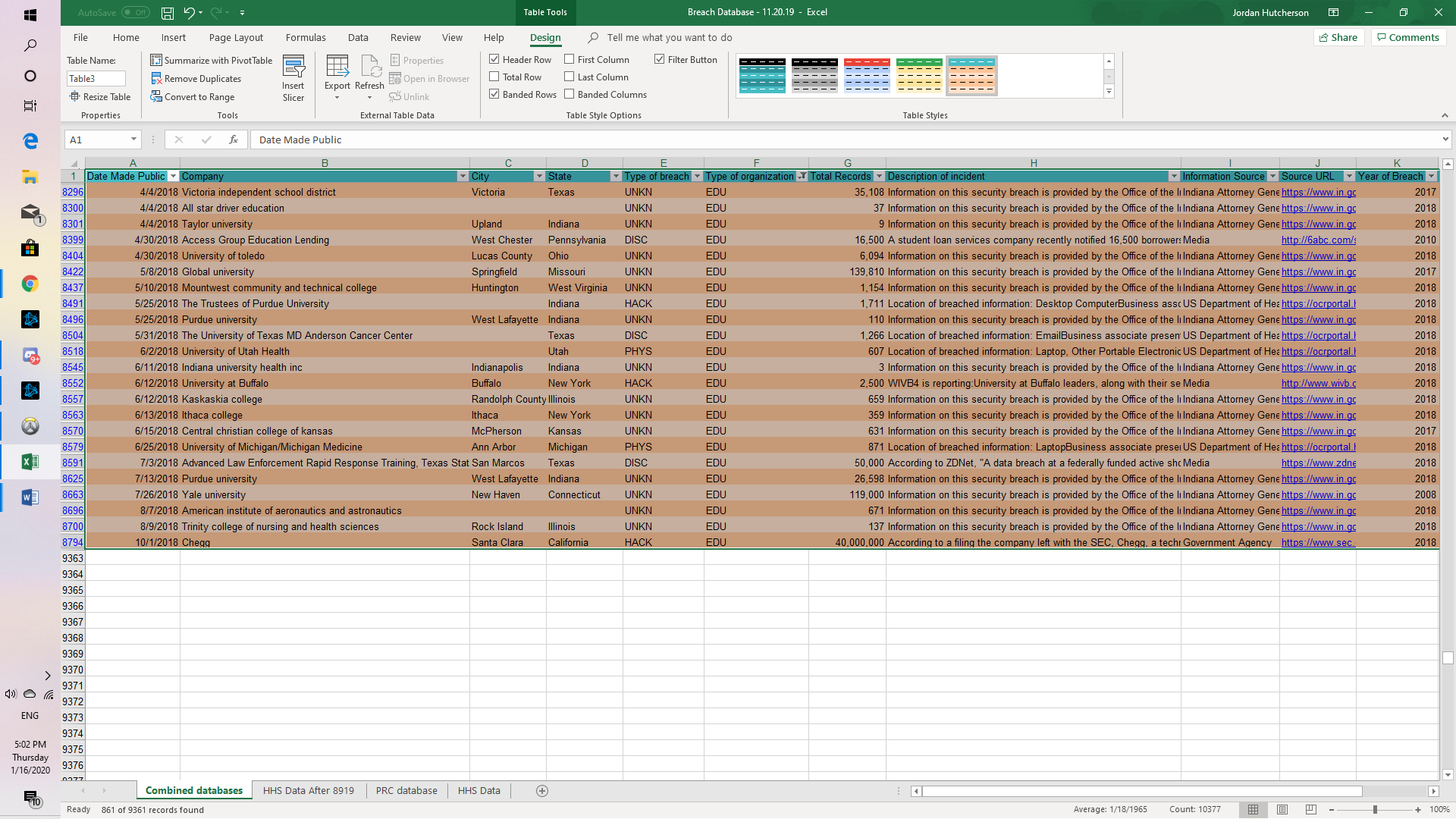
Hands on project 1-1

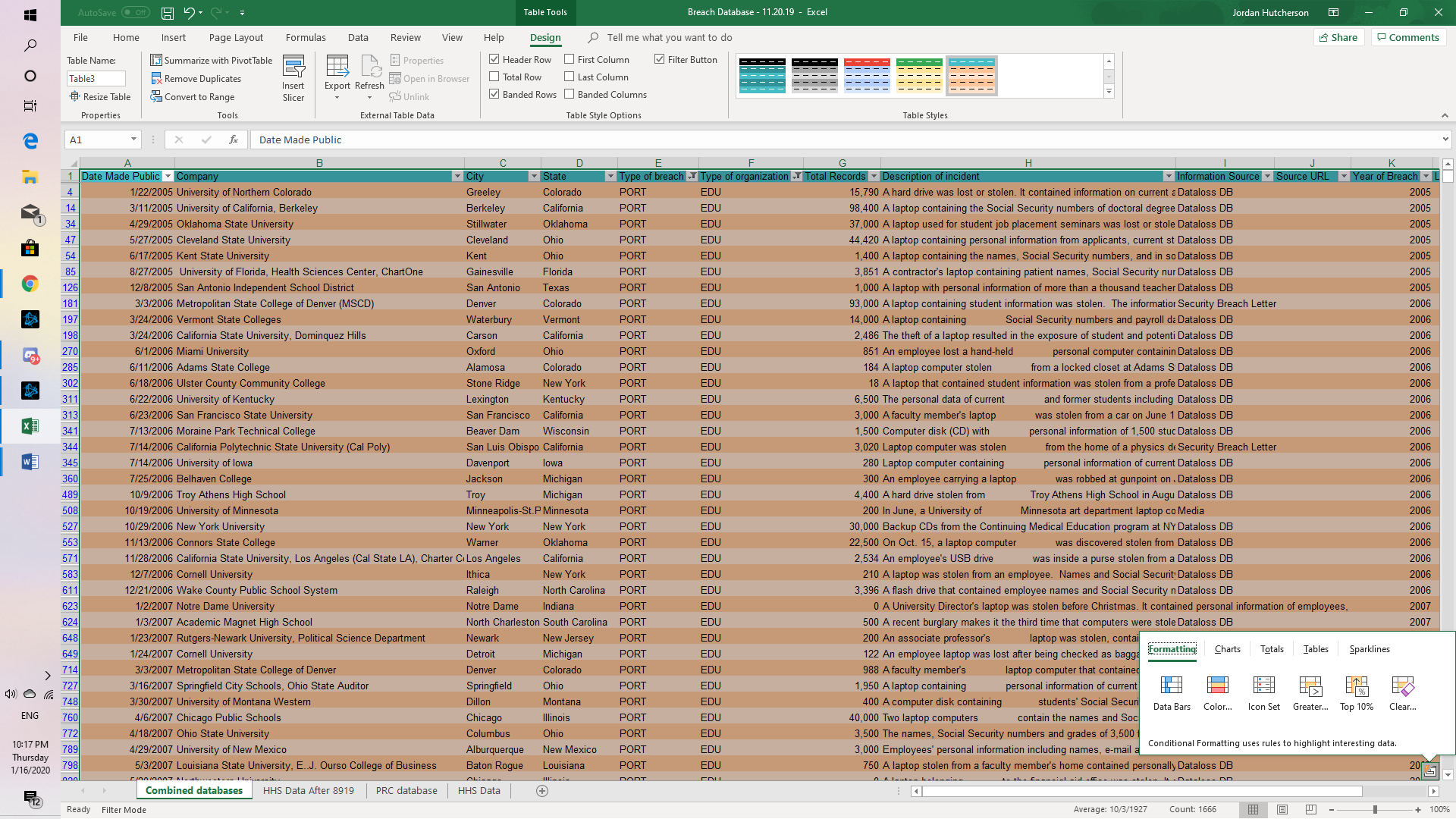
In the search bar enter a school, organization, or business with which you are familiar to determine if it has been the victim of an attack in which your data has been compromised: George Mason University.



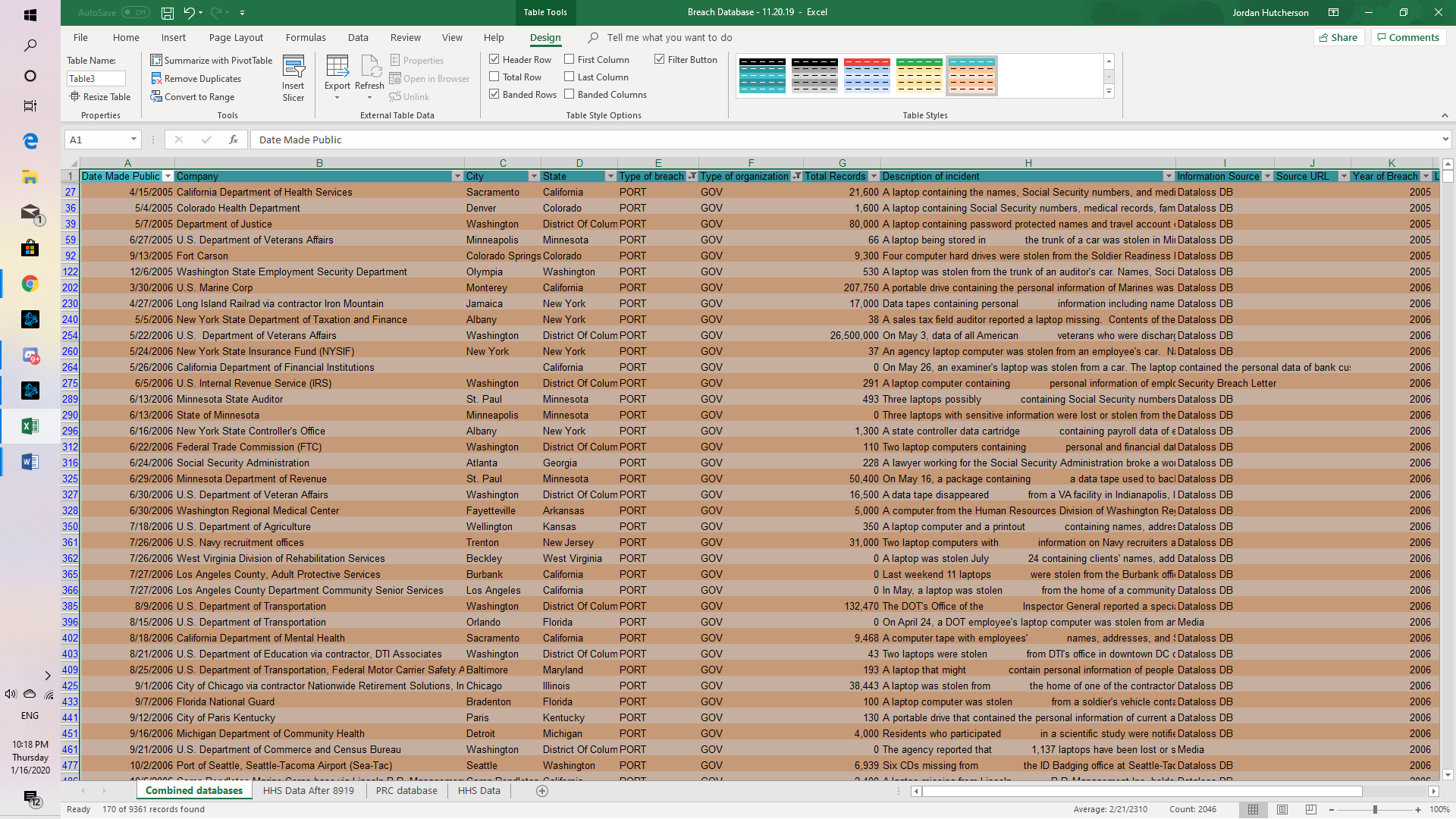
Read the **Breach Subtotal** information. How many breaches that were made public pertain to educational institutions? How many total records were stolen?

8794 were made public to educational institutions and was stolen. 

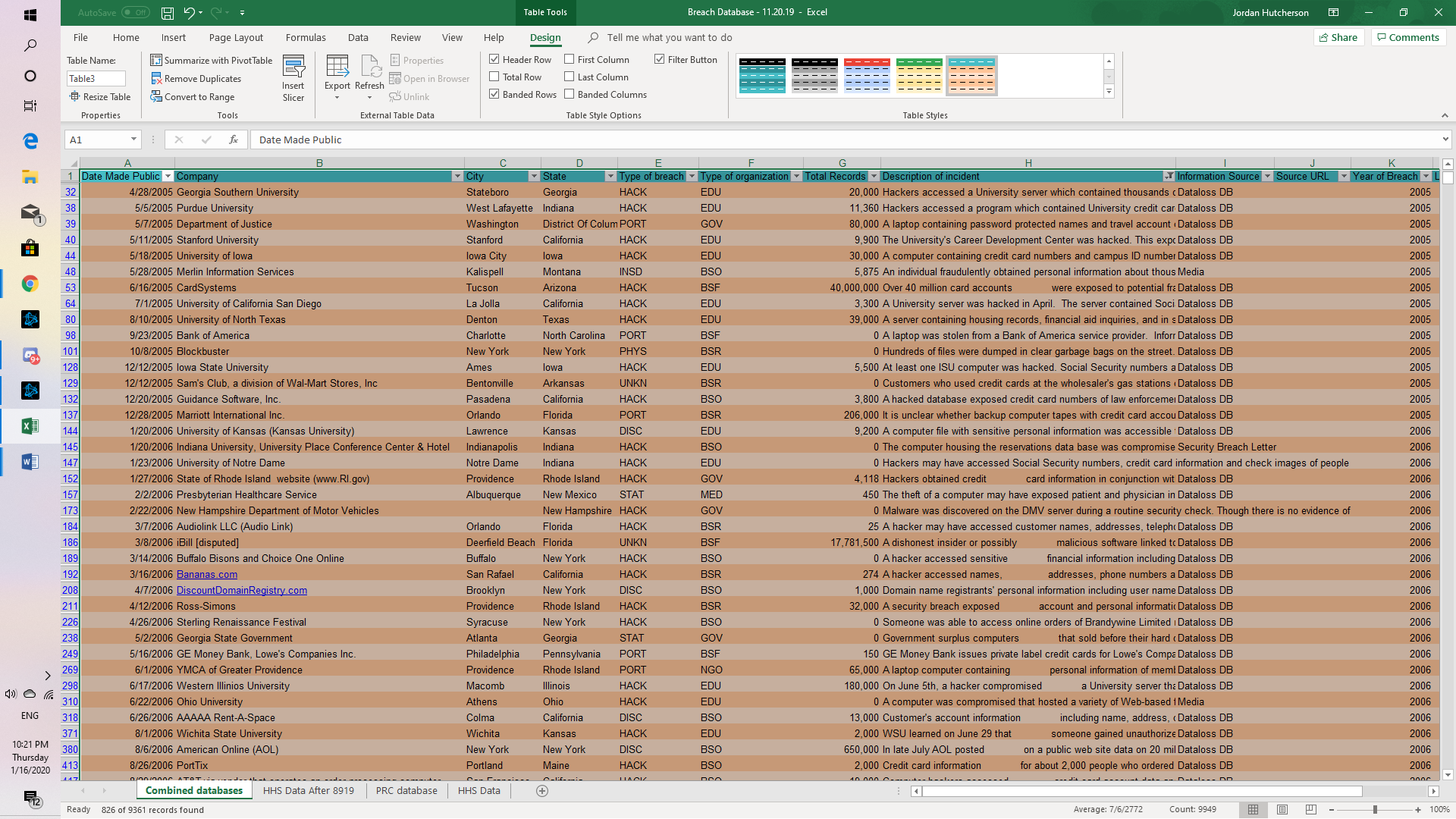
Now search for breaches that were a result of lost, discarded, or stolen equipment that belonged to the government and military. Under **Choose the type of breaches to display**, check **Portable device (PORT) - Lost, discarded or stolen laptop, PDA, smartphone, portable memory device, CD, hard drive, data tape, etc**.



Under **Select organization type(s)**, check **GOV - Government & Military**.



Now create a search based on criteria that you are interested in, such as the Payment Card Fraud against Retail/Merchants during the current year.



Open the file and then scroll down the different breaches. What should the government be doing to limit these breaches?

The government could train federal employees on security best practices. It’s the IT department’s responsibility to know what’s at stake when weak security policies are in place, not the end-users. They could also implement a bug bounty program from outside sources which allow software developers to discover bugs in the system before they can do widespread damage. Hack the Pentagon is was a great security initiative to bring outside sources to identify IT infrastructure weaknesses in a controlled environment.

One-way professionals can use this information is having all employees encrypt their hard drives with built in programs which are free. Hacking isn’t always about illegally accessing your data through the web. It can be more immediate. Someone can steal a company computer with valuable information on it and have access to so much data and lastly they could have IT department show the company employees or do it themselves to set your operating system to auto-update because companies are always offering updates that enhance the security of apps and operating system’s they build. If you have the computer to auto-update it will ensure you are never unnecessarily vulnerable to attacks.

They are many reasons professionals can look at this data and just not care and be un-ethical about it. One of many reasons companies get hacked is failure to check code before it’s deployed. Injections, which is a popular vector of attack which is covered in chapter 1, has been a known vulnerability for 15 years. By checking code/testing it. Businesses can remove vulnerabilities before launching the app/software. I think another big issue that ill cover is failure to update default passwords. This is a big issue I think because people/companies use easy passwords that are so simple. Neglecting to change default passwords is an underlying issue in massive DDos attacks. If a business has the same password on multiple devices, access to one means access to all and we know where that leads too.