WINSTON
&STRAWN
LLP

At A Glance—The 2019 Verizon Data Breach Investigations Report

JUNE 28, 2019

Recently, Verizon released its 2019 Data Breach Investigations Report (Report), analyzing cybersecurity trends. The Report is based on an analysis of 41,686 security incidents, including 2,013 confirmed data breaches. Several of the Report's findings are useful in helping organizations identify likely attack vectors, prioritize defensive measures, and prepare to respond to potential incidents.

First, the Report found that year-over-year trends show that breaches by state actors are on the rise, while breaches by organized crime groups are falling. This may suggest an increase in attackers' sophistication and resources, as well as a shift in priorities since attacks by state actors are less often purely financially motivated.

Second, the Report highlighted the importance of being prepared to respond to a security incident *before* the attack takes place. For instance, in a successful breach, the data exposure typically happens in minutes while discovery and containment may take months.

Third, the Report found that the effectiveness of phishing attempts seem to be in decline even while nearly a third of all breaches still involve phishing. In large part, this is because the click rate on phishing emails has lessened and employees are increasingly likely to quickly report when they click on a phishing email or link. Increased awareness of phishing and other types of social engineering attacks is important as it is often a company's senior executives who face such attacks. For instance, the Report found that C-level executives are twelve times more likely to face a social engineering attack as opposed to nine times more likely in the past.

Finally, the Report found that ransomware attacks remain a serious threat across all industries. In the past year, ransomware accounted for roughly a quarter of all security incidents.

TIP: The report breaks down security incidents in detail by industry, attack method, and attack vector. We recommend looking at the report for details specific to your industry and company infrastructure, and contacting Winston's Global Privacy & Data Security Task Force to make sure your company has an appropriate incident response plan in place.

1 Min Read

Authors

David Houck

Eric Shinabarger

Related Locations

Chicago   Houston

Related Topics

Data Breach

Related Capabilities

Privacy & Data Security   Technology, Media & Telecommunications

Related Regions

North America

Related Professionals

David Houck

Eric Shinabarger

This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.