CYBERSECURITY TIPS AND TOOLS

CRISIS COMMUNICATION DURING A CYBERSECURITY INCIDENT

Frosty Walker
Chief Information Security Officer
Texas Education Agency
Frosty.Walker@tea.texas.gov
(512) 463-5095
The Data Security Advisory Committee (DSAC) provides guidance to the Texas education communities, maximizing collaboration and communication regarding information security issues and resources which can be utilized within the educational communities served.

The DSAC is currently comprised of representatives from school districts, ESCs, TEA and the private sector.
Cybersecurity Tips and Tools
Crisis Communication

Clear, crisp, consistent, and constant communication is critical and calming.
Communications to Consider

- Alert Notifications
- Issue Investigation – Internal
- Application not available Notifications - External
- Findings Communications – Internal
- Remediation Communications - Internal
- Third Party Communications
- Leadership Communications – Internal
- Media Communications
- Breach Notification
Alert Notification

• Developers, Web Teams--who should they contact when they see anomalies?

• Internal users--who should they contact when they see anomalies?

• External users--who should they contact when they see anomalies?
Issue Investigation - Internal

Security Team
Operations Team
Development Team
Leadership
• Application not available Notifications - External
What was found?

Examples

- SQL injection vulnerability
- Improper permissions on a file or directory, etc.

Resulting in

Examples

- Extraction of data
- Potential unauthorized exposure
Remediation Communications - Internal

Findings
How it can be resolved?
Effort to resolve

Leadership
Third Party Communications

Contact Information
Permission to run Vulnerability Scan
Remedy timeframe

All of this information should be in your contract information.
Sec. 521.053. NOTIFICATION REQUIRED FOLLOWING BREACH OF SECURITY OF COMPUTERIZED DATA. (a) In this section, "breach of system security" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by a person, including data that is encrypted if the person accessing the data has the key required to decrypt the data. Good faith acquisition of sensitive personal information by an employee or agent of the person for the purposes of the person is not a breach of system security unless the person uses or discloses the sensitive personal information in an unauthorized manner.

If the individual whose sensitive personal information was or is reasonably believed to have been acquired by an unauthorized person is a resident of a state that requires a person described by Subsection (b) to provide notice of a breach of system security, the notice of the breach of system security required under Subsection (b) may be provided under that state's law or under Subsection (b).
Leadership Communications – Internal

No Issue Find
Compromise
Potential Exposure-Notification Required
Breach-Notification Required
Media (Public) Communications

A media notice should be developed through your usual public communication processes and should contain the following information:

- Brief description of the details of the event
- Description of the individuals affected in the aggregate
- Description of actions taken by the agency
- Statement as to whether evidence indicates the data may have been misused
- Contact information for questions
Breach Notification to Individuals Impacted

<Date>
<<Title>> <<First Name>> <<Last Name>>
<<Address>>
<<City>>, TX. <<Zip>>
Dear <<Title>> <<Last Name>>:

Your name and certain personal information was [exposure type/description]. This means that information may have been exposed without your authorization or the authorization of [your Entity]. We apologize for any inconvenience this offers you. [Although there is no evidence that any information has been misused, [your Entity] is providing you with free credit monitoring coverage.]

[Describe the incident and what the agency is doing to mitigate the incident.]
We are committed to helping you safeguard your information. [your Entity] is providing you with free credit monitoring and identity theft services for one year. This service includes an insurance policy of up to $[ ] in identity theft coverage, a year of [name of your Entity’s contracted Breach Management Vendor product] coverage, and a full-service identity restoration team to guide you through the recovery process if anyone tries to misuse your information. You must enroll to take advantage of this free service.

We have set up a website that will help you protect your information and will provide you with updates on this matter. You may also call [name of your Entity’s contracted Breach Management Vendor] to ask for help in keeping your data safe. **If you are enrolling a minor child, you will need to call [Breach Management Vendor] to process their enrollment manually. Child enrollment cannot be conducted online.**
We recommend that you also take the following steps to protect your identity:

- Contact one of the national credit reporting agencies below and ask for a fraud alert on your credit report. The agency will alert all other agencies. Remember to renew these fraud alerts every 90 days. The state does not have authority to do this for you, as the credit bureaus must have your permission to set up the alerts.

- The credit reporting agencies do not knowingly maintain credit files on children under the age of 18. You may contact each agency to determine if a child has a file or if the child’s information has been misused:
<table>
<thead>
<tr>
<th>Credit Bureau</th>
<th>Address</th>
<th>Website</th>
<th>Fraud Hotline (toll-free)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Equifax</td>
<td>P.O. Box 740241 Atlanta, GA 30374</td>
<td><a href="http://www.fraudalerts.equifax.com">www.fraudalerts.equifax.com</a></td>
<td>1-877-478-7625</td>
</tr>
<tr>
<td>Experian</td>
<td>P.O. Box 2002 Allen, TX 75013</td>
<td><a href="http://www.experian.com">www.experian.com</a></td>
<td>1-888-397-3742</td>
</tr>
<tr>
<td>TransUnion</td>
<td>P.O. Box 6790 Fullerton, CA 92834</td>
<td><a href="http://www.transunion.com">www.transunion.com</a></td>
<td>1-800-680-7289 Report fraud: <a href="mailto:fvad@transunion.com">fvad@transunion.com</a></td>
</tr>
</tbody>
</table>
• Request a copy of your credit report from the credit reporting agencies and carefully review the reports for any activity that looks suspicious.

• Monitor your [bank account activity / health care records / medical insurance company explanation of benefits] to ensure there are no transactions or other activity that you did not initiate or authorize. Report any suspicious activity in your records to your [bank / health care provider / health insurance company’s privacy officer].

• Report any suspicious activities on your [credit reports or bank account / health care or health insurance records] to your local police or sheriff’s office and file a police report. Keep a copy of this police report in case you need it to clear your personal records.


• [Enroll in free credit monitoring and identity theft services provided by the state. There is no cost to you for the service, but you must enroll. You can enroll online at___or by contacting [Agency’s contracted Breach Management Vendor’s] Customer Care Center toll-free at_____.]
• To enroll your minor child, please call [Agency’s contracted Breach Management Vendor’s] Customer Care Center at to manually enroll them. Child enrollments cannot be conducted online.

• Monitor the website at [your Entity’s contracted Breach Management Vendor’s agency / your Entity’s own site] for periodic updates.

[Your Entity] regrets that this action is necessary. Please be assured that we are committed to helping you protect your credit and identity and in ensuring that your information is safe and secure.

If you have any questions, please call [your Entity] or contact by email at.

Sincerely,
[Authorized signatory]
Questions?