NOV 03
Will Paige

Banks should prepare to spend big on cyberdefenses as ransomware payments reach record levels

Article

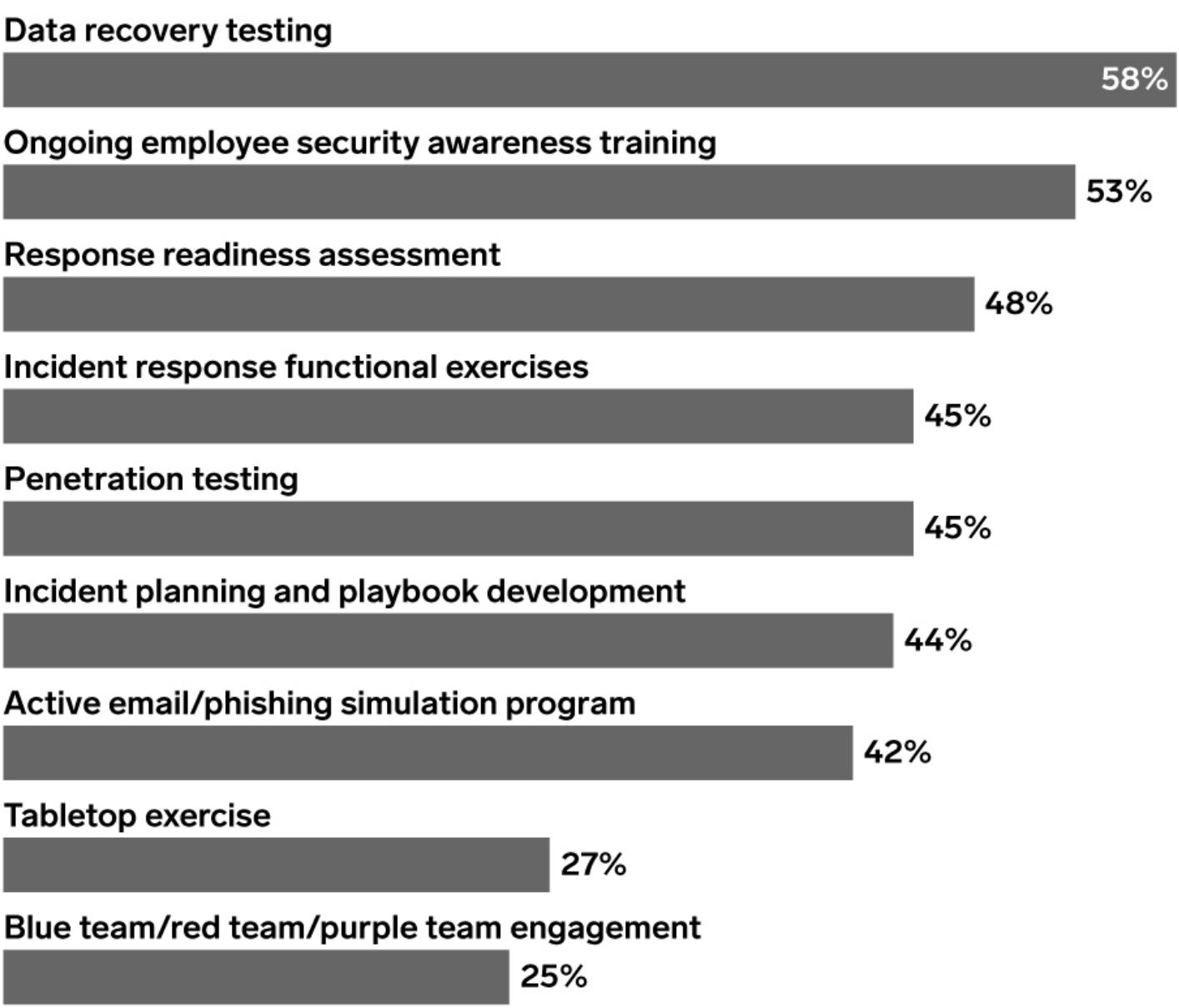
The news: US banks and financial institutions spent almost $1.2 billion in ransomware-related payments in 2021—almost triple the previous year, according to the US Treasury Department.

Cyberattackers target Wall Street: The Treasury's Financial Crimes Enforcement Network (FinCEN) said in a new report that ransomware posed a "significant threat" to banks.

- The number and total value of ransomware-related payments reached record levels and far exceeded that of any previous year, per the report.
- The increase was blamed on a mix of more ransomware attacks and improved reporting.

Ongoing Enterprise Ransomware Preparedness Activities and Processes According to IT and Cybersecurity Experts in North America and Western Europe, Jan 2022

% of respondents



Source: OwnBackup, "The Long Road Ahead to Ransomware Preparedness" conducted by Enterprise Strategy Group, March 31, 2022

274553

eMarketer | InsiderIntelligence.com

What should banks do?

1. **Invest now:** Cybersecurity was a leading concern for US bank executives polled this year by Cornerstone Advisors, second only to worries around attracting qualified talent. Spending big to improve cybersecurity can feed back into banks' bottom lines by strengthening digital trust and confidence among customers. And investing now can save money in the long run by preventing costly data breaches and fraud.
2. **Prioritize compliance:** Spending on regulatory technology will top $130 billion in 2025, per Juniper Research. And given that FinCEN described ransomware as a "serious threat" to US national security, more stringent regulation could be on the way. Banks should monitor this closely and be prepared to report on cybersecurity incidents and ransomware payments to watchdogs.
3. **Consider the wider ecosystem:** There's been a sharp increase in cases of island hopping, where cyberattackers target companies' more vulnerable partner networks rather than launching direct attacks. This is a particular problem for banks, which commonly partner with smaller fintechs, data networks, and developers to participate in open banking, banking as a service (BaaS), and embedded finance. Banks need to monitor and protect against any potential weak points in their full partner network.

Areas of Enterprise IT Environment Affected by Successful Ransomware Attacks According to IT and Cybersecurity Experts in North America and Western Europe, Jan 2022

% of respondents

Source: OwnBackup, "The Long Road Ahead to Ransomware Preparedness" conducted by Enterprise Strategy Group, March 31, 2022

274552

eMarketer | InsiderIntelligence.com