NCSHA

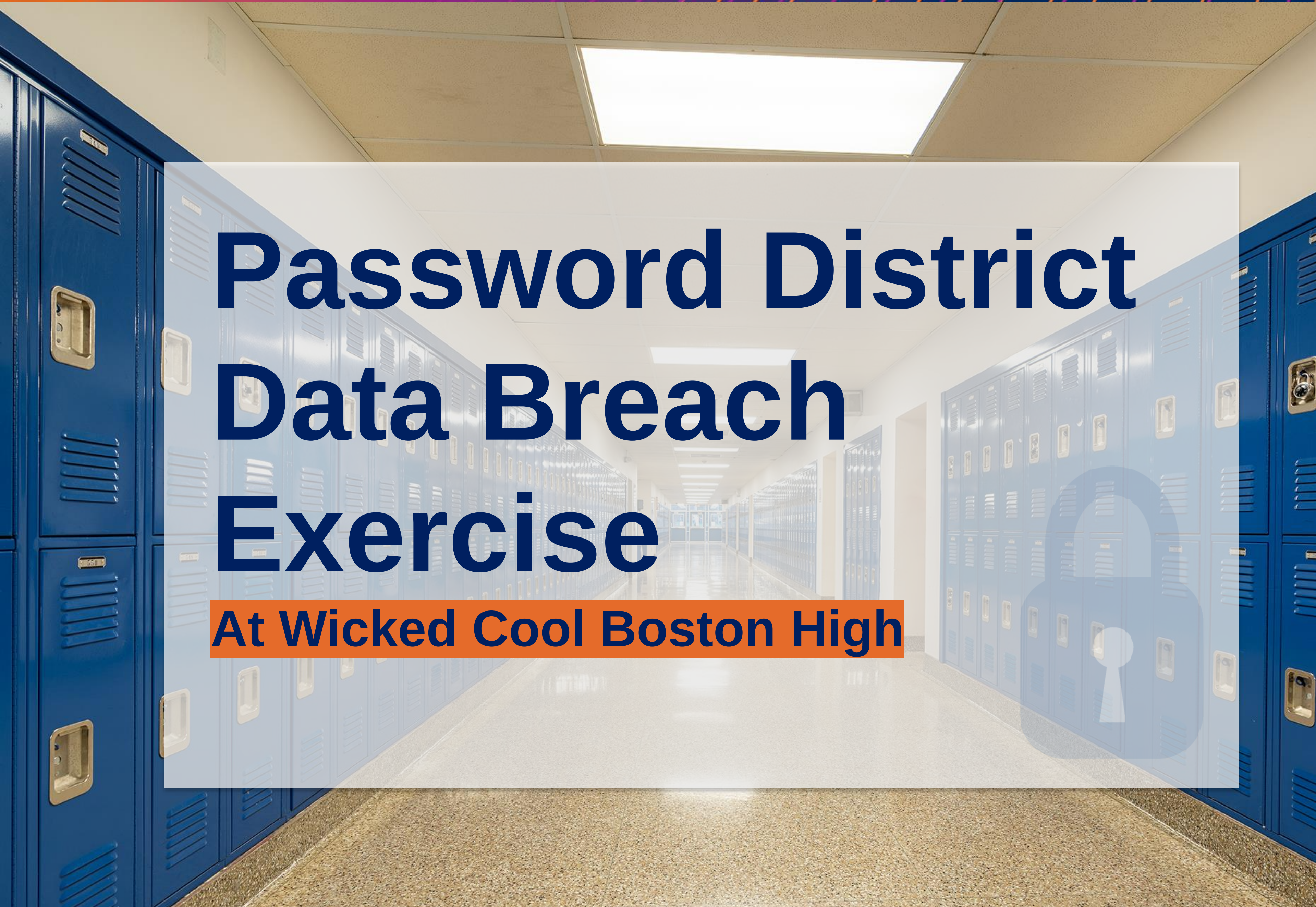
October 16, 2023

2023 BOSTON

Cybersecurity Tabletop

DISCUSSION LEADER
Delbert Collins, Director of Information Technology | South Carolina State Housing Finance and Development Authority

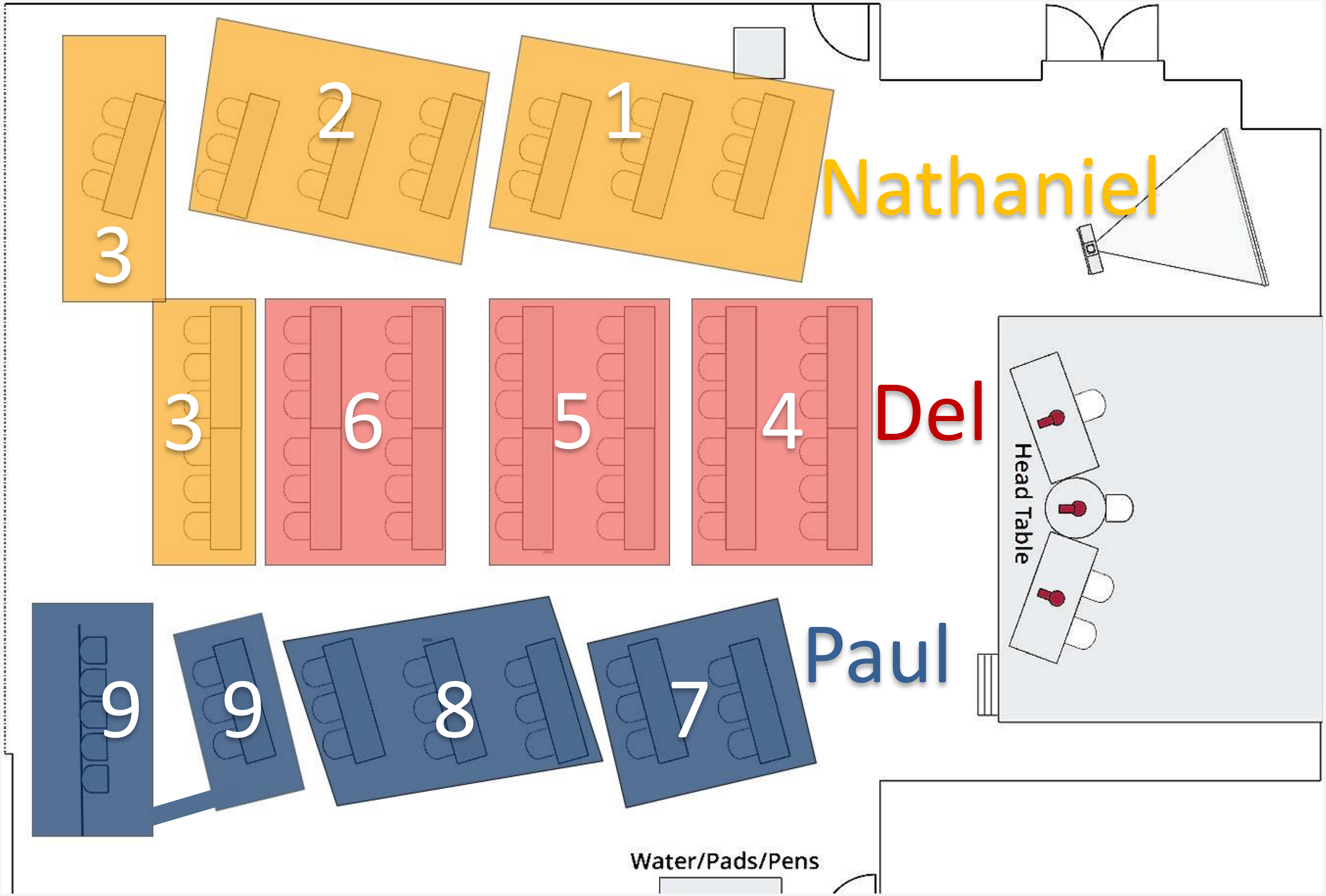
SPEAKERS
Nathaniel Borrero, Information Security Manager | Rhode Island Housing
Paul Cackler, Chief Information Officer | New York City Housing Development Corporation



Password District Data Breach Exercise

At Wicked Cool Boston High

Step One: Split into Groups



Password District Data Breach Exercise

- Tabletop 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.

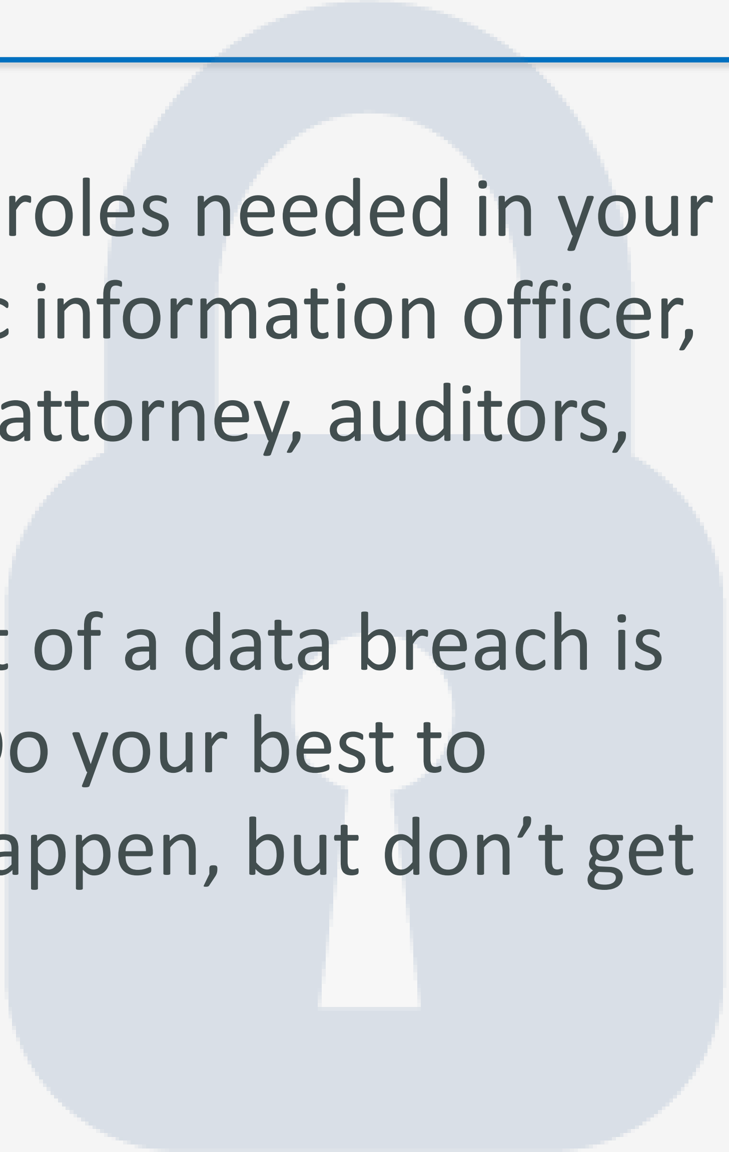
Password District Data Breach Exercise

- 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.



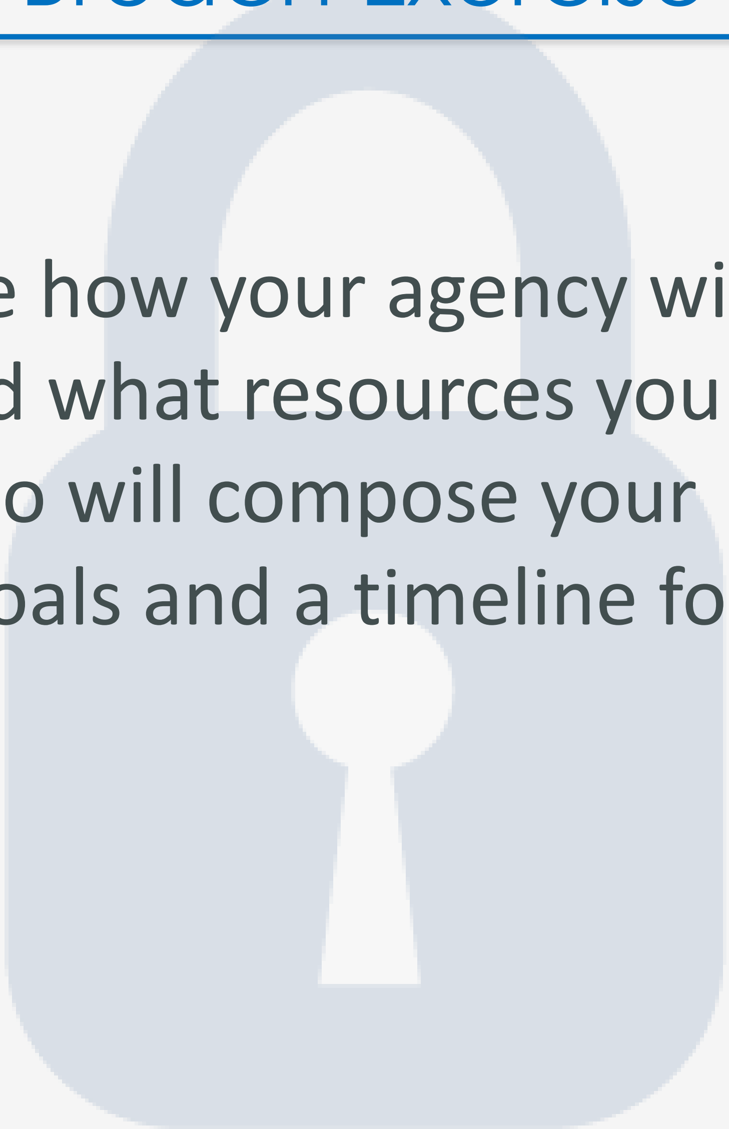
Password District Data Breach Exercise

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.

Password District Data Breach Exercise (cont.)



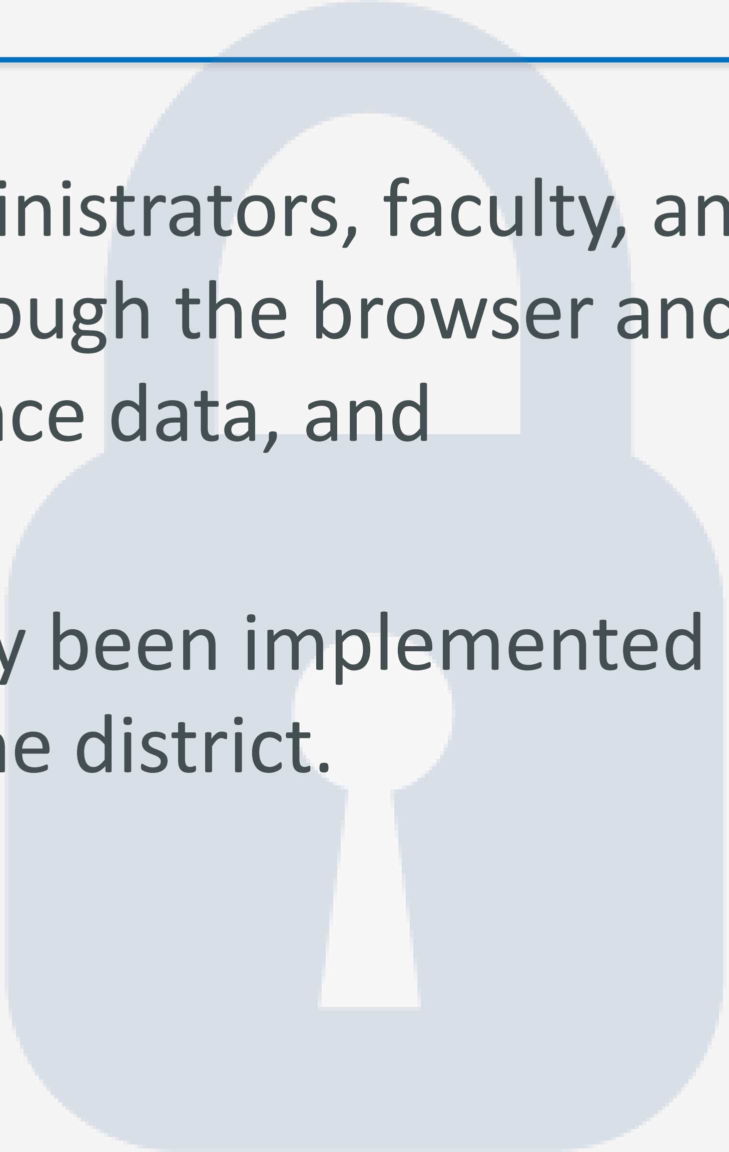
2.Response Plan – Outline how your agency will approach the scenario and what resources you will mobilize. Describe who will compose your response team. Identify goals and a timeline for your response.

Background

- Your school district has 46,169 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.)*

- The new SIS allows administrators, faculty, and other users to log in through the browser and upload grades, attendance data, and assessment data.
- The new system has only been implemented in a few test locations in the district.



Scenario

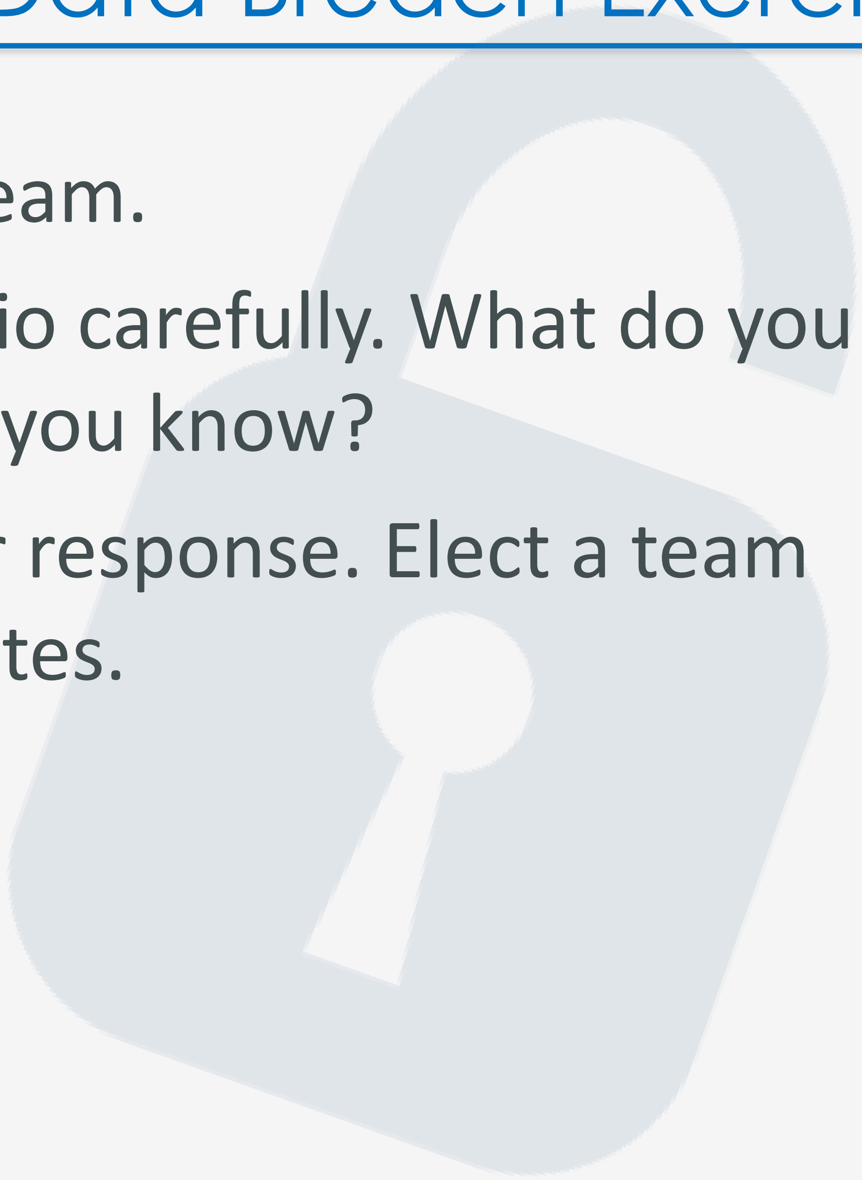
- Yesterday, a teacher, Mr. Conan O'Brien, notified the district IT manager that some course grades have been changed in the system. All the students in one course had their grades changed to reflect much better scores than they actually earned.

Scenario

- Initial investigation shows that someone logged on using the teacher’s login information and manually changed the grades.
- Additionally, the logs indicate that several reports were also downloaded from other systems, including some that contained private information (like SSN) about the school’s employees.

Password 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.



Password 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?

Password District Data Breach Exercise

10 Minutes

Where Are We?

- Have you begun to build a response plan?
- Can you make any concrete conclusions?
- Does the fact that the breach includes SSNs change the way you respond?

Scenario Update

- Logs indicate that the login occurred from the school’s Wi-Fi network after school hours.

Scenario Update

- Logs indicate that the login occurred from the school’s Wi-Fi network after school hours.
- Reports have surfaced about students offering to change additional grades for money. No names have yet been revealed.

Password District Data Breach Exercise

10 Minutes

End

Where Are We?

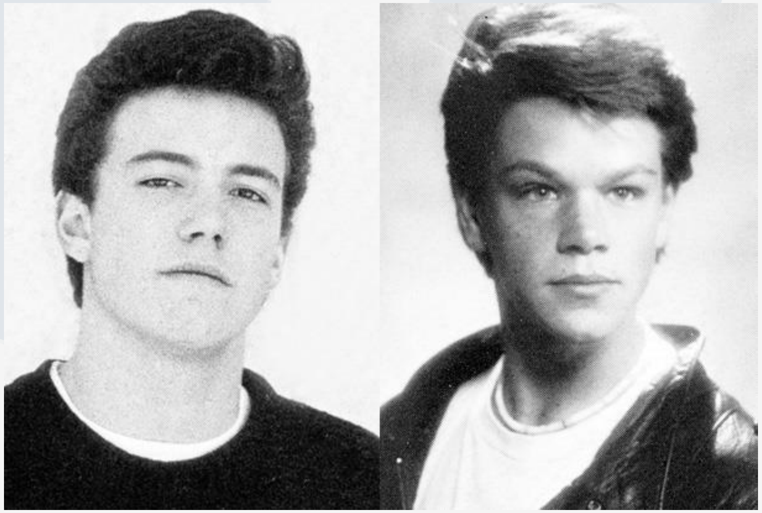
- Has the updated information changed your approach to the scenario?
- Think about what controls you could put in place to avoid a scenario like this.

Scenario Update

- Two juniors are rumored to be the culprits.

Scenario Update

- Two juniors are rumored to be the culprits.
- When questioned, they admit that they located a sticky note with a teacher’s username and password, which they used to log in to change the grades.



Scenario Update

- Students said that they also accessed some other school systems, including a database of employees that listed names, addresses, SSNs, employee ID numbers, etc.

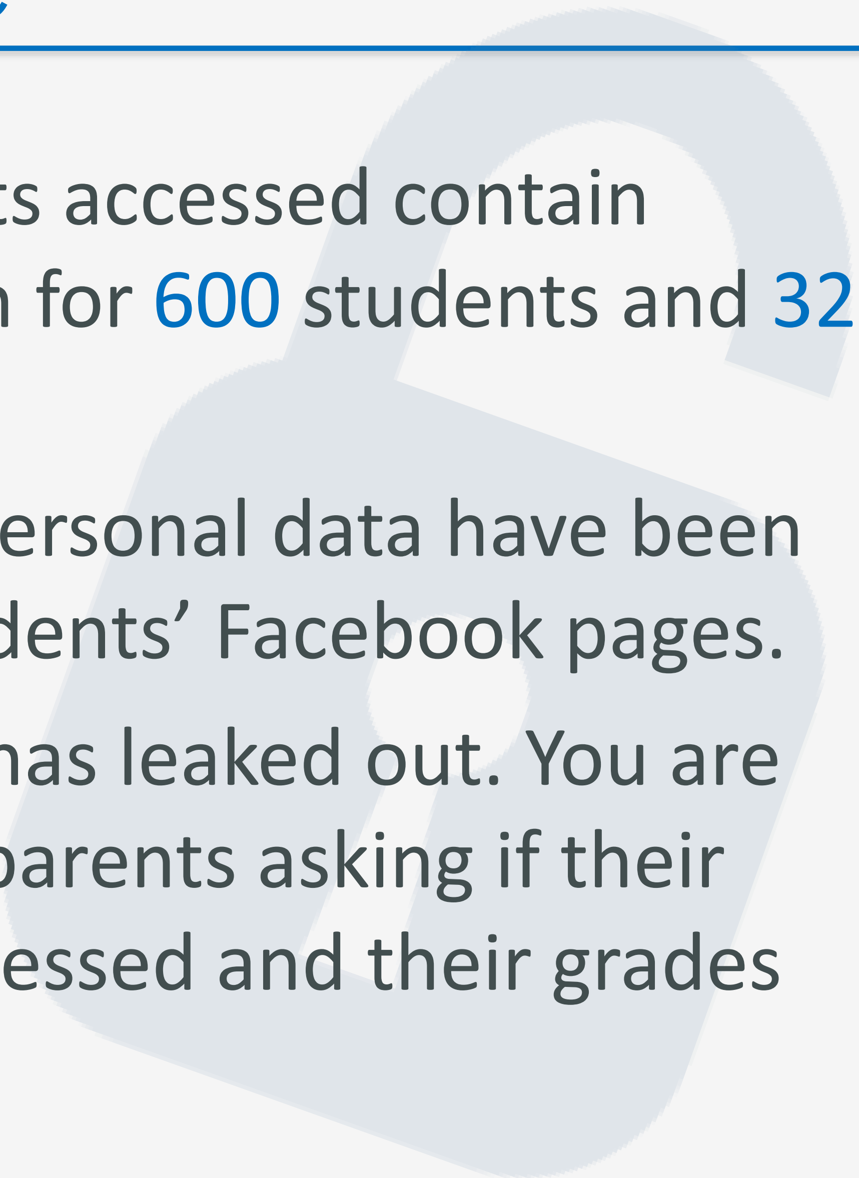
Password District Data Breach Exercise

10 Minutes

Where Are We?

- How has the updated information changed your approach to the scenario?
- What other information would be useful?

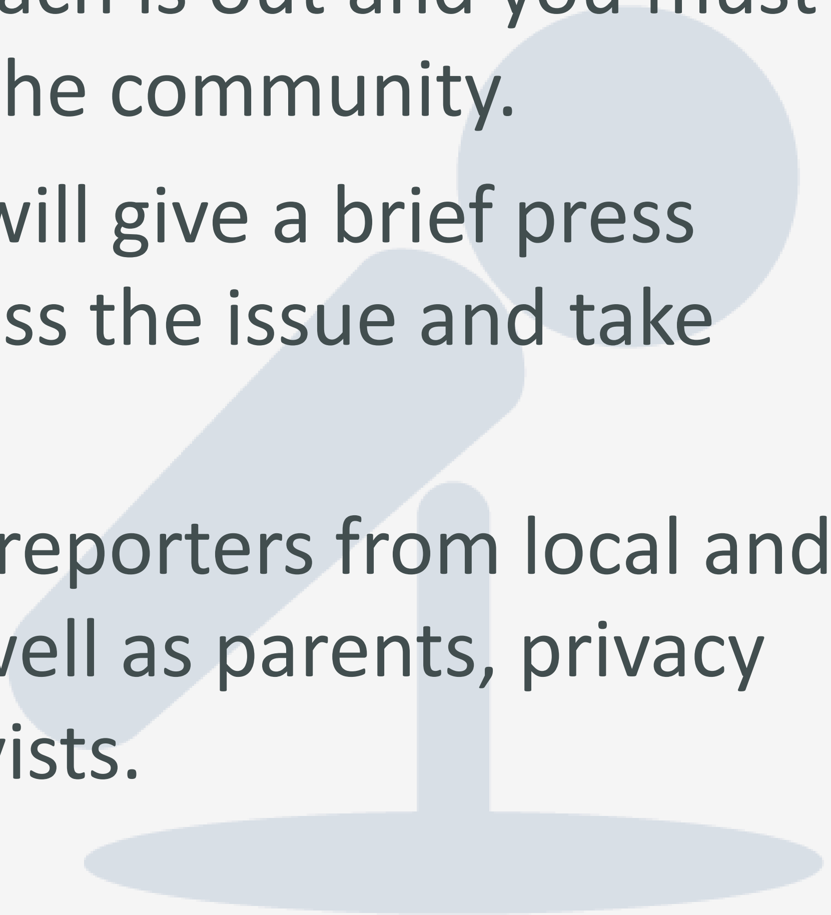
Scenario Update



- The data the students accessed contain personal information for 600 students and 32 employees.
- Some of the staff’s personal data have been published to the students’ Facebook pages.
- News of the breach has leaked out. You are receiving calls from parents asking if their child’s data were accessed and their grades changed.

Press Conference

- The news of the breach is out and you must brief the press and the community.
- Your spokesperson will give a brief press conference to address the issue and take questions.
- In the audience are reporters from local and national media, as well as parents, privacy advocates, and activists.



Password District Data Breach Exercise

10 Minutes

Where Are We?

- How did it go?
- Was your message received well?

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?

Password District Data Breach Exercise

10 Minutes

Unveil 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?

Ps! Don’t Forget to Report

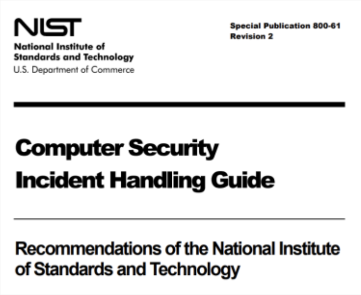
- Lots of people have never ever reported incidents to the federal govt. It’s the law to do so. Data breaches involving financial PII, in particular, have to be reported. This is where you go to do so: https://www.cisa.gov/forms/report at least through October of 2024.

Resources

- NIST's Computer Security Incident Handling Guide | PDF

- CISA Tabletop Exercise Packages: Tools for stakeholders to conduct planning exercises on a wide range of threat scenarios | Website

- KnowBe4's Ransomware Hostage Rescue Check List |PDF



NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 800-61
Revision 2

Computer Security
Incident Handling Guide

Recommendations of the National Institute of Standards and Technology

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

KnowBe4
Human error. Conquered.

Ransomware Hostage Rescue Checklist

What You Need to Know to Prepare and Recover from a Ransomware Attack