Attack Summary : Cyber Attack Takes Weather Channel Offline

[Records Exposed: N/A]

[Industry: Media]

[Type of Attack: Ransomware]

Exploited Vulnerability: On Thursday, April 18, 2019, The Weather Channel live broadcast went offline for about an hour according to The Wall Street Journal, which the company later confirmed in a Twitter statement was due to a 'malicious software attack.' The FBI subsequently started an investigation into the ransomware attack that shut down the Weather Channel's live program, which forced the cable channel to resort to a taped program.

Remedy Actions Taken and Recommended Future Mitigation Strategy:: Jason Glassberg, the cofounder of the security firm Casaba Security, told Business Insider what to do if you accidentally fall victim to a ransomware attack:

Alert law enforcement. While they might not be able to help you much, they should still be made aware of the crime.

Turn off your infected computer and disconnect it from the network it is on. An infected computer can potentially take down other computers sharing the same network.

Back up the data on a separate hard drive so you can at least recover the data you lost from the point of the last backup. While the malicious software itself can be removed, getting your data back is a whole different story.

Finally, you have to decide whether or not you are going to pay the ransom, which is a highly debated topic. "We have seen many scenarios where even if the user pays, they don't get the recovery keys. So it's one of the reasons we tell our customers that paying the ransom is not the best course of action," says Steve Grobman, the chief technology officer of Intel's Security Group.

"For starters, paying the ransom may not result in you getting your keys back. And you are also providing additional incentives for the criminal element to continue to build ransomware and make it more effective and help it become an even bigger problem in the future."

Reference:

https://www.deloitte.com/global/en/services/risk-advisory/perspectives/cybersecurity-threats-and-incidents-