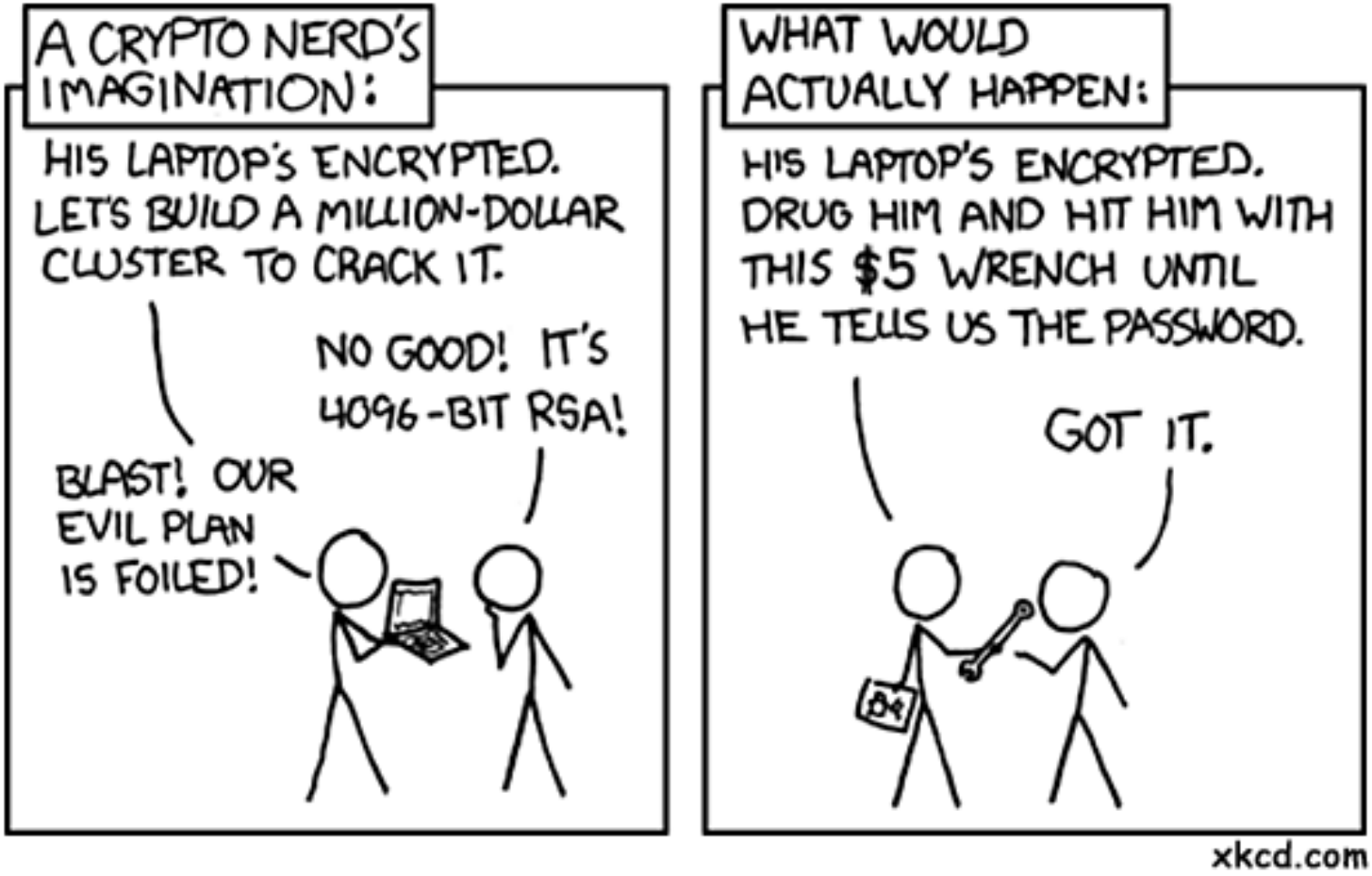
Colorado Data Breach Exercise

Michael B. Hawes
Statistical Privacy Advisor
U.S. Department of Education


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.
xkcd.com

District Data Breach Exercise

- Table top exercise that simulates a data breach within a complex organization.
- Intended to put you in the shoes of critical decision makers who have just experienced a data breach.
- This is a REAL-LIFE data breach that happened in the last 90 days in the education world. IT CAN HAPPEN TO YOU!!

District Data Breach Exercise

- You will be divided into teams to react and respond to the scenario.
- Over time, the scenario will be more fully revealed and you will discover more about what happened.

Be Prepared for the Unexpected!

Suggestions

- Think about each of the roles needed in your organization (e.g., public information officer, data system leadership, attorney, auditors, etc.).
- The full extent or impact of a data breach is rarely known up front. Do your best to anticipate what might happen, but don't get ahead of yourself.

District Data Breach Exercise

Each team will develop two key products:

1. **Public and Internal Communications/ Messaging** – Develop the message(s) you will deliver to your staff, students, parents, the media, and the public.

During the event, you will be asked to participate in press conferences about the scenario. Be prepared to respond to members of the media about what is happening and how your organization is responding.

District Data Breach Exercise (cont.)

2. Response Plan – Outline how your agency will approach the scenario and what resources you will mobilize. Describe who will compose your response team. Identify goals and a timeline for your response.

Background

- Your school district has 15,000 students.
- Your district provides centralized IT services and support for K12 schools as well as access to a centrally managed Student Information System (SIS).

Background *(cont.)*

- Approximately one year ago, your SIS vendor had a data breach in which a small portion of your students education records were exposed to the public facing internet.
- Your SIS vendor provided those students' parents free credit monitoring/identity theft insurance for 1 year.
- As a result of this breach, you updated your policies on vendor contracts requiring FERPA's *reasonable methods* for protecting data.

Scenario

- A concerned citizen calls your central district office upon discovering publically available data on “Dropbox”. They didn’t know who posted it, but thought you should be aware.

District Data Breach Exercise

1. Gather with your team.
2. Go over the scenario carefully. What do you know? What don't you know?
3. Begin building your response. Elect a team member to take notes.

Data Breach Exercise *(cont.)*

4. During the scenario, you will receive additional information about the breach. Read each of these updates as the scenario unfolds.
5. We will occasionally pause to discuss where we are, and eventually give a press statement.

This exercise works best if approached as a "murder mystery" game. The more you synthesize the information and role play, the more useful the exercise becomes.

Questions?

ACME District Data Breach Exercise

10 Minutes

Questions to consider…

- Is there evidence of an actual breach?
- Do you have any legal responsibilities at this point?
- How do you respond to the findings? Acknowledge? Remain mute? Aggressively investigate?

Scenario Update

The news of the Dropbox breach has now reached the media. The Colorado Springs Gazette reports that about 1,200 students who possess individualized education programs (IEPs) had personal information posted to a public Dropbox site attending schools in Colorado. The Superintendent wants answers on how this happened and wants a brief prepared for her press conference.

Scenario Update

- How do you respond to your leadership?
- What information do you plan to provide?
- What are the assumptions you are making about the situation?
- Are you working on your resume?

ACME District Data Breach Exercise

10 Minutes

End

Scenario Update

Upon further forensic investigation, the data was inadvertently made available online "for several hours" on Tuesday and has since been taken down. In addition, it appears that it was posted by a district staff member.

Questions to Consider…

- How does this change your approach?
- Do you notify parents at this point? Are you required to by law? If so How?
- Does this event change your approach to the response activities? How?

ACME District Data Breach Exercise

10 Minutes

Next Assignment

- Red Team: Press Conference – You decide to take your response activities to the streets and hold a press conference where you will inform the public what is going on, how it happened and what you are currently doing to respond to the situation. Each group will select a "spokesperson" who will answer questions from the crowd.

- Green Team: Staff Training – Provide a summary of potential internal trainings needed to mitigate future incidents from occurring. Include specific topics that you plan to include in your training plan.

ACME District Data Breach Exercise

10 Minutes

Develop Incident Response Plan

- Use your notes from the scenario discussion.
- Identify an incident response team (e.g., CIO, Data Coordinator, IT Manager, legal counsel).
- Outline the steps to identify the source of the breach, catalog the data affected, and identify how it occurred.
- Should you involve law enforcement? When? What legal requirements exist?
- What preventative corrective actions should you implement?

ACME District Data Breach Exercise

10 Minutes

Your Response Plan

- Take us through your response plan. Include the who, what, when, and how of your activities.
- What were the driving factors in your decision-making process?
- Did your plan evolve as the scenario became more clear? How?
- How should you prepare to enable a prompt reaction to a potential breach?

Wrap-up

- Lessons learned from press conference.
- Incident Response Plans – what might work for us?
- What have you learned? Will it affect your behavior?
- How could this exercise be more useful to you?

Related PTAC Resources

- Contractor Responsibilities Under FERPA
- Training videos for district staff & to share with parents
- Data Breach Checklist & Activity Downloads

CONTACT INFORMATION

United States Department of Education,
Privacy Technical Assistance Center

(855) 249-3072
(202) 260-3887

privacyTA@ed.gov

http://ptac.ed.gov

(855) 249-3073