[$6.872 BILLION]

How the largest cyber loss in U.S. history was forecast— *10 months earlier*

Update since UnitedHealth Group Feb 2024 Breach

ArxNimbus

arxnimbus.com

HOW IT HAPPENED

- Change Healthcare, acquired by UnitedHealth Group in Oct 2022, server was breached by an affiliate of the ALPHV ransomware gang due to a lack of multi-factor authentication (MFA). A substantial portion of the U.S. population's personal and protected health information (PHI) was compromised.

- UnitedHealth Group paid a $22 million ransom for the 6 terabytes of Change Healthcare data ALPHV claimed to have. There were also reports of a secondary attempt to extort the company by the same threat actors under a different ransomware group name, leading to another potential ransom payment.

WHERE WE'RE AT

- In the 2024 Senate Financial Committee hearing, Andrew Witty, CEO at UnitedHeath Group, told lawmakers that former and current U.S. military personnel among those likely impacted.

- Without minimum cybersecurity standards from the Department of Health and Human Services (HHS), lawmakers expressed concern over the possibility of more attacks on health care providers.

- Individuals whose data was stolen are still being notified and directed on what actions to take. HHS is emphasizing the importance of HIPAA breach notifications and has provided guidance and flexibility to healthcare providers affected by the incident.

WOULD/COULDA/SHOULDA

- **What if this had been predicted within 8% – some 310 days earlier?**

- According to the Healthcare Financial Management Association, auditor financial analysis of the losses now shows an expected total loss of $6.87B from this breach.

- On 4/17/23, an ArxNimbus risk profile was completed on United Healthcare as part of a cyber insurance analysis. The risk profile projected a loss exposure of **$7.87B.** This was determined through a classical **actuarial analysis**. The results are in compliance with NIST frameworks, and the process uses Thrivaca™ technology and employs a NIST-reviewed and approved patented methodology.

Learn more about these Thrivaca™ results

WHY YOU SHOULD CARE

- Who will pay for this breach? Ultimately, YOU, in the form of increased premiums and deductibles.

- **Multi-Factor Authentication (MFA) is cited as the culprit. It is one of the easiest, most basic risk management steps anyone** (individuals or organizations) can take, yet they didn't…until it was too late.

- Many have sought to claim that cybersecurity risk cannot be properly quantified or forecasted. This is a myth. Throughout history, every risk known to society has become understood—and therefore insurable—through actuarial methods that properly show the impact of the event and—more difficult to attain—the probability of it happening.

WHAT SHOULD YOU DO

- **Follow up on Breach Notifications**: If you are notified, take the steps recommended in the notification, such as changing passwords, monitoring accounts, and following any specific advice provided.

- **Proactive cybersecurity measures:** Any organization, any industry, any size is a target and not immune. Implement multi-layered security protocols, including regular updates and patch management, robust firewalls, encryption, and strong access controls. *Regularly audit these measures to ensure they are effective.*
- Since breaches often involve third-party vendors (as in the case of Change Healthcare), it is critical to evaluate and monitor the cybersecurity posture of all partners and suppliers. This includes ensuring they adhere to industry standards and regulatory requirements.

It’s time for us to go beyond technical considerations of cybersecurity, and add the business perspective. Doing so will allow us all to properly step up to understand the magnitude of the issue, and fund the protections that allow us all to get to a safer place. Advanced Actuarial Cyber Risk Quantification: It’s not magic, it’s math! #ACRQ

Follow us for breach news impacts

ArxNimbus

Eradicate cyber risk.

Source: https://cyberscoop.com/change-healthcare-attack-stolen-data-ransom-andrew-witty-unitedhealth/