INSIDER INTELLIGENCE | eMarketer

AUG 12
Jacob Bourne

A basic laptop hacked a top encryption algorithm in an hour, and there's no backup plan

Article

The news: A promising algorithm designed to guard against future, more sophisticated cyberattacks was **hacked in an hour by a single-core PC**.

- The **US National Institute of Standards and Technology (NIST)** selected four encryption algorithms as candidates for protecting against the code-breaking power of future quantum computers, but one of the finalists was unable to withstand existing hacking capabilities, per Ars Technica.
- The algorithms are part of the **NIST's post-quantum cryptography (PQC) plan to replace current encryption standards with more advanced ones by 2024** to protect against quantum breaches, per Forbes.
- The plan involves a massive technology overhaul that the **World Economic Forum** expects will require over **20 billion digital devices be upgraded or replaced in a costly global migration that could span a decade**.

How we got here: The worsening cybersecurity landscape, marked by a continuous increase of sophisticated attacks, is on track to reach a crescendo as quantum computing advances.

- In 1995, a researcher created Shor's algorithm, which is capable of defeating current computer security standards.
- The algorithm's limitation is that it can only run on a quantum computer that's more advanced than the ones available today, though that notion could already be outdated.
- In the interim, **hackers are in a "harvest now, decrypt later" mode**.
- The quantum hacking scheme involves bad actors—governments and individuals—harvesting encrypted data to keep until they get a quantum computer powerful enough to access the sensitive data, in an event dubbed **Y2Q**.
- As the quantum field advances, the federal government is trying to fend off the looming global security catastrophe.

The problem: A **Zapata Computing** team demonstrated that a class of more efficient, less precise algorithms, known as heuristic algorithms, **can break current advanced encryption systems using simpler quantum computers**. And the NIST is reportedly ignoring the issue.

The NIST's planned sweeping upgrade might not work, leaving businesses and taxpayers holding the bill while all our sensitive data is exposed.

- More frequent and sophisticated cyberattacks are already targeting businesses of all sizes, individuals, healthcare institutions, and government agencies.

- The growing problem can erode consumer confidence, with data privacy compromised while people shop, bank, and interact online.

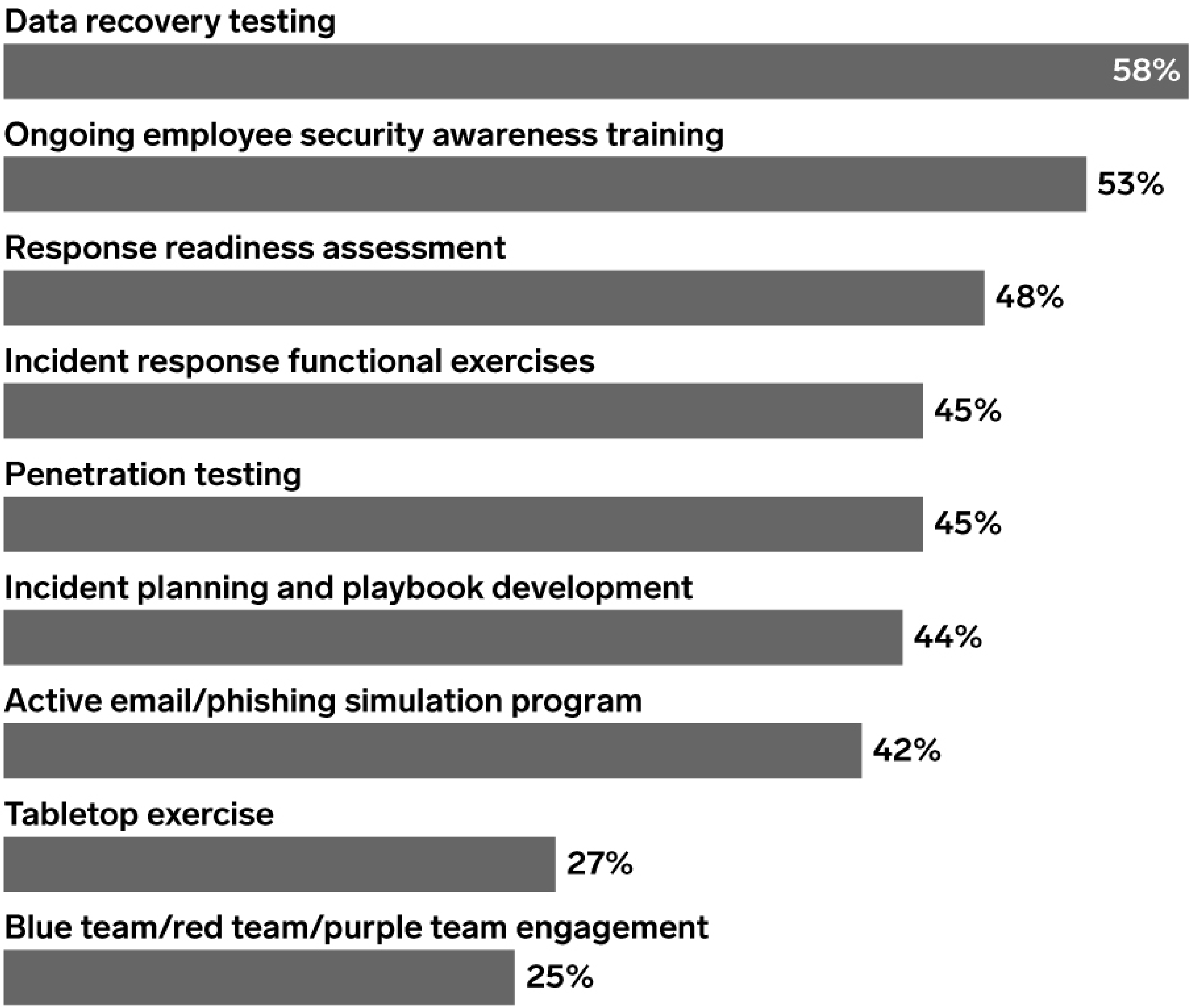
What can be done? A broader coalition of academics, private sector experts, and government security officials could pool their knowledge to devise more foolproof solutions.

- Companies can diversify their security systems and make them more flexible for updating as existing encryption standards become obsolete.
- The NIST could incentivize developers to tackle the heuristic algorithm security gap and other blind spots.
- A global security overhaul of billions of digital devices likely requires a cybersecurity talent base that doesn't exist. More investment could be made to build an army of highly trained cybersecurity professionals.

Dive deeper: *Learn more about the vulnerable digital business world in our The Cybersecurity Risk report.*

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

This article originally appeared in Insider Intelligence's Connectivity & Tech Briefing—a daily recap of top stories reshaping the technology industry. Subscribe to have more hard-hitting takeaways delivered to your inbox daily.

- *Are you a client? Click here to subscribe.*

Want to learn more about how you can benefit from our expert analysis?Click here.