BITSIGHT

REPORT

From Months to Minutes: Can New Regulations Accelerate the Cyber Incident Disclosure Process?

In the wake of numerous high profile cyber incidents, including ransomware and attacks impacting critical infrastructure, policymakers are considering new cyber incident disclosure laws to improve cybersecurity. On March 15, 2022, President Biden signed legislation[1] requiring critical infrastructure organizations to disclose "substantial" cyber incidents to the Federal government within 72 hours. The Securities and Exchange Commission (SEC) is also considering new regulations[2] requiring disclosure of "material" cyber incidents within 96 hours.

Are organizations prepared to meet these new cyber incident disclosure requirements?

Bitsight analyzed more than 12,000 publicly disclosed cybersecurity incidents from 2019-2022 to assess the current state of cyber incident disclosure. We examined how organization size and incident severity affects the timeliness of incident discovery and disclosure. By understanding the current state, policymakers gain perspective on whether organizations will be able to meet new disclosure requirements. Bitsight's observations suggest that compliance with these new obligations will be difficult to achieve. Bitsight observes:

- **Cyber incident discovery and disclosure is a long, slow process.** In a world that requires speed and rapid response, data suggests that the time between incident occurrence, discovery, and disclosure is quite slow. Cyber incidents are typically discovered and disclosed after weeks and months, rather than hours and days. It takes the average organization 105 days to discover and disclose an incident from the date the incident occurred; of that time, organizations don't discover an incident until 46 days after it has occurred, and they don't disclose an incident until 59 days after discovery. This is well beyond the 72-96 hour disclosure requirements envisioned by policymakers.

- **Larger organizations are faster at discovering and disclosing incidents than smaller organizations, but they are still slow.** The largest organizations (10,000+ employees) are 30% faster at discovering and disclosing incidents compared to others. However, it takes the largest organizations an average of 39 days to discover an incident and 41 days to disclose an incident, far beyond the timeframes proposed in new requirements.

- **It takes twice as long for organizations to disclose higher severity incidents once they are discovered compared with lower severity incidents.** It takes the average organization over 70 days to disclose a moderate, medium or high severity incident once it has been discovered compared with the 34 days it takes to disclose low severity events. Yet new regulations require the disclosure of these "substantial" or "material" incidents within 72-96 hours. Achieving compliance with these new obligations may be difficult to attain.

[1] https://www.techtarget.com/searchsecurity/news/252514713/Biden-signs-law-on-reporting-critical-infrastructure-cyber-attacks
[2] https://www.sec.gov/news/press-release/2022-39

New legislation and regulations on cyber incident disclosure

There are several new cyber incident disclosure regulations and laws under consideration:

- On March 15, 2022, President Biden signed legislation requiring critical infrastructure organizations to disclose "substantial" cyber incidents to the Federal government. Critical infrastructure organizations include hospitals, utilities, transportation, and others that provide vital functions that are essential to physical or economic security or public health or safety. The "Strengthening American Cybersecurity Act of 2022" requires organizations to report substantial cyber incidents to the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) within 72 hours. Advocates believe that new requirements will provide governments and interested parties with greater data and visibility into critical incidents, which can be used to improve overall defenses.

- On March 9, 2022, the Securities and Exchange Commission (SEC) held an open hearing to discuss new, mandatory requirements for public companies to disclose cybersecurity incidents and risks to regulators and investors. SEC Chair Gary Gensler previously stated that cybersecurity information "presented in a consistent, comparable, and decisionuseful manner" will benefit organizations and investors. Among the requirements, the proposed SEC rule would require incident disclosure within four business days after a public company has determined that it has experienced a "material" cyber incident.

By focusing on "incidents," these new proposals are designed to address gaps in current breach disclosure laws. Fifty U.S. states and numerous countries have data breach notification laws[3] in place, which place differing obligations on organizations to notify customers, impacted individuals, government officials, and other entities when they experience a data breach. Data breaches are typically defined as incidents where sensitive, protected, or confidential data is copied, viewed, stolen, or used by unauthorized persons. Laws vary on their requirements for the timeliness of breach notifications —some require disclosure "without unreasonable delay" while others require notification within specific time frames (ex: within 10, 45, or 60 days of discovering a breach).

How are incidents and breaches related? Data breaches are a type of security incident, which covers many more types of cyber scenarios. For example, the "Strengthening America" law might require the disclosure of data breaches, but also a broad range of other cyber incidents that may have impact on national security, public health, or safety, but did not necessarily result in data loss or compromise. Other cyber incidents requiring disclosure could include the compromise of valuable intellectual property or ransomware incidents.

> "
>
> Compared with traditional data breach laws, new cyber incident disclosure requirements cover a broader set of incidents and require more rapid, timely disclosure.

[3] https://www.itgovernanceusa.com/data-breach-notification-laws

Analyzing publicly disclosed security incidents

To better understand the state of current incident disclosure, Bitsight analyzed more than 12,000 publicly disclosed cyber incidents that occurred around the globe between 2019-2022.

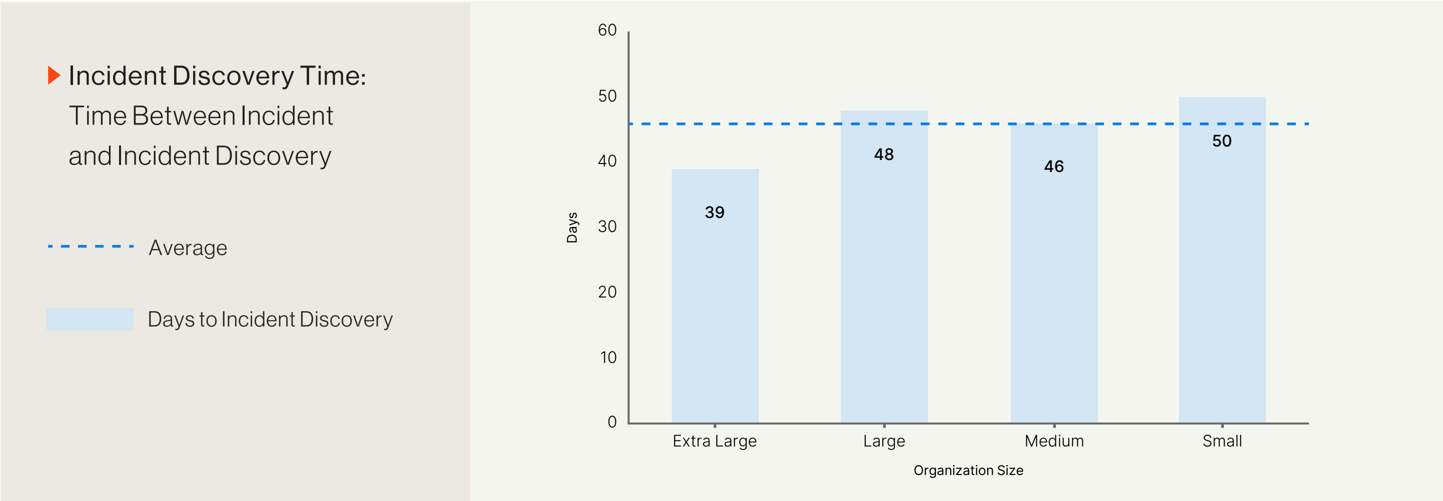
- Our analysis considered a broad array of cyber incidents, which include publicly disclosed events of unauthorized access or exposure, often (but not always) involving data loss or theft.
- The information we collect from public disclosures typically includes the type of incident, date of the original incident, date of incident discovery, and date of disclosure.
- Disclosing organizations are segmented by employee count: Extra Large (10,000+ employees), Large (1,000-10,000 employees), Medium (500-1,000 employees), and Small (<500 employees).
- We analyzed the severity of incidents by leveraging BitSight's severity classification methodology (0-3 scale). In this framework, higher severities are due to a combination of more serious incidents (e.g. ransomware v. human error) and higher record counts.

The following sections outline our findings related to the time it takes organizations to discover and disclose incidents, including the impact of organizational size and incident severity.

1. Incident discovery time

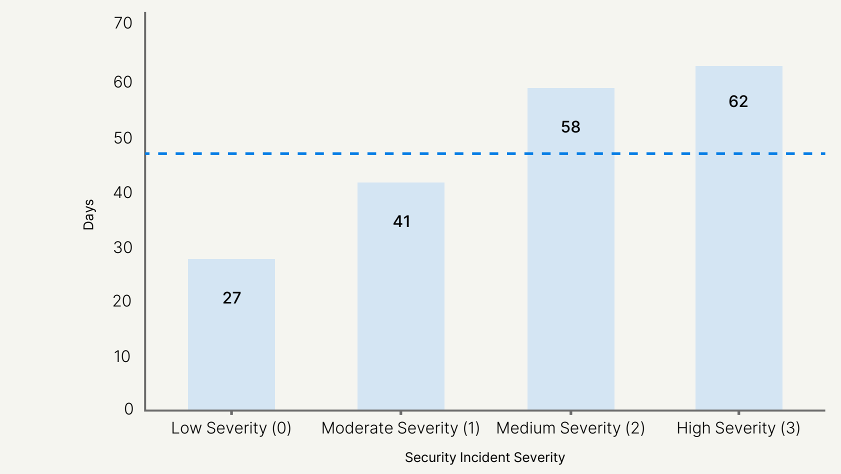
First, we measured the time it takes for organizations to discover that an incident has occurred. We call this "Incident Discovery Time."

Despite massive global investment in cybersecurity technology and capabilities in recent years and a growing focus on the importance of rapid detection and remediation, cyber incident discovery remains a significant challenge for organizations of all sizes. According to Bitsight's analysis of publicly disclosed incidents, it takes 46 days for the average organization to discover a cyber incident in their environment. BitSight finds that Extra Large organizations on average are slightly faster (~20 percent) at incident discovery than the average organization.


Incident Discovery Time: Time Between Incident and Incident Discovery

Bitsight analyzed whether the severity of an incident impacts discovery timeframes. We find that organizations discover low severity incidents more than 2 times faster than medium and high severity incidents. One potential explanation for this discrepancy: employee mistakes (which typically result in less severe consequences) may be more easily discoverable compared with the sophisticated techniques leveraged by determined attackers.

Incident Discovery Time: Time Between Incident and Incident Discovery by Severity

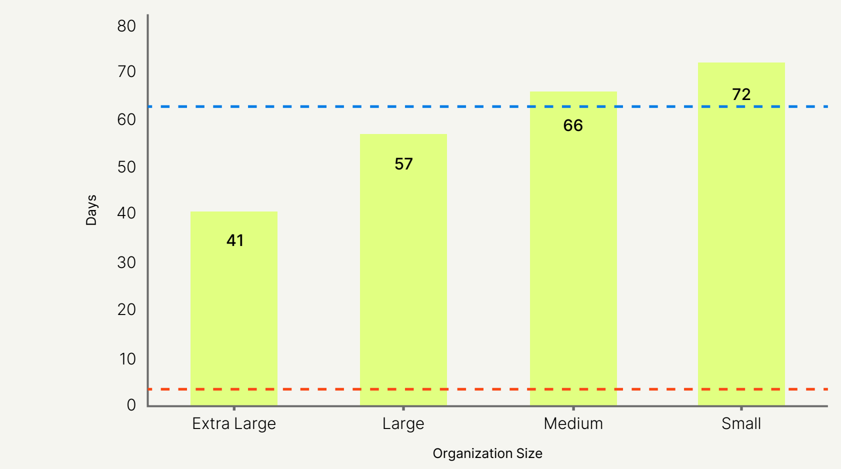


2. Delay in incident disclosure

Second, we measured the time it takes organizations to disclose that an incident has occurred. We call this "Disclosure Delay."

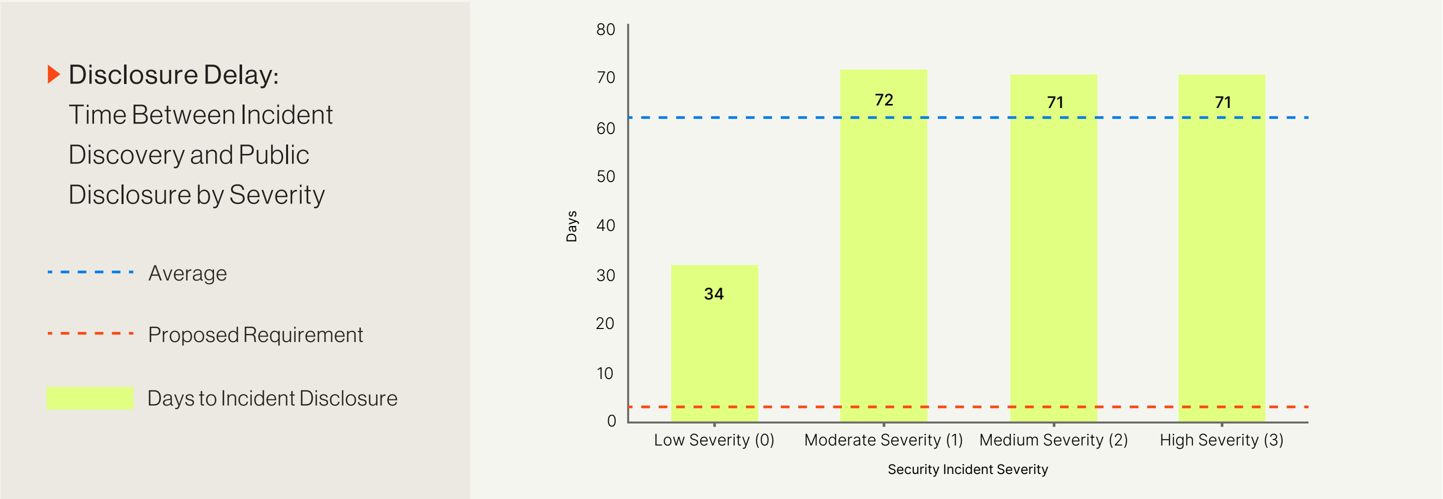
Organizations who discover a cyber incident typically take weeks—if not months—to disclose the incident publicly. It takes the average organization 59 days to disclose an incident after initially discovering it. Bitsight finds that the largest organizations (10,000+ employees) are 50 percent faster to disclose incidents compared with other organizations. Uncertainty about disclosure obligations (what to disclose, to whom, how, and when) and confusing jurisdictional requirements may be contributing factors to these delays. It is also possible that larger organizations may have greater experience or better understanding of their legal obligations compared with smaller organizations.

Disclosure Delay: Time Between Incident Discovery and Public Disclosure



The severity of an incident is a factor in disclosure timeliness. After discovering an incident, it takes organizations twice as long to disclose moderate, medium, and high severity incidents compared with low severity incidents. It is possible that organizations are more hesitant or careful about disclosing incidents that could have more damaging financial, legal, or reputational impact.

In both charts we have mapped the new and proposed incident disclosure requirements to highlight the significant gap that exists between historical performance and the proposed disclosure timeframes. It is important to note that new regulations require the disclosure of "substantial" or "material" incidents within 72-96 hours. Achieving compliance with these new obligations may be difficult to attain given past performance in disclosing "medium" or "high" severity incidents.

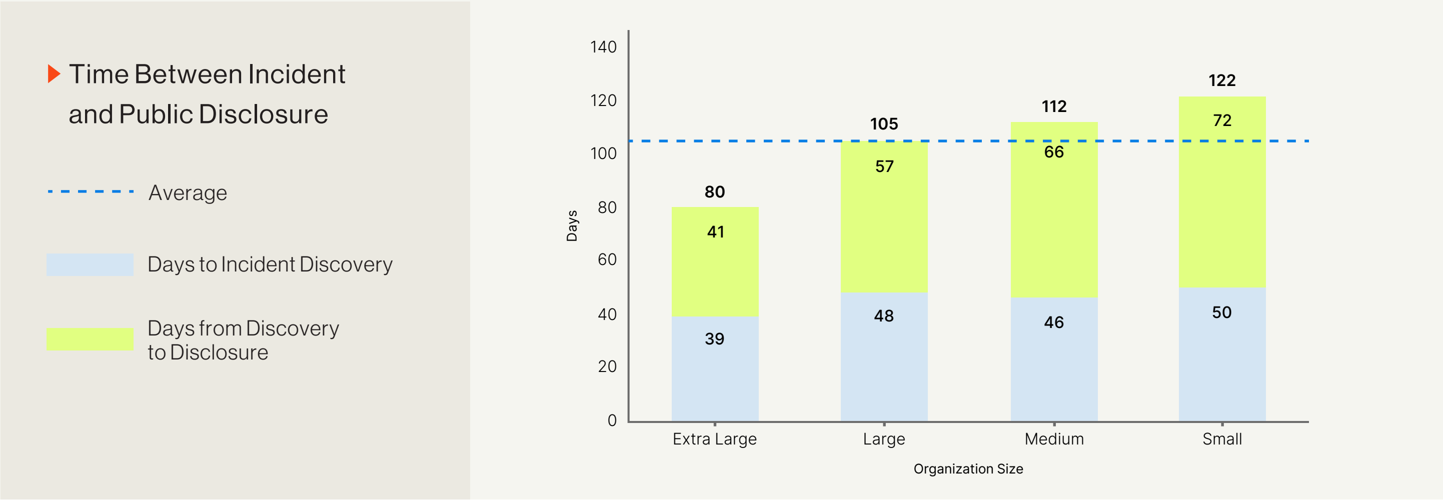

Disclosure Delay: Time Between Incident Discovery and Public Disclosure by Severity

3. The overall incident disclosure timeline

Finally, we combine the time it takes for organizations to discover and disclose information to get the full picture. We call this "Overall Incident Disclosure Timeline."

It takes the average organization 105 days to disclose a security incident from the date the incident initially occurs. Bitsight finds that the largest organizations (10,000+ employees) take on average 80 days between the date of the initial incident to the date of disclosure; this timeline is 30 percent faster compared with the average rate. However, 80 days between the initial incident and disclosure—including 41 days to disclose an incident once it has been discovered—is much longer than the timelines in the new policy proposals discussed above.

Incident severity clearly has a significant impact on the overall incident disclosure timeline. It takes twice as long for organizations to discover and disclose moderate, medium, and high severity incidents compared with low severity incidents. For more severe incidents, the average time for discovery and disclosure is more than four months.


Time Between Incident and Public Disclosure

Conclusion and recommendations

New laws and regulations require fast, timely cyber incident disclosure of significant, material incidents. Advocates of these measures believe this will improve overall defenses.

Based on Bitsight's analysis of publicly disclosed incidents from 2019-2022, these new requirements may be difficult to implement without significant changes in organizational preparedness and capabilities.

Government officials should expect that organizations will have difficulty in meeting notification requirements measured in hours or days. Organizations of all sizes—including the largest organizations—face challenges in timely incident discovery and disclosure, despite legal obligations to do so. Organizations of all sizes particularly struggle to provide timely notification of severe and material incidents—the very incidents that policymakers would like to become more aware of.

While new incident notification laws may be a critical step in improving government situational awareness, Bitsight also recommends that government officials continue pursuing additional methods of data collection in order to gain real-time understanding of challenges affecting critical infrastructure and other organizations.

Organizations can do more to improve their cybersecurity posture and reduce the likelihood that they will experience a significant or material cyber incident. Bitsight finds that timely remediation of vulnerabilities, reducing attack surface exposure, and implementing sound cybersecurity hygiene all measurably reduce the likelihood of experiencing cyber incidents, including ransomware[4]. Focusing on detection and response is critical in shrinking the overall timeline between incident occurrence, discovery, and disclosure. Organizations should focus on measures that:

- Improve incident detection and monitoring capabilities.
- Improve awareness of disclosure obligations
- Ensure that the company's incident response plan includes a damage assessment process to determine incident materiality

Bitsight will continue to monitor changes in discovery and disclosure patterns in the months ahead.

Maham Haroon, Jake Olcott, Tom Montroy and John Burger contributed to this analysis.

[4] https://www.bitsight.com/blog/ransomware-prevention