ROUND TABLE:

INFLUENCE AND IMPACT OF CYBER SECURITY ON COMPANIES AND EMPLOYEE BEHAVIOR

AGENDA

Introduction

Overview

Talking Points/ Open Discussion

OPEN DIALOGUE

KEY TALKING POINTS

1. Increased Investment in Security Infrastructure
2. Operational Changes
3. Impact on Business Operations
4. Reputation and Trust
5. Legal and Financial Consequences
6. Innovation and Digital Transformation
7. Talent and Workforce Development
8. Globalization and Supply Chain Risks
9. 10 Best Practices

POLL

Question 1:

How many of you have seen a phishing email (work or personal)?

Question 2:

What action did you take when receiving a phishing email? Did you click on it “accidentally”?

INCREASED INVESTMENT IN SECURITY INFRASTRUCTURE

April 26th -Moody's: Hospitals bulk up cybersecurity teams, budgets

Healthcare cybersecurity budgets and teams have grown significantly since 2019 as threats become more pronounced, according to an April survey report from Moody's Investors Service. On average, respondents reported cybersecurity teams jumped headcount by 30% from 2019 to 2022 and cybersecurity spending hit 7% of the total IT budget last year, up from 5% in 2019. Eighty-one percent of healthcare companies said cybersecurity was a line item in their budgets, which is higher than the 74% average across all industries. Becker's Health IT

April 30th -Biden cybersecurity plan for hospitals entails carrots first, then sticks

The Biden administration's plan to improve cybersecurity at hospitals starts off with incentives, but eventually hospitals will face penalties for not adopting measures to protect patient data, HHS Deputy Secretary Andrea Palm. Stat+

OPERATIONAL CHANGES

Question 1:

How many of you are aware of operational changes because of cyber security?

Question 2:

Any one here has or is currently participating on an implementation group to improve “best practices”?

IN THE NEWS

April 23rd -FTC finalizes changes to healthcare breach reporting rule

The FTC finalized a rule Friday that aims to tighten the reins on digital health apps sharing consumers' sensitive medical data with tech companies. The agency issued a final version of its revised Health Breach Notification Rule to underscore the rule's applicability to health apps in a bid to protect consumers' data privacy and provide more transparency about how companies collect their health information.

May 2nd -Change Healthcare cyberattack was due to lack of multifactor authentication, CEO says

The Change Healthcare cyberattack that disrupted healthcare systems nationwide earlier this year started when hackers entered a server that lacked a basic form of security: multifactor authentication. UnitedHealth CEO Andrew Witty said Wednesday in a U.S. Senate hearing that his company, which owns Change Healthcare, is still trying to understand why the server did not have the additional protection. His admission did not sit well with Senate Finance Committee members who spent more than two hours questioning the CEO about the attack and broader healthcare issues. "This hack could have been stopped with cybersecurity 101," Oregon Democratic Sen. Ron Wyden told Witty.

IMPACT ON BUSINESS OPERATIONS

Question 1:

How many of you have experienced downtime because of a cyber security issue?

IN THE NEWS

May 9th -Cyberattack disrupts Ascension

A cyberattack has disrupted “clinical operations” at Ascension, forcing it to take steps to minimize any impact to patient care, an Ascension spokesperson said Wednesday. “There has been a disruption to clinical operations, and we continue to assess the impact and duration of the disruption,” said the statement from Ascension, which has medical centers in Waco and Austin. Ascension recommended that its healthcare clients temporarily cut off network connections to Ascension as the incident is being addressed. CNN

May 10th -Ascension expects IT outages “for some time”

A cybersecurity incident has left 140-hospital Ascension with its EHR disabled, some appointments and surgeries postponed, and the expectation that the 19-state health system will operate on downtime procedures "for some time." Ascension said its EHR, MyChart, and some phone systems are unavailable, with employees and operations resorting to downtime procedures. Certain non-emergency elective procedures, tests and appointments have been postponed. Patients are advised to bring notes detailing their symptoms and a list of their medications, including prescription numbers or containers, so their care team can call in prescriptions to pharmacies. Becker’s Health IT

REPUTATION AND TRUST

Question 1:

How many of you when you have a bad experience complete a survey detailing why you had a bad experience?

Question 2:

If you were at a nice restaurant and had an issue (i.e. poor service, bill incorrect), did you complain and/or never go back?

IN THE NEWS

July 31st -Change Healthcare begins breach notifications

UnitedHealth Group's Change Healthcare has begun sending out letters to individuals affected by its Feb. 21 ransomware attack. "On July 29, 2024, Change Healthcare began mailing written notices to individuals affected by the incident," an update on UnitedHealthcare's website reads. "Change Healthcare is committed to notifying potentially impacted individuals as quickly as possible on a rolling basis, given the volume and complexity of the data involved." Change Healthcare also reported the ransomware attack to HHS' data breach portal. Change Healthcare said on April 22 that an initial sampling of the breached data showed the attack compromised protected health information and personally identifiable information from a large swath of the country. Becker's Health IT

April 23rd -UnitedHealth: Hackers stole health data on "substantial portion of people in America"

UnitedHealth Group has confirmed that a ransomware attack on its health tech subsidiary Change Healthcare resulted in a huge theft of Americans' private healthcare data. UnitedHealth said in a statement on Monday that a ransomware gang took files containing personal data and protected health information that it says may "cover a substantial proportion of people in America." The health insurance giant did not say how many Americans are affected but said the data review was "likely to take several months" before the company would begin notifying individuals that their information was stolen in the cyberattack. TechCrunch

LEGAL AND FINANCIAL CONSEQUENCES

- Fines and Penalties
- Insurance Costs

July31st -Average healthcare data breach costs hit $9.77 million

Healthcare saw the most expensive data breaches across all industries, with average breach costs reaching $9.77 million, a Tuesday report from IBM found. According to the report, organizations in the healthcare, financial services, industrial, technology and energy sectors faced the highest breach costs across all industries. Breach costs have increased by 10% from 2023. Becker's Health IT

INNOVATION AND DIGITAL TRANSFORMATION

- Balancing Innovation with security
- Using Cybersecurity as a competitive advantage

TALENT AND WORKFORCE DEVELOPMENT

Question 1:

Based on the national average what do you think the average spend per employee for cybersecurity is?

TALENT AND WORKFORCE DEVELOPMENT

- National Average Spent on training employees
  - Small to Mid-Sized businesses $500 - $2,000
  - Large Enterprises $2,000 - $4,000
- Factors that affect the workforce costs
  - Industry
  - Training Format
  - Certifications
  - Frequency

GLOBALIZATION AND SUPPLY CHAIN RISKS

- How many 3rd Party vendors/partners use your data?
- For companies who cross borders state/country, are there addition risks?

IN THE NEWS

April 26th -Kaiser reports data breach affecting 13.4 million people

A data breach at Kaiser Foundation Health Plan affected the information of more than 13 million individuals, according to a report filed with the federal government. The not-for-profit insurance company, part of Oakland, California-based Kaiser Permanente, on April 12 notified the Health and Human Services Department of the breach. The report was made public Thursday. The incident represents the largest health-related data violation, in terms of number of individuals affected, published to the OCR breach portal so far this year. It is the second largest since healthcare organizations began reporting this information in 2010, behind Anthem's breach in 2015. Modern Health Care

July 9th -Healthcare groups say cyber rule should explicitly name insurers, vendors

Healthcare and hospital groups say a federal cybersecurity reporting proposal should explicitly include insurers and third-party vendors, citing the impact of the major cyberattack against medical claims clearinghouse Change Healthcare. The proposed rule, released by the Cybersecurity and Infrastructure Security Agency this spring, would require companies broadly in critical infrastructure industries to report cyber incidents within 72 hours of discovery and document ransom payments within 24 hours. CISA decided not to include sector-specific reporting criteria for insurance companies, health IT providers and labs or diagnostics facilities. But the American Hospital Association argued the exclusion doesn't make sense, as disruption to a single company could ripple across the entire industry. Healthcare Dive

10 BEST PRACTICES PUBLISHED BY CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA)

1. Implement Multi-Factor Authentication (MFA)
2. Patch and update software regularly
3. Use Strong, unique passwords
4. Limit user privileges
5. Implement Network Segmentation
6. Backup Data Regularly
7. Secure and monitor Remote Access
8. Educate and Train employees
9. Implement end Point Detection and Response (EDR)
10. Develop and Test an Incident Response Plan

CREDITS

- News Articles: Executive News Briefing published by Baylor Scott & White Health Communication
- "How has cybersecurity affected companies" Cyber security has profoundly affected companies in several key areas transforming how they operate, protect data, and manage risks. *ChatGPT*, Open AI, 12 Aug. 2024.
- "What are the top 10 best practices for cybersecurity by CISA" CISA provides comprehensive guidance on best practices to enhance an organization's cybersecurity posture. *ChatGPT*, Open AI, 13 Aug. 2024.

THANK YOU

Christopher Kubin, FHFMA

Christopher.kubin@bswhealth.org