CYBERFORCE | Q

PHISHING

Is the leading cause of cyber security incidents and ransomware, threatening patient care and increasing financial risk in healthcare institutions.

This study outlines the issues faced by healthcare organizations due to phishing, and the strategies and actions of CyberForce | Q to protect healthcare organizations and their patients.

Created by CyberForce | Q

54%

OF RANSOMWARE CAUSED BY PHISHING

Phishing is the most common cause of ransomware infection[1]

80%

OF SECURITY INCIDENTS ARE A RESULT OF PHISHING

Phishing accounts for over 80% of reported security incidents[2]

IMPACT OF A BREACH

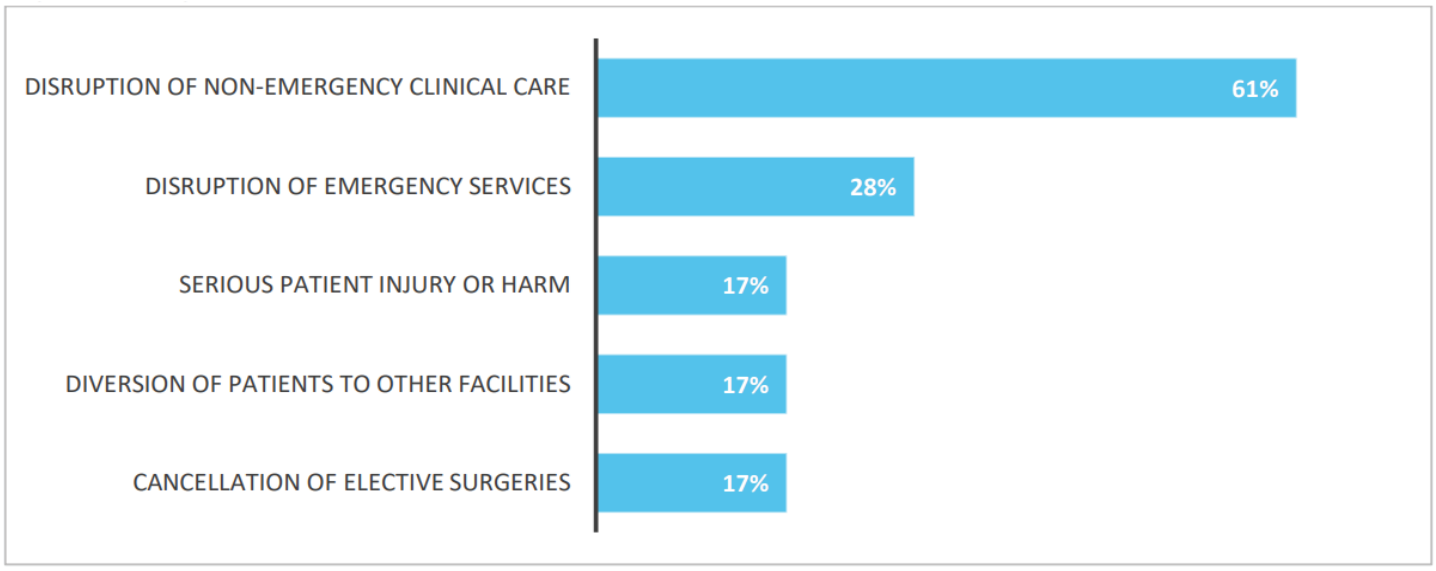
One prominent example of the dangers of cyber attacks is Scripps Health. Scripps was breached in 2021, with the information of **over 147,000 individuals** being exposed[3].

From this attack, the organization incurred costs of **almost $113 million**[3]. In addition, patient care was compromised as patients were diverted or their care was postponed[4]. As a result of the breach, Scripps is facing multiple **class action lawsuits** for their negligence of taking the appropriate steps to prevent the cyber attack[5].

Ransomware attacks can even lead to deaths. There is a lawsuit against Springhill Medical Center in Alabama regarding a **baby's death** from disabled IT systems, making critical data about the heart rate unavailable[6]. Another example is Dusseldorf University Clinic, where a ransomware attack led to a woman being redirected to another hospital **and dying during the transfer**[7].

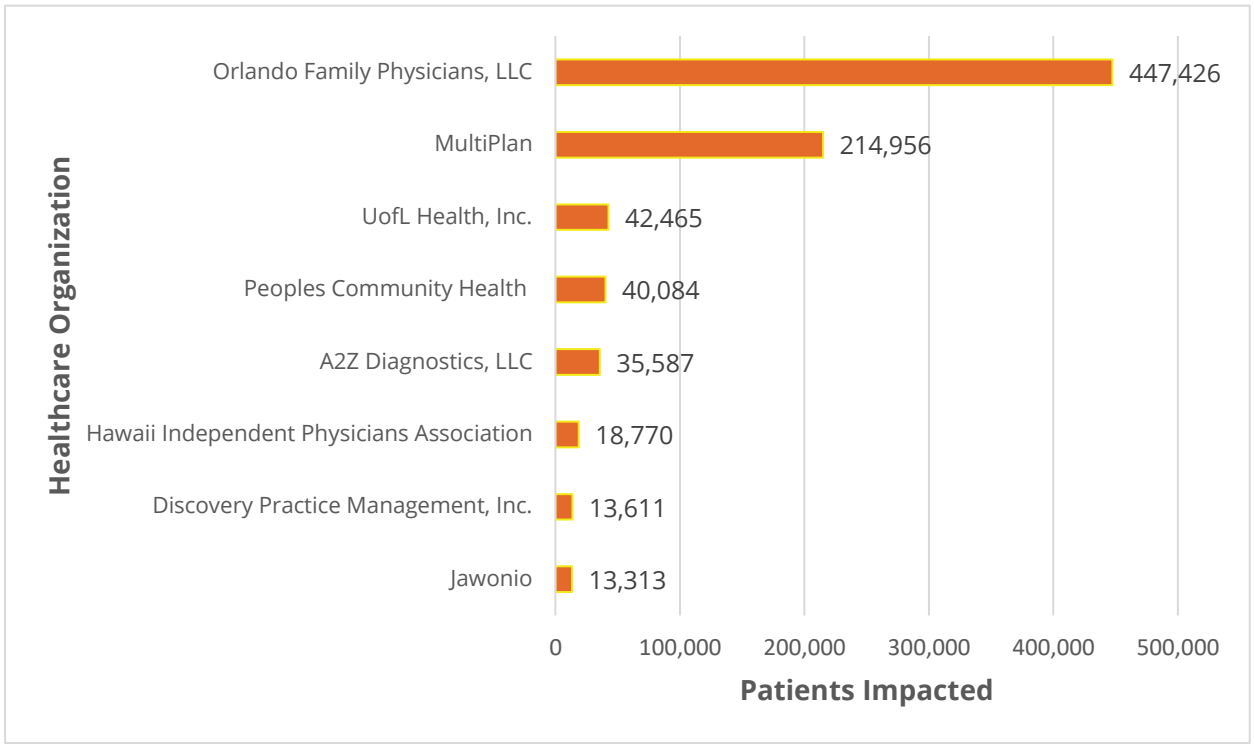
PATIENT CARE DISRUPTION

For healthcare organizations, patient care is one of the top priorities. Cyber attacks jeopardize the security of patient information and can also create significant issues to patient safety. In a study by the Healthcare Information and Management Systems Society (HIMSS), organizations who were victim to a cyber attack observed several issues related to providing patient care[8]. The table below shows the percentage of organizations that experienced the related disruption to their patient care[8].



HIMSS.org

Unfortunately, these disruptions to patient care and patient data, are becoming more and more common with the rise of cyber attacks. Below is a list of several breaches that took place in June 2021 and July 2021, with the amount of patients impacted by these breaches, as reported by HIPAA[9].



FILTERING THE NOISE

CyberForce|Q provides a unique collective Health Security Operations Center (HSOC), that allows participants to share tactical information between peer health organizations. Between just July and August 2021, the HSOC investigated a total of 8,616 cases.

Of these cases, the HSOC filtered out nearly 97% of phishing noise for the participants, saving time, money, and resources for these organizations. This allows the cybersecurity and IT teams of these organizations to focus their efforts on using their experience and skill to innovate in their department, conduct in-depth investigations, and continuously find ways to protect patient data.

97%
Phishing Noise Filtered Out

8,616
Phishing Cases (July-August 2021)

0
Breaches

HEALTHCARE EXAMPLE

Below is a real event that occurred in a participant's environment on August 24, 2021. An employee observed and reported a phishing attempt that the CyberForce|Q team analyzed and responded to in order to avert a breach.

9:06PM EST
Employee reports a suspicious email.

9:08PM EST
CyberForce|Q receives case in incident management technology. An automated playbook runs, checking the e-mail. It finds the email suspicious and sets priority to "High."

9:09PM EST
Case assigned to CyberForce|Q analyst.

9:10PM EST
Investigation begins. The email prompts users to download an attached invoice. Once opened, the invoice connects to a malicious URL.

9:12PM EST
Email categorized as phishing and escalated to CyberForce|Q Senior Analyst for further investigation.

9:13PM EST
Senior Analyst finds malicious email was received by 10 users. Analyst takes action to remove emails and block traffic to the malicious URL and IP address.

10:33PM EST
Investigation concludes. The organization's team is informed of phishing incident and breach is averted.

Due to the partnership between the participant and CyberForce|Q, the phishing attempt was able to be discovered and a potential breach was averted, in a short period of time. The event that took place was reported after business hours, but as a 24x7x365 service, CyberForce|Q was able to protect the organization's environment against the phishing incident. In addition, the participants's processes are integrated, to provide a flow of information to the organization, whenever an incident occurs. With these actions, CyberForce|Q assists with continuing to provide world-class healthcare to the participant's patients, and avoid becoming another unfortunate news story like Scripps or even worse, causing the death of a patient like Springhill or Dusseldorf.

Incident Identified and Breach Averted in Less Than 1.5 Hours

With 24x7x365 Monitoring, Incident Response was Immediate

Participant's Systems Integrated with Investigation Process

REFERENCES

(1) Felix Richter. Phishing the Most Common Cause of Ransom Attacks. Statista.com. https://www.statista.com/chart/25247/most-common-causes-of-ransomware-attacks/. Published July 6, 2021.

(2) Chuck Brooks. Alarming Cybersecurity Stats: What You Need To Know For 2021. Forbes.com. https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html. Published March 2, 2021.

(3) Marianne Kolbasuk McGee. Scripps Health Reports Financial Toll of Ransomware Attack. healthcareinfosecurity.com. https://www.healthcareinfosecurity.com/scripps-health-reports-financial-toll-ransomware-attack-a-17288. Published August 13, 2021.

(4) Marianne Kolbasuk McGee. Security Incident Leads Scripps Health to Postpone Care. healthcareinfosecurity.com. https://www.healthcareinfosecurity.com/security-incident-leads-scripps-health-to-postpone-care-a-16514. Published May 3, 2021.

(5) Scripps Health Facing Multiple Class Action Lawsuits over Ransomware Attack. HIPAAJournal.com. https://www.hipaajournal.com/scripps-health-facing-multiple-class-action-lawsuits-over-ransomware-attack/. Published June 24, 2021.

(6) Hospital ransomware attack led to infant's death, lawsuit alleges. Healthcareitnews.com. https://www.healthcareitnews.com/news/hospital-ransomware-attack-led-infants-death-lawsuit-alleges. Published October 1, 2021.

(7) Police launch homicide inquiry after German hospital hack. BBC.com https://www.bbc.com/news/technology-54204356. Published September 18, 2020.

(8) 2020 HIMSS Cybersecurity Survey. HIMSS.org. https://www.himss.org/sites/hde/files/media/file/2020/11/16/2020_himss_cybersecurity_survey_final.pdf. Published 2020.

(9) June 2021 and July 2021 Healthcare Data Breach Reports. HIPAAJournal.com