COSTS AND CONSEQUENCES OF GAPS IN VULNERABILITY RESPONSE

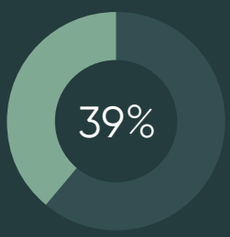
THE RACE TO OUTPACE THE ATTACKERS CONTINUES

17%

Increase in cyberattack volumes over the last 12 months

27%

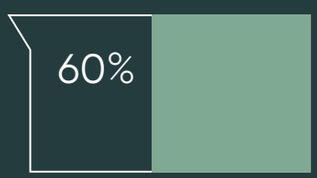
Increase in cyberattack severity over the last 12 months



39% of breach victims knew they were vulnerable before they were breached

60% of breach victims said they were breached due to a vulnerability for which a patch was availiable

ORGANIZATIONS ARE NOT KEEPING UP WITH THE HACKERS



60% say attackers are outpacing enterprises with technology such as machine learning and artificial intelligence

52% of respondents say their organizations are at a disadvantage in responding to vulnerabilities because they use manual processes

48%

Almost half of respondents (48%) report that their organizations had one or more data breaches in the past two years. 60% of these respondents say these breaches could have occurred because a patch was available for a known vulnerability but not applied

PATCHING HELPS PREVENT DATA BREACHES

MANUAL PROCESSES AND SILOED TOOLS DELAY PATCHING

No common view of assets and applications across security and IT

+

No easy way to track whether vulnerabilities are being patched

+

Things slip through the cracks because emails and spread-sheets are used to manage the patching process

=

AUTOMATION AND ADDITIONAL STAFF REDUCE RESPONSE TIME TO VULNERABILITIES

80%

80% of organizations that use automation say they have the ability to respond to vulnerabilities in a shorter timeframe

36%

Only 36% of respondents say their companies have enough staff to patch fast enough to prevent a data breach

Organizations that invest in automation experience the following benefits:

1. reducing downtime, patching in a timely manner
2. able to prioritize the most critical vulnerabilities
3. increasing the efficiency and effectiveness of the IT staff

Learn how organizations reduce the time to respond to vulnerabilities.

Get the Report

servicenow | Ponemon INSTITUTE