BCLP. Client Intelligent

Insights

NAVIGATING A SECURITY INCIDENT - COMMUNICATION "DOS" AND "DON'TS"

Sep 12, 2024

Communication during a data breach is challenging in the best of circumstances, and control of information, especially early in a breach response, is critical. Below are some DOs and DON'Ts for communicating during a data breach. If you have any questions about this guidance or other issues relating to incident response preparation, please do not hesitate to contact our team.

The security incident response process inevitably brings a myriad of challenges for a company unfortunate enough to experience one. Although implementing an appropriate communication strategy may not be at the top of the list of the initial concerns for a company in the throes of a ransomware attack or other type of security incident, it should be. Appropriate communication discipline will help protect attorney-client privilege and similar legal protections and mitigate the significant risks (legal, reputational, financial) associated with the unintended disclosure of incident-related communications.

With this in mind, we have included below a set of *Communication Dos and Don'ts* to help companies approach this aspect of the incident response process. To implement the Dos and Don'ts, we recommend that companies work these principles into their Incident Response Plan and disseminate them to the incident response team at the outset of every incident response effort. It will also be important to remind internal teams and external service providers that while copying internal or external legal counsel on communications, as well as designating materials as subject to Attorney-Client Privilege and/or designating materials as "Work Product", are important steps, doing so will not automatically create relevant legal privileges. Moreover, there is always the risk that communications may inadvertently be sent to the wrong recipients and/or acquired either as part of the legal process or by the bad actors themselves. Therefore, thinking carefully about the content and manner of dissemination is essential in mitigating the inevitable fall-out from a security incident and moving forward as quickly as possible.

Communication Dos and Don'ts

1. **DO** communicate via telephone where possible.

2. **DO** include a Project Name (e.g., “Project Yellow: Notification Content”) in all emails and other written communications.

    - In certain situations, a communication may need to go to a smaller group. In those instances, the remaining Dos and Don’ts should still be followed.

3. **DO** mark any emails concerning legal opinion, legal analysis, litigation strategy and risk as “Privileged and Confidential” and include designated counsel (internal and/or external counsel) on all such communications.

4. **DO** designate emails as “private.”

5. **DO** limit email content to factual and/or objective information, when possible. If an email communication contains work product or content subject to the attorney-client or legal professional privilege, do not forward it to anyone outside of the original distribution list.

6. **DO** assume that any written communication might ultimately be discoverable or made public at some point (i.e., White Board Test).

7. **DO** segregate written communications in a separate, designated (protected) location and maintain communications in accordance with any litigation hold instructions.

8. **DO** start a new email thread and be mindful of the necessary recipients of information contained in the email. Send the email to only those with a need to know the information and confirm the recipient list before hitting send.

9. **DO NOT** include subjective conclusions/assessments (e.g., “this was a big mistake,” “our systems were not adequately protected”) in email communications.

10. **DO NOT** circulate forensics or other reports via email, particularly in draft form. Reports should be reviewed using a screen sharing application or similar means, and any dissemination via email or otherwise should be done only when the report has been finalized and at the direction of counsel.

11. **DO NOT** communicate about the incident via other unofficial means (e.g., texts, instant messaging, other non-company communication applications), unless the nature of the incident mandates use of an approved secondary communication method.

12. **DO NOT** destroy or delete any written communications related to the incident until receiving specific instructions to do so.

13. **DO NOT** forward email communications.

14. **DO NOT** continue to use the same email thread for new topics and avoid reflexive “reply all” responses.

15. **DO NOT** mix legal and business advice; use separate communications.

When in doubt, pick up the phone and obtain input from either your internal or external legal counsel prior to sending a written communication. Communication is a key and integral component of a strong response to incidents and having and following your protocol provides a mechanism for rapidly notifying stakeholders, coordinating internal and external stakeholders, monitoring customer or employee sentiment, and minimizing reputational damage, all while protecting your company's interest and legal privileges.

For more information about this topic or about how BCLP can help assist you with incident response and preparedness (i.e., tabletop exercises), please contact Amy de La Lama, Christian Auty or Daniel Rockey.

RELATED CAPABILITIES

- Data Privacy & Security

MEET THE TEAM

Amy de La Lama

Boulder

amy.delalama@bclplaw.com
+1 303 417 8535

Christian M. Auty

Chicago

christian.auty@bclplaw.com
+1 312 602 5144

Daniel T. Rockey

San Francisco

daniel.rockey@bclplaw.com
+1 415 268 1986