The CrowdStrike Incident: A Guide for ACEA Members

In today's digital age, cybersecurity is crucial for industries worldwide, including those in construction and engineering. On Friday, July 19th, a widespread incident involving CrowdStrike, an Austin-based cybersecurity company, highlighted the significance and potential pitfalls of cybersecurity software. Let's delve into the fundamental aspects of CrowdStrike and the recent events to better understand its impact.

CrowdStrike is a cloud-based cybersecurity platform founded in 2011. It provides advanced security solutions to prevent hacks and data breaches for various industries, from airlines and hospitals to retailers and financial institutions. CrowdStrike's software, particularly its flagship Falcon platform, offers multiple security services, including antivirus capabilities, endpoint protection, threat detection, and real-time monitoring.

On July 19th, a global disruption occurred due to a flawed update in CrowdStrike's Falcon Sensor software. This update caused widespread outages, leaving many workers greeted with blue computer screens and no access to their systems. The pain experienced by companies was substantial. Airports saw long lines and frustrated travelers as flights were grounded. Hospitals faced delays in critical medical procedures, putting patient care at risk. Media outlets struggled to broadcast, and businesses across various industries experienced significant downtime. The financial implications were severe, with lost revenue and increased costs for emergency IT support.

CrowdStrike's software updates are typically automatic and silent, designed to keep systems secure without user intervention. However, a defect in this update caused Windows-based systems to crash, resulting in what's known as the "blue screen of death." The issue was not due to a cyberattack but a flawed software update. CrowdStrike quickly identified the problem and began working on a fix. Some systems automatically installed the fix, while others required manual intervention from IT specialists. Recovery efforts depended on the resources and size of each organization's IT team, with smaller companies potentially facing longer downtimes.

This incident underscores the critical role of cybersecurity software and the vulnerabilities inherent in relying on a single provider. CrowdStrike's reputation for handling major security issues, such as the Sony Pictures hack in 2014 and the Democratic National Committee hack in 2016, demonstrates its expertise. However, the recent outage shows that even the most advanced systems can experience failures, emphasizing the need for diversified cybersecurity strategies.

For contractors and engineers, the takeaway is clear: cybersecurity is vital, and its integration into your operations must be robust and adaptable. Evaluate your cybersecurity framework continuously. Ensure your systems are updated, have contingency plans for potential disruptions, and consider diversifying your cybersecurity providers to mitigate risks.

Creating a business continuity plan for each aspect of your business is crucial. This plan should include strategies for maintaining operations during a cybersecurity incident, such as regular backups, alternative communication methods, and a clear action plan for IT personnel. Ensure all employees are trained on these procedures to minimize downtime and maintain productivity. CrowdStrike's recent outage serves as a reminder of the interconnectedness of our digital world and the importance of maintaining a resilient cybersecurity posture. By staying informed and prepared, you can safeguard your operations against unforeseen disruptions and maintain the integrity of your business.

Josh Wilmoth is President & CEO of Central Texas Technology Solutions (CTTS), a leading IT services company. CTTS assists businesses by proactively addressing digital threats and providing a plan to safeguard business processes.