The CISO's Playbook: Stay Ahead of Friday Breach Effects

SecurityScorecard

Background

While ransomware attacks spike on holidays and weekends, the most common day to discover a breach is Friday. This phenomenon poses challenges for every organization, its workforce, partners, customers, and society in general.

SecurityScorecard examined four years of data breach reports to uncover discovery trends for every day of the week. Here's your **Friday Breach Effect Report**

Breach Discovery Methods

SecurityScorecard analyzed data breach trends reported over a four-year period. Breaches included all instances of data exposure, whether deliberate or accidental, and by both external bad actors and insider threats.

Although SecurityScorecard aimed to examine data breaches globally, the complexity of international breach reporting requirements, or the lack of them, presented unique data collection challenges. In countries that have implemented the General Data Protection Regulation (GDPR), reporting data breaches to the regulator is mandatory, but the regulator does not have to notify the public. Other countries don't mandate reporting at all. In the U.S., a patchwork of state rules often—but not always—requires organizations to publicize breaches and inform customers. The net effect is that many U.S. incidents are usually well publicized, while breaches in other countries aren't, effectively creating a U.S. bias in the data set.

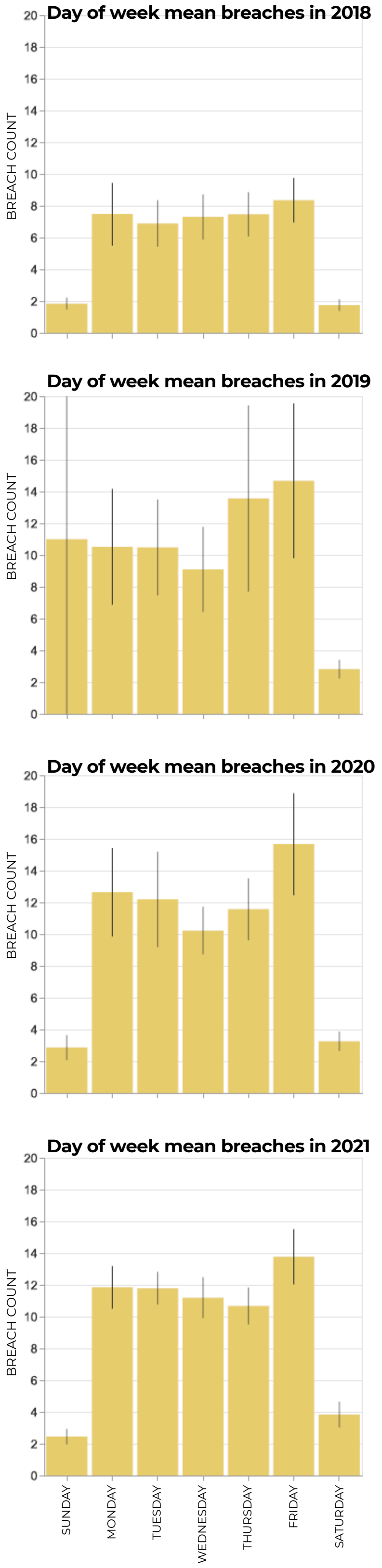
Organizations must be hyper vigilant as the week winds down.

SecurityScorecard tracked incidents by the date of discovery, which may differ from when the breach actually occurred. In some instances, breach discovery dates were estimated from press reports or other sources.

Key Findings

- The multi-year data analysis revealed that **breaches were reported more frequently on Fridays**, with a statistically significant **Friday Effect** in 2021.
- A spike of Sunday breach discoveries in 2019 serves as a cautious reminder that cyberattacks occur on any given day of the week.

Daily Breach Trends



The chart to the left shows the number of breaches reported for each day of the week between 2018 and 2021. It also shows the 95% confidence interval for each day.

The Friday Effect

The multi-year data analysis revealed that breaches were reported more frequently on Fridays, with a statistically significant Friday Effect in 2021.

The cause of the Friday Effect is hard to pin down. It could be that workers lose work-related devices more frequently on Fridays, or that security teams spend more time on analysis on Fridays, or it could be that attackers are more active as the weekend approaches. We have seen claims that the Friday Effect is due to companies trying to manage the release of bad news, but we've seen no evidence this is the case.

Whatever the cause of the effect, it's become increasingly obvious over the years. Security teams must prepare for attacks as the weekend draws near.

A Sunday Anomaly

On a warm May Sunday in 2019, a strain of key-logging malware infected several cloud services, resulting in the exfiltration of data from multiple websites (the Magecart skimmer [2]). This caused a spike in the mean number of reported breaches and confidence intervals on Sundays, and an abnormally high breach count for May 2019.

Although this anomaly didn't exceed the frequency of Friday breach reports, it is a good reminder that cyberattacks can happen on any given day of the week.

Heightened Cybersecurity Alert

Regardless of Friday data breaches or the Sunday anomaly, organizations can expect a rapid increase in ransomware attacks in the coming years, many of which will likely occur during the weekend, according to various industry experts [1].

Organizational leadership, security teams, and other staff must be vigilant and alert, especially at week's end.

The CISO's Playbook

CISOs need to train their organizations regularly in how to prevent and manage a breach. SecurityScorecard's analysis concludes that organizations should regularly schedule unannounced training on Fridays and implement security best practices that include incident response simulations, tabletop exercises, and specific, defined contingency plans for onsite and offsite personnel in every department. Add the following list to your data breach playbook today and avoid headaches in the aftermath of an attack tomorrow:

Arm incident responders with a solid game plan and establish effective communication protocols to eliminate hesitation during a breach event.

- Can you contact every internal stakeholder late on a Friday night?
- Is your roster and schedule of on-call incident responders current?
- Are cybersecurity escalation paths clearly documented and automated to rapidly manage unacknowledged security alerts?
- Do onsite security managers and SOC teams, as well as work-from home security personnel, have data breach contingency plans, and do they understand their specific role in your playbook?

Operationalize PR management & marketing teams to swiftly diffuse public scrutiny and tend to the needs of your customers during a breach crisis.

- Have they "blessed" a communications template to anticipate—and hopefully outpace—the public narrative that will rapidly grow on social media and in the press?
- Are they available late on Fridays? Have you retained a third-party brand agency to support internal staff and address exhaustive media relations?
- Do you have multiple channels for communication with customers, partners, and service providers in case the breach impacts your email or website platforms?

Embrace governance, risk & compliance advisors to navigate the regulatory landscape.

- Do they know which U.S. and international notification requirements are in play, and which clauses apply to your organization?
- Are they familiar with cyber insurance breach notification and claims procedures to speed recovery of financial losses?

Prepare for the unpredictable. Vulnerabilities are often discovered by a press inquiry or the dreaded ransom note. Hackers, media, and anyone with access to the right resources can learn what software, services, and relative components that your website uses. They can determine your vulnerability to a data breach in a matter of minutes.

Consequently, **the first strategic move in every CISO's playbook is to assess their organization's cybersecurity posture, and that of their partnerships,** because being forewarned is forearmed. Such knowledge can allow an organization to **own the narrative.** It will ultimately reduce the adverse effects of a breach on public perception and customer trust.

References

[1] https://us-cert.cisa.gov/ncas/alerts/aa21-243a

[2] https://en.wikipedia.org/wiki/Web_skimming

[3] Benjamin Edwards, Steven Hofmeyr, Stephanie Forrest, Hype and heavy tails: A closer look at data breaches, Journal of Cybersecurity, Volume 2, Issue 1, December 2016, Pages 3–14, https://doi.org/10.1093/cybsec/tyw003

[4] https://www.mass.gov/info-details/requirements-for-data-breach-notifications

[5] https://en.wikipedia.org/wiki/Web_skimming

[6] https://gdpr.eu/gdpr-fines-so-far/

About SecurityScorecard

SecurityScorecard helps security professionals work collaboratively to solve mission-critical, cybersecurity issues in a transparent way. The SecurityScorecard platform provides continuous, non-intrusive cyber risk monitoring of any organization and its ecosystem.

info@securityscorecard.com

1-800-682-1707 | securityscorecard.com

Start responding to cybersecurity questionnaires faster. Learn more at https:// securityscorecard.com/platform/atlas.

SecurityScorecard