November 3, 2022

Breach Reporting Trends: Fundamental Shifts on the Horizon

Kim Peretti
Alston & Bird

Edi Goodman
TransUnion

Nick Barnaby
General Dynamics

Marie Dukes
FMC Corporation

Privacy+ Security Forum

Speakers

Kim Peretti

Partner and Chair, Privacy Cyber & Data Security
Alston & Bird

Edi Goodman

International Privacy Lead Counsel
TransUnion

Nick Barnaby

Deputy General Counsel and Assistance Corporate Security
General Dynamics

Marie Dukes

Chief Global Employment & Data Privacy Counsel
FMC Corporation

Agenda

Privacy+ Security Forum

1. Breach Notification Statutes – US Trends
2. Breach Notification Statutes – Global Trends
3. Cyber Incident Reporting Statutes – US Trends
4. Cyber Incident Reporting Statutes – Global Trends
5. Cybersecurity Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)
6. Practical Tips

Breach Notification Statutes – US Trends

Privacy+ Security Forum

Breach Reporting - US

- All 50 states have state data breach notification statutes.
  - Updates to these laws in 2021 and 2022 have, among other things, expanded the definition of personal information and expand reporting to state regulators.
- The FTC stated that Section 5 of the FTC Act creates a “de facto breach disclosure requirement” in a May 2022 blog post.
  - Going forward, this indicates notification may be required even if there is no statutorily defined PII compromised in an incident, including to consumers and B2B notification.
- On December 9, 2021 the FTC published a notice of proposed rulemaking to the Federal Register including a reporting requirement for financial institutions of certain cybersecurity events to the FTC.
  - Would require reporting in the event of a cybersecurity event in which the covered financial institution determines customer information has been misused or is reasonably likely to be misused and 1,000 or more consumers have been affected ore reasonably may be affected.

Breach Notification Statutes – Global Trends

Privacy+ Security Forum

Breach Reporting - Global

- China's PIPL became effective in 2021, requiring personal information processors to immediately inform the relevant competent departments and data subjects subject to a risk of harm test.
- Brazil's LGPD, passed in 2018 and fully came into force in 2021, requires reporting to the ANPD and the data subjects subject to a risk of harm test.
- The European Data Protection Board published a proposed updated version of regulatory guidance on personal data breaches under GDPR in 2022. The proposed guidance seeks to impose heavier notification obligations on U.S. controllers.
- New breach reporting requirements in force in Quebec as of September 22, 2022, in addition to requirements of PIPEDA, with notice due to the Commission as well as individuals when a breach presents a risk of serious injury.

Cyber Incident Reporting Statutes – US Trends

Privacy+ Security Forum

Cyber Incident Reporting - US

Privacy+ Security Forum

- Insurance companies are required to report material cyber incidents for an increasing number of states that have adopted a version of the NAIC Data Security Model Law.
  - While versions of the Model Law vary in the 21 states that have adopted it, in general incidents must be reported to the chief insurance regulatory official of the state within 72 of determining a qualifying incident occurred.
- Banking organizations are required to report computer security incidents to their primary federal regulator.
  - Effective May 2022, reporting must be within 36 hours of determining that the event has crossed the "notification incident" materiality threshold, meaning a computer-security incident that has or is reasonably likely to disrupt or degrade the banking organization's business lines or ability to carry out operations.
- Defense contractors are required to report qualifying cyber incidents to the DOD within 72 hours of discovery of the incident (DFAR 252.204-7012(c)).

Cyber Incident Reporting Statutes – Global Trends

Privacy+ Security Forum

Cyber Incident Reporting – Global

Privacy+ Security Forum

- In May 2022, the Council and the European Parliament agreed on NIS 2.0, which expands the organizations that are subject to the law and reduces the timeline for reporting to the relevant authorities from 72 hours to 24 hours.
  - Requires notice to the relevant competent authority and, where applicable, their customers of "any significant cyber threat" that "could have potentially resulted" in a substantial disruption or loss.
- India's CERT-In issued Directions in April 2022 imposing a strict 6-hour reporting window for cybersecurity incidents.
  - Broadly applying to most businesses operating in India, the new directions doubled the types of incidents for which reporting is required.
  - Reporting does not trigger on severity or actual impact to data, networks, or systems, but on being brought to notice about the incident.

Cyber Incident Reporting for Critical Infrastructure Act of 2022

Privacy+ Security Forum

Cyber Incident Reporting for Critical Infrastructure Act Of 2022 (CIRCIA)

Privacy+ Security Forum

- **Who?** "Critical infrastructure," as defined by subsequent CISA rulemaking.
- **What?** Report "covered cyber incidents" and ransom payments to DHS-CISA.
- **When?** "Covered cyber incidents" within 72 hours of when a covered entity "reasonably believes" a covered cyber incident occurred. Ransom payments with 24 hours of payment.

CIRCIA: Covered Cyber Incident Defined

Subsequent CISA rulemaking will define "covered cyber incident," to include at a minimum the occurrence of:

i. a cyber incident that leads to **substantial loss of confidentiality, integrity, or availability** of such information system or network, or a **serious impact on the safety and resiliency** of operational systems and processes;

ii. a disruption of business or industrial operations, including due to a denial of service attack, ransomware attack, or exploitation of a zero day vulnerability, or

iii. unauthorized access or disruption of business or industrial operations due to . . . a **compromise of a cloud service provider**, managed service provider, or other third-party data hosting provider **or by a supply chain compromise**;

CIRCIA: When Does a Corporation "Reasonably Believe" a Cyber Incident Occurred?

Privacy+ Security Forum

"A covered entity that experiences a covered cyber incident shall report the covered cyber incident to the Agency not later than 72 hours after the covered entity **reasonably believes** that the covered cyber incident has occurred."

CIRCIA: Content Requirements for "Cyber Incident" Reporting

- Content requirements will be further defined by CISA Rulemaking.
- But reports must include, where available and applicable:
  - A description of the covered incident
  - A description of the **vulnerabilities exploited** and the **security defenses that were in place**, as well as the **tactics, techniques, and procedures** used to perpetrate the covered cyber incident
  - Any identifying or contact information related to each actor reasonably believed to be responsible for such cyber incident
  - The **category or categories of information** that were, or are reasonably believed to have been, subject to unauthorized access or acquisition.

CIRCIA: Content Requirements for Reporting Ransom Payments

Privacy+ Security Forum

Reporting of ransom payments will include, at a minimum, where available and applicable:

- A description of the attack, including estimated date range of the attack
- A description of the **vulnerabilities, tactics, techniques, and procedures** used to perpetrate the ransomware attack
- Any identifying or contact information related to each actor reasonably believed to be responsible for the ransomware attack
- The name and other information that clearly identifies the covered entity that made the ransom payment or on whose behalf the payment was made
- Contact information for the covered entity or an authorized agent of the entity
- The date of the ransom payment
- The ransom payment demand, including the type of virtual currency or other commodity requested
- The ransom payment instructions
- The amount of the ransom payment

*Reporting of ransom payments would be required even if the ransomware attack is not a covered cyber incident under the law.

Privilege and Liability Protections

- A Federal, State, local, or Tribal government shall not use information about a covered cyber incident or ransom payment obtained **solely through** reporting [under this Act] to regulate, including through an enforcement action, the activities of the covered entity….”

- Reports describing covered cyber incidents or ransom payments submitted to the Agency are exempt from FOIA disclosure, **do not break privilege**, and are not subject to ex parte communications rules.

Privilege and Liability Protections
(continued)

(c)(3) no report submitted to the Agency pursuant to this subtitle **or any communication, document, material, or other record, created for the sole purpose of preparing, drafting, or submitting such report**, may be received in evidence, subject to discovery, or otherwise used in any trial, hearing, or other proceeding in or before any court, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, provided that nothing in this subtitle shall create a defense to discovery or otherwise affect the discovery of any communication, document, material, or other record **not created for the sole purpose of preparing, drafting, or submitting such report**.

How Should You Prepare for CIRCIA?

Privacy+ Security Forum

- ✓ Review existing lists of critical infrastructure entities and analyze whether your organization might be covered.
- ✓ Review/update incident response plans to:
  - ✓ Implement escalation procedures to ensure that legal is informed of potential covered breaches immediately
  - ✓ Confirm that legal will decide when a reportable breach has occurred
  - ✓ Craft CISA reports cautiously with an eye towards lawsuits and regulatory investigations
  - ✓ Establish separate CISA reporting workstream to maximize use of new privilege

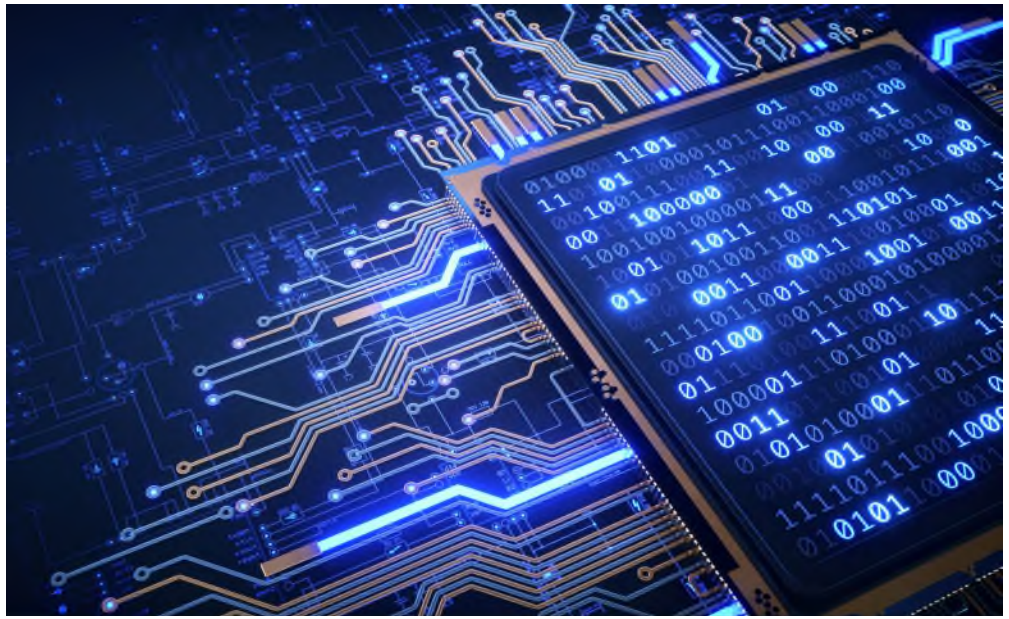
Practical Tips

Privacy+ Security Forum

Practical Tips to Address the Evolving Reporting Landscape

Privacy+ Security Forum

- Track the global landscape and educate your company of trends in cyber incident reporting, not just reporting of data breaches
- Develop global compliance programs.
  - What countries do you operate in, and what breach and incident reporting laws are you subject to?
- Incident response planning and testing.
  - In addition to maintaining a plan, the plan needs to be tested at the operational and executive levels.
- Review/update agreements with third party response partners given developing privilege case law.
- Consider engaging vendors doing cybersecurity training or review under privilege.



Questions and Contacts

Kim Peretti

Partner and Chair, Privacy Cyber & Data Security
Alston & Bird

Edi Goodman

International Privacy Lead Counsel
TransUnion

Nick Barnaby

Deputy General Counsel and Assistance Corporate Security
General Dynamics

Marie Dukes

Chief Global Employment & Data Privacy Counsel
FMC Corporation