JBS Summarization

Phishing campaigns are on the rise. Companies and organizations should remain vigilant in protecting their infrastructure from cyber-attacks. JBS failed to protect their infrastructure from cyber-attacks. Ransomware accounted for 20% of all cyber-attacks. The most common ransomware attack is phishing. Phishing attacks in the U.S. account for 47% of cyber-attacks.

A Russian based group by the name of REvil held several American companies’ hostage by demanding ransomware in releasing the company’s data. JBS failed to protect their infrastructure from cyber-attacks. Ransomware accounted for 20% of all cyber-attacks. The most common ransomware attack is phishing. Attacks on US organization’s account for 47% of cyber attacks

In the report, the findings included the following:

* REvil monetized access to victim networks and sold that access to other REvil affiliates.
* Before encrypting victim organization networks, REvil used double extortion methods to first steal sensitive data from victims and then publish that data on REvil’s public blog.
* REvil harassed victim company employees via email and telephone in an attempt to coerce the companies into paying ransoms

CrowdStrike Summarization:

On July 19, 2020, a systems administrator at CrowdStrike caused the largest IT outage in American history. The system administrator performed a windows update which was neither validated, verified or followed the change management approval process. There was a security flaw discover in the Falcon sensor version 7.11 and above which caused the system to crash

The outage caused damage to many organizations to include Delta Airlines and financial institutions.

The moral to the story is always validate before you implement any software updates. Also follow the change management process and review any baseline changes before implementing any updates.

Reference:

*The Latest Ransomware Statistics (Updated January 2025) | AAG IT Support*.

https://aag-it.com/the-latest-ransomware-statistics/. Accessed 2 Apr. 2025.

*America’s Data Held Hostage: Case Studies in Ransomware Attacks on American Companies*. United States Senate, Mar. 2022,

p. 44, <https://www.hsgac.senate.gov/wp-content/uploads/imo/media/doc/Americas%20Data%20Held%20Hostage.pdf>.

“CrowdStrike Outage Explained: What Caused It and What’s next.” *WhatIs*, https://www.techtarget.com/whatis/feature/Explaining-the-largest-IT-outage-in-history-and-whats-next. Accessed 2 Apr. 2025.