RESEARCH UNCOVERS CYBERSECURITY STATE-OF-PLAY IN UK HEALTHCARE SECTOR

67% OF HEALTHCARE ORGANIZATIONS SUFFERED A CYBERSECURITY INCIDENT IN THE LAST 12 MONTHS

48%
VIRUSES OR MALWARE FROM THIRD-PARTY DEVICES, INCLUDING IOT DEVICES AND USB STICKS

39%
EMPLOYEES SHARING INFORMATION WITH UNAUTHORIZED RECIPIENTS

37%
USERS NOT FOLLOWING PROTOCOL/DATA PROTECTION POLICIES

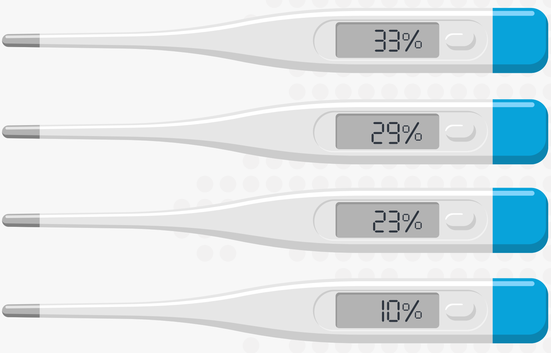
28%
CLICKING ON MALICIOUS LINKS IN EMAILS AND SOCIAL MEDIA

> *Cybersecurity strategies across healthcare organizations need to rapidly evolve to account for new threats against the sector. While many aspects of staying secure come from keeping employees trained to recognize threats, technology should play a key role in helping reduce the risks that come with innovation.*
>
> ALYN HOCKEY, VP PRODUCT MANAGEMENT

24%

WHEN ASKED ABOUT THE PROPORTION OF IT SPEND ALLOCATED FOR CYBERSECURITY PURPOSES, LESS THAN A QUARTER OF RESPONDENTS AGREED THAT BUDGETS WERE AT AN ADEQUATE LEVEL.

WHAT HAS HAD THE GREATEST IMPACT ON IT SPEND AND/OR BOARD LEVEL INVOLVEMENT?



WHERE DO HEALTHCARE ORGANIZATIONS FOCUS THEIR CYBERSECURITY INVESTMENT?

46%
DATABASE SECURITY

44%
DATA LOSS PREVENTION

27%
TRAINING AND EDUCATION

26%
ENDPOINT SECURITY

clearswift
by HelpSystems

Statistics in this infographic come from a survey conducted by research firm Vanson Bourne on behalf of Clearswift in November 2019