Policy Conference Early Bird

Ransomware and other Cyber Attacks Are you Prepared?

ADAMS AND REESE LLP

The contents of this handout or its associated presentation are intended for general information purposes only. Application of the information reported herein to particular facts or circumstances should be analyzed by legal counsel. Adams and Reese LLP is a registered limited liability partnership. Neither the firm nor the presenters assume liability for the use or interpretation of information contained herein.
Key Contacts:

Adam Griffin
601-832-7650
adam.griffin@arlaw.com

Jim Keith
601-259-8018
jim.keith@arlaw.com
**Approximate Agenda:**

<table>
<thead>
<tr>
<th>Time</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>1:00-1:15</td>
<td>Welcome and introduction, including discussion of known recent attacks on schools and school districts</td>
</tr>
<tr>
<td>1:15-2:00</td>
<td>Preventing ransomware and other common attacks</td>
</tr>
<tr>
<td>2:00-2:15</td>
<td>Break</td>
</tr>
<tr>
<td>2:15-3:00</td>
<td>Incident response planning</td>
</tr>
<tr>
<td>3:00-3:30</td>
<td>Mock Scenarios and discussion</td>
</tr>
<tr>
<td>3:30-3:45</td>
<td>Break</td>
</tr>
<tr>
<td>3:45-4:00</td>
<td>Misdirected payments</td>
</tr>
<tr>
<td>4:00-4:30</td>
<td>Cyber insurance coverage for ransomware and other attacks</td>
</tr>
<tr>
<td>4:30-5:00</td>
<td>Vendor contracts and vendor breach issues</td>
</tr>
</tbody>
</table>
Preventing Ransomware and Other Common Attacks

Some things you can do:
- Air-gapped backups
- Multiple copies of data
- Security software
- Update software
- Upgrade from Windows 7
- USB drives disabled
- Training
- Training
- Training
- Implement the principle of least privilege
- Plan
- Practice
Incident Response Planning

- Identification
- Preliminary investigation
- Stop it
- Initial notifications
  - Counsel
  - Insurance
  - Law enforcement
- Restoration
- Investigation and collection/preservation of information
- Additional notifications
- Prevention and remediation
Scenarios

Scenario #1
Monday morning, Coach Smith comes to the technology coordinator to say he was working hard over the weekend on lesson plans on his district-owned computer and clicked a link in an email that made a message appear saying he needed to pay some bitcoin to unlock the files on his computer. He called his nephew who had been talking about bitcoin at Thanksgiving, and got his nephew to buy some bitcoin to pay the ransom. He paid the ransom and now his computer seems to be working fine.

1. Should the technology coordinator investigate further, or move on to the other issues she is facing today?
2. What should happen to Coach Smith?

Scenario #2
On a Sunday night, one of the organization’s network intrusion detection sensors alerts on unusual network activity involving large file transfers. The network administrator reviews the alerts: it appears that thousands of .ZIP files are being copied from inside the District’s network to outside it. The network administrator contacts the technology coordinator to investigate the activity further. They are unable to see what the .ZIP files hold because their contents are encrypted.

1. Is this likely a data breach?
2. Who should be alerted first?

Scenario #3
The day before state testing begins, the first person in to the district office notices her computer will not work and appears to have been subjected to a ransomware attack. The attack quickly spreads across the entire district before it can be stopped. Virtually every computer and server is infected. The phone system is also affected. The District has to shut down for the day, cancel all classes, and turn away any students who try to come to school. The attackers only want $10,000 in bitcoin to provide the password that they promise will decrypt all of the files and restore everything back to functionality.

1. Do you pay the ransom?
2. Do you tell anyone you paid the ransom?
Scenario #4
The District’s business officer notices some strange activity on his email account. He notifies the technology coordinator, who determines the account has likely been compromised, but he is unsure of the scope of what may have been viewed by someone else.

1. Should the District notify its cyber insurance carrier?
2. What are the potential ramifications of not providing that notification?