IRON MOUNTAIN® DELL EMC CIO Strategic Marketing Services

A CYBERATTACK IS INEVITABLE.

ARE YOU PROTECTING WHAT MATTERS MOST?

Few healthcare organizations are likely to forget 2017's WannaCry malware attack, which caused dozens of health trusts in the UK's National Health Service to shut down, eventually spreading across 150 countries.

The plain fact is that cybercriminals know that healthcare organizations are an especially alluring target. These organizations are sitting on massive amounts of potentially vulnerable personal health and financial information. At the same time, increased regulatory requirements leave them threatened by steep compliance penalties if a breach occurs.

IDG recently surveyed IT decision-makers at healthcare organizations to understand their most concerning cybersecurity risks and to gauge their preparedness for potential future attacks.

THE SURVEY FOUND THAT

THE VAST MAJORITY

(86%) OF THESE ORGANIZATIONS HAVE EXPERIENCED ONE OR MORE CYBERSECURITY EVENTS, INCLUDING MALWARE ATTACKS, EXTERNAL HACKS, AND/OR ACCIDENTAL DATA LOSS.[1]

WHICH CYBERSECURITY RISKS ARE THESE ORGANIZATIONS MOST WORRIED ABOUT?

THE SHORT ANSWER: A BUNCH OF THEM.

OF THE ORGANIZATIONS SURVEYED,

37% **HAVE EXPERIENCED A RANSOMWARE ATTACK.**

1 in 5 **(19%) THAT EXPERIENCED A RANSOMWARE ATTACK DID NOT SUCCESSFULLY BLOCK THE ATTACK.**

Interestingly, IDG found that "those at larger healthcare organizations (5,000 employees or more) and those with VP+ titles are more likely to report that their organization ***did not successfully block a ransomware attack.***"

OVERALL, 62%
BELIEVE THAT A FUTURE RANSOMWARE ATTACK AT THEIR ORGANIZATION IS "HIGHLY LIKELY."

MORE THAN

HALF

(58%) OF THESE ORGANIZATIONS TOOK "DAYS, WEEKS, OR LONGER" TO GET AFFECTED DATA BACK TO A GOOD STATE AFTER THEIR MOST SERIOUS SECURITY EVENT.

AND

65%

HAD TO REVERT TO DATA VERSIONS THAT WERE "DAYS OR WEEKS" OLD.

WHAT ARE THE TOP COMPLIANCE REGULATIONS DRIVING DATA SECURITY INITIATIVES AT THESE ORGANIZATIONS?

HIPAA was cited by half of them (49%)

Smaller organizations were more likely to indicate the Agency for Healthcare Research and Quality (AHRQ) and the Environmental Protection Agency (EPA).

Despite reporting that they now focus the bulk of their cybersecurity measures on prevention, healthcare organizations still rely on regular backups to protect their most valuable data (which represents 14% of all data, on average).

60% Loss of data

and

52% destruction/encryption of data

are the most concerning threats to backup data.

CYBERSECURITY PAIN MANAGEMENT

The respondents were asked to imagine a cloud-based solution that takes a copy of an organization's mission-critical data and disconnects it from the network, essentially isolating this data set from the network. How valuable would this be for their organization?

"EXTREMELY OR VERY VALUABLE": 73%

They were also asked to imagine a cloud-based solution that provides a "clean room" to ensure that the data to be restored hasn't been compromised before they bring it back to the network. How valuable would this clean room capability be?

"EXTREMELY OR VERY VALUABLE": 79%

Iron Cloud CPR (Critical Protection and Recovery) is a managed data protection solution to safeguard and restore critical data, providing confidence in recovery in the event of a destructive cyberattack. As part of an enterprise risk containment plan, Iron Cloud CPR helps mitigate reputational damage, costs and lost revenue potential from unplanned operational downtime.

IRON MOUNTAIN® DELL EMC CIO Strategic Marketing Services

To learn more, go to
www.ironmountain.com/ironcloudCPR

[1] According to 100 IT decision-makers in the U.S. surveyed by IDG Research March 19-28, 2018