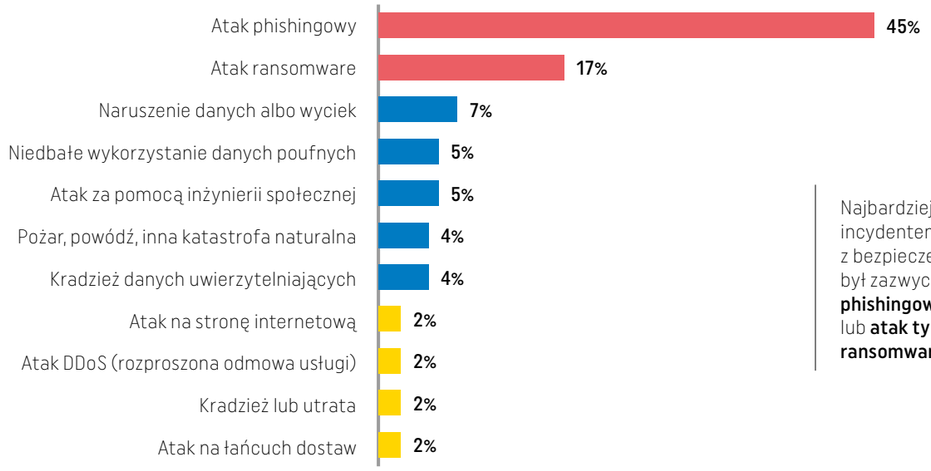
STAN CYBERBEZPIECZEŃSTWA 2022

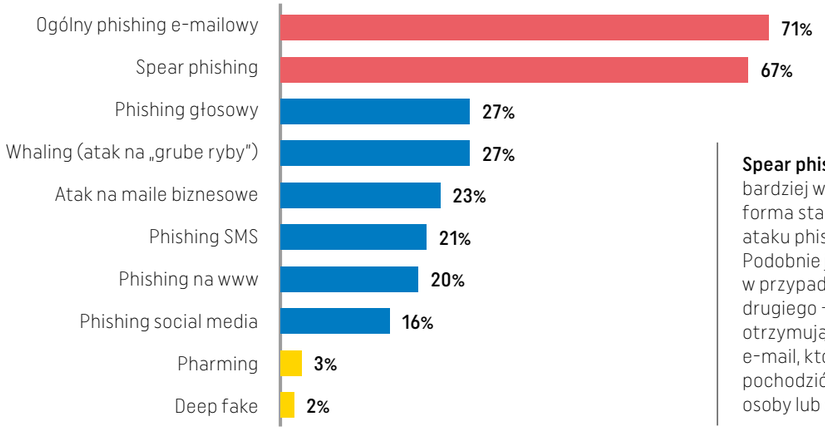
Z nowego, corocznego raportu HIMSS Healthcare Cybersecurity wynika, że chociaż COVID-19 zwiększył świadomość w zakresie znaczenia bezpieczeństwa danych w ochronie zdrowia, nadal występują duże niedociągnięcia. Wszyscy respondenci zetknęli się z incydentami bezpieczeństwa, z czego 32% to poważne naruszenia, a 12% – krytyczne. Raport został opracowany na podstawie opinii 167 specjalistów ds. bezpieczeństwa cybernetycznego w ochronie zdrowia.

● Z JAKIEGO RODZAJU NIEBEZPIECZNYM INCYDENTEM BEZPIECZEŃSTWA DANYCH SPOTKAŁEŚ/AŚ SIĘ W OKRESIE OSTATNICH 12 MIESIĘCY?



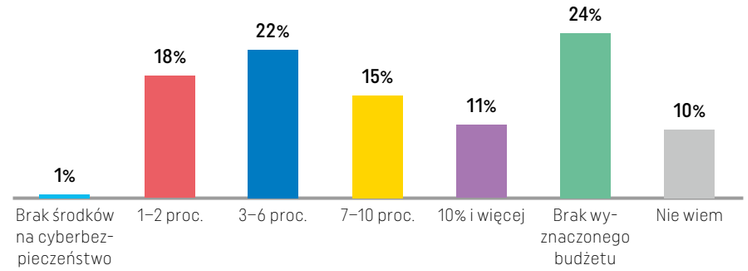
Najbardziej znaczącym incydentem związanym z bezpieczeństwem był zazwyczaj **atak phishingowy (45%)** lub **atak typu ransomware (17%)**.

● W PRZYPADKU PHISHINGU, JAKI BYŁ TO DOKŁADNIE RODZAJ ATAKU?



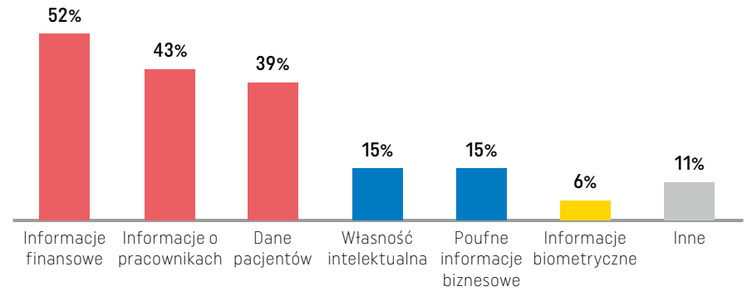
Spear phishing to bardziej wyrafinowana forma standardowego ataku phishingowego. Podobnie jak w przypadku tego drugiego – ofiary otrzymują wiadomość e-mail, która wydaje się pochodzić od zaufanej osoby lub organizacji.

● JAKI PROCENT BUDŻETU ORGANIZACJI PRZEZNACZA SIĘ NA CYBERBEZPIECZEŃSTWO?

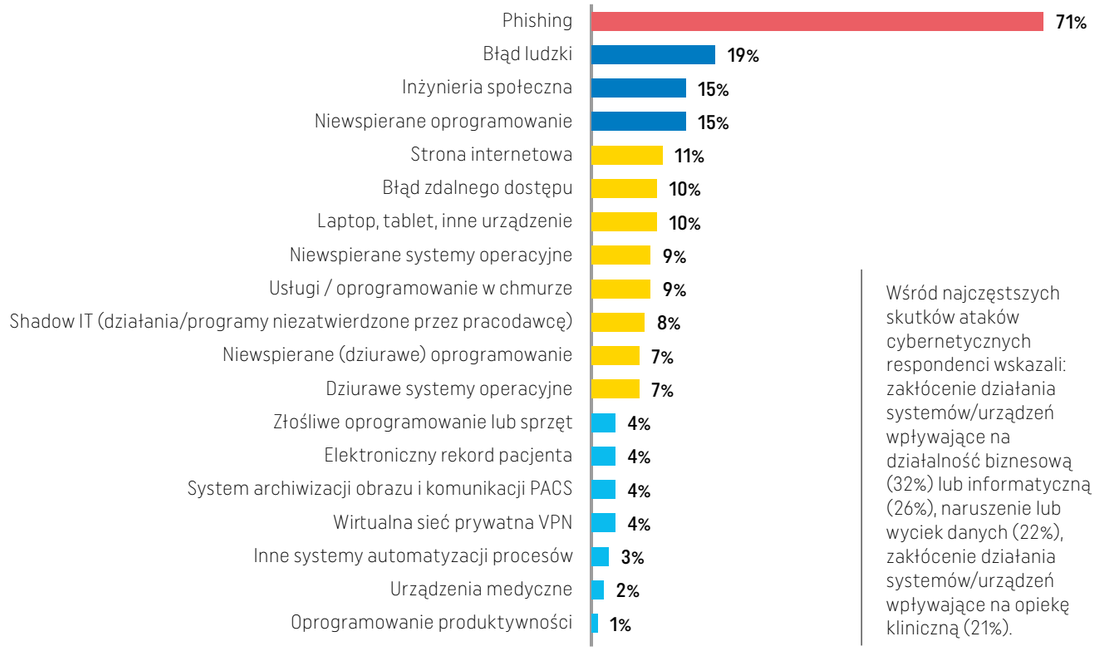


Dla 47% badanych największych wyzwaniem jest brak środków na cyberbezpieczeństwo, z kolei dla 43% – niestosowanie się personelu do procedur i polityk bezpieczeństwa.

● CO BYŁO CELEM W INCYDENTACH NARUSZENIA BEZPIECZEŃSTWA DANYCH?



● JAKI ELEMENT BYŁ ŹRÓDŁEM POWAŻNEGO INCYDENTU BEZPIECZEŃSTWA DANYCH?



Wśród najczęstszych skutków ataków cybernetycznych respondenci wskazali: zakłócenie działania systemów/urządzeń wpływające na działalność biznesową (32%) lub informatyczną (26%), naruszenie lub wyciek danych (22%), zakłócenie działania systemów/urządzeń wpływające na opiekę kliniczną (21%).

Źródło: HIMSS Healthcare Cybersecurity Survey 2021