

SECTION 02

The self-detection paradox

100% say their detection is Excellent or Good. 58% got breached anyway. Both numbers come from the same 170 respondents.

Confidence is running ahead of the numbers

The detection self-rating has inverted in 12 months. Breach prevalence has not.

100%

Rate their real-time breach detection as Excellent or Good. Zero rated it Fair or Poor.^[4]

Asked to rate their detection ability in real time, 100% of respondents selected Excellent (48%) or Good (52%). No one rated detection as Fair or Poor. In the same sample, 58% experienced at least one email-related data breach in the past 24 months.^[4]

Those two numbers cannot both describe a healthy system. Either detection is not performing the way leaders believe, or prevention is where the failure is happening. The post-breach behavior data tells us what breached organizations themselves believe.

42% → 0%

The detection self-rating has inverted in 12 months. Perceived capability is rising faster than breach prevention is improving.

58%

Experienced at least one email-related data breach in the past 24 months. 23% experienced more than one.^[4]

After their most recent email breach, the top three actions were: (1) implemented or strengthened encryption policies at 47%, (2) added or increased phishing simulation training at 44%, (3) changed email providers or security vendors at 42%.^[4]

Encryption policy changes topped the list. Not better monitoring. Not faster alerts. Not new detection tooling. Organizations that lived through a breach concluded that prevention, specifically encryption, was what needed to change first.

18%

Of breached organizations made no significant changes at all. 1 in 5 experienced a breach and did nothing.^[4]



Secure every email you send and receive

Paubox combines healthcare compliance with AI to protect organizations from the most sophisticated attacks.

[Talk to an expert](#)

