

Cybersecurity in the CONNECTED HOSPITAL

Abbott conducted in-depth research among physicians and hospital administrators to understand the cybersecurity challenges our hospital customers face.

WE SURVEYED:



300
Physicians



100
Hospital Administrators

WHAT WE FOUND:



While physicians and administrators see cybersecurity as a priority, the majority of them feel underprepared to combat cyber risks.

BENEFITS OF CONNECTED DEVICES OUTWEIGH THE RISKS



87%

of surveyed physicians



80%

of surveyed hospital administrators

AGREE THAT THE BENEFITS OF CONNECTED MEDICAL TECHNOLOGY OUTWEIGH THE RISKS

PHYSICIANS AND ADMINISTRATORS FEEL UNDERPREPARED ON CYBERSECURITY



75%

of surveyed physicians



62%

of surveyed hospital administrators

FEEL INADEQUATELY TRAINED OR PREPARED TO COMBAT CYBER RISKS.

CYBERSECURITY IS A SHARED RESPONSIBILITY



71%

of surveyed physicians



74%

of surveyed hospital administrators

VIEW CYBERSECURITY AS A SHARED RESPONSIBILITY AMONG HEALTHCARE ECOSYSTEM STAKEHOLDERS.

BROAD SUPPORT FOR INDUSTRY-WIDE STANDARDS



82%

of surveyed physicians



73%

of surveyed hospital administrators

BELIEVE THERE SHOULD BE AN INDUSTRY-WIDE SET OF STANDARDS AND LANGUAGE FOR CONNECTED DEVICE SECURITY.

NEED FOR IMPROVED COMMUNICATION



15%

of surveyed physicians



45%

of surveyed hospital administrators

HAVE SEEN OR READ A MEDICAL DEVICE SECURITY ADVISORY IN THE LAST SIX MONTHS.

WHAT COMES NEXT:

The connected healthcare ecosystem must come together to address the cyber risks that face the entire healthcare industry.



INDUSTRY-WIDE STANDARDS

to ensure cybersecurity protections are built into the earliest phases of medical device development.



INVESTMENT IN INCIDENT RESPONSE PROCESSES

for identifying and responding to vulnerabilities in a timely manner, while supporting safe clinical care.



IMPROVED EDUCATION, FOCUS AND TRAINING

to increase all stakeholders' understanding of cyber risk in the healthcare setting.