PKWARE

The Ripple Effect of a Data Breach

Data breaches are often defined in dollar amounts, but it's not simply a cost problem. Nor are breaches just about the data. It's about an organization's ability to continue producing and selling their products and/or services.
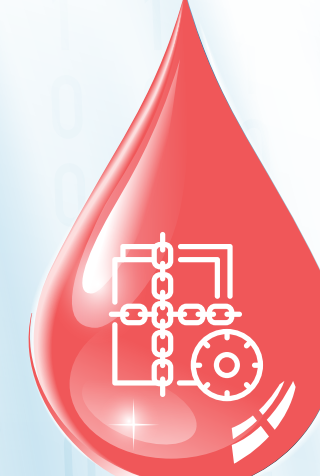
Security is actually a business problem.

↑**10%** The global average total cost of a data breach has increased to **$4.24** million

$4.62 million
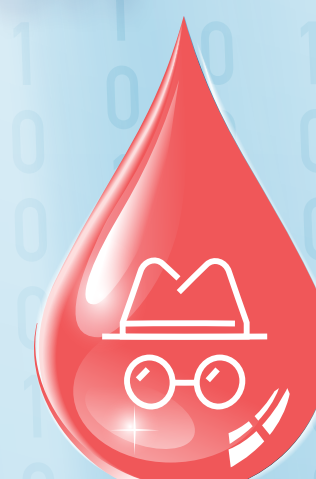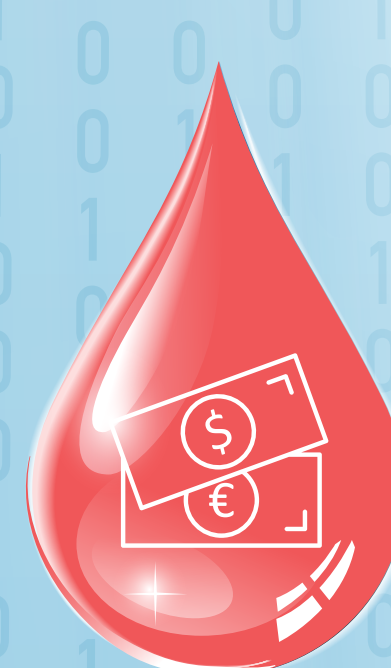The cost goes up higher when ransomware is involved

38% Lost business accounts for the largest share of the average cost of a data breach at approximately **$1.59** million
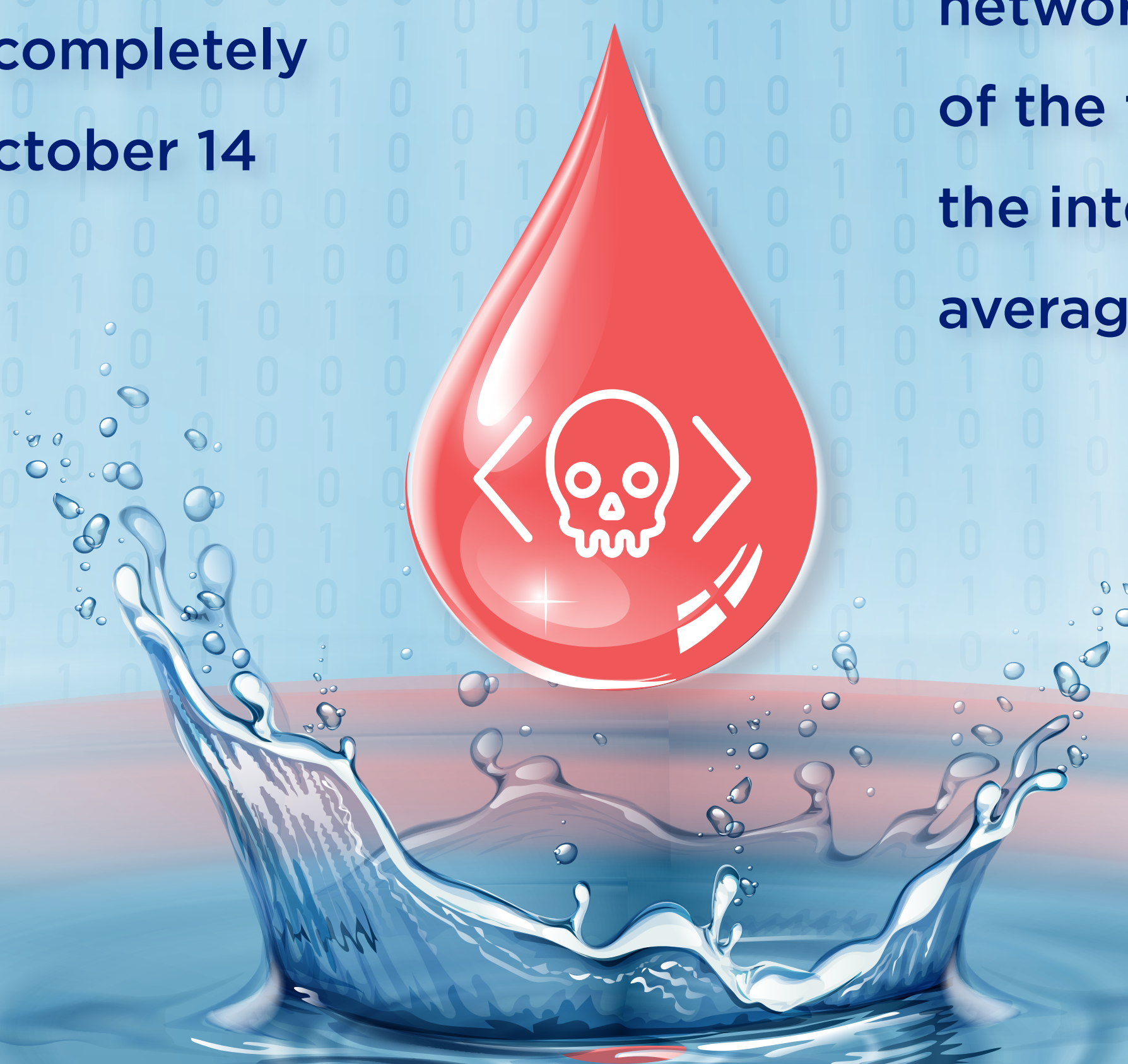
287 days
On average, it takes **212** days to identify and **75** days to contain a data breach. If the breach occurred on January 1, it would not be completely resolved until October 14

2 days
Attackers can breach a network perimeter **93%** of the time and penetrate the internal network an average of **48** hours later

Initial Impact
Inability to access critical information

Detection and Escalation
Uncover what happened and determine the most immediately necessary fix

Notification
Inform impacted individuals as well as compliance regulators (GDPR, CCPA, etc.)

Post-Breach Response
Provide activities and services for breach victims to secure and monitor their data
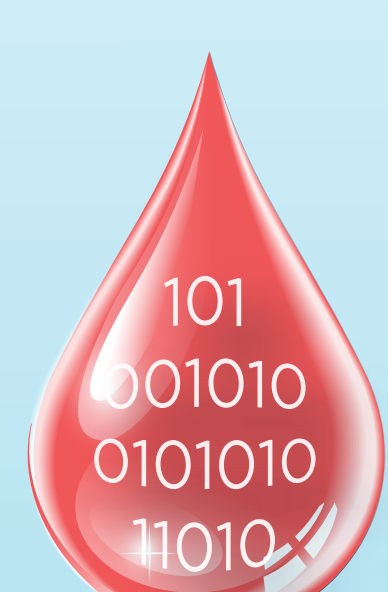
Lost Business
Replace revenue lost during system downtime, and mitigate the effects of reputation loss

Time
It takes an average of 287 days to identify and contain a data breach, longer if >50% employees are remote

The complexity of today's cyber environments—from hybrid environments spread across locations and teams to remote and hybrid work—all but guarantees the inevitability of a data breach. Essentially, cybersecurity teams should plan for failure: Assume your organization will at some point suffer a breach and put measures in place that can limit the widespread effects.

Learn more about the far-reaching effects of a data breach and how to minimize the damage in our free ebook, How Much Can You Lose in A Cyber Attack?

DOWNLOAD NOW

pkware.com/resources