

A Checklist for Cyber Incident Response Communications

WRITTEN BY

Sadia Mirza | Karla Ballesteros | Whitney L. Shephard

Published in [Law360](#) on July 14, 2023. © Copyright 2023, Portfolio Media, Inc., publisher of Law360. Reprinted here with permission.

Popular file transfer tool MOVEit's recent [data security vulnerability](#) prompted many businesses to communicate, internally and externally, about the impact of the incident on its business.

Businesses from various industries — including insurance, finance, government, health care, education, professional services, media and entertainment, and software providers — adopted different messaging approaches in terms of timing, transparency and content.

This serves as a reminder that there is no one-size-fits-all approach to incident response communications.

While there is no single strategy that will work for all businesses or all incidents, there are certain questions that every business should ask before communicating about an incident.

These questions, when considered, help ensure that any messaging will not further expose the organization to legal and business risks, and instead improve the narrative around its response.

Is the timing right?

When dealing with a security incident, it is good to consider the story that will be told about the business's response.

One storyline that is often favorable is that the business notified affected individuals or customers as soon as possible.

With that said, organizations need to balance the need, or desire, to quickly inform affected parties of the incident with ensuring that there is enough information to answer the questions that will inherently come up.

These questions may include: What information was affected? What was the root cause? Has the incident been contained?

Thus, in certain circumstances, the ideal situation may be providing notice only after the investigation is complete.

Businesses, however, may not always have the luxury to wait, as certain situations may warrant notice sooner. For example, if the incident has already been published in the media, or customers are aware that services are down or have been affected, a business may be forced to address the incident head on, even while the investigation is ongoing.

Likewise, there may be contractual or legal notification obligations that trigger a notification requirement. Or, as with the MOVEit incident, businesses may need to notify third parties because there is a need to take immediate action — e.g., patch a zero-day vulnerability.

Regardless of when the business decides to notify, it needs to keep its story in mind. Companies should be prepared to explain their timeline from the discovery of the incident up to the point of notification.

One narrative to consider, which arguably aligns with breach notification laws, is that providing notice too soon — when there was not enough information about the nature or scope of the incident — would cause unnecessary panic and result in overnotification. Thus, the business took its time to conduct a reasonable investigation to ensure it understood the incident instead of rushing to provide notice.

Alternatively, when notice is provided at the onset of an incident, a business should use that fact to its advantage.

While there may be challenging conversations to be had about the incident at that time, the business will ultimately be able to walk away saying that it provided notice as quickly as possible in the interest of being transparent and forthcoming.

Has the business prepared for the follow-up?

Assume the company has decided to provide notice of the incident. Has it, however, thought through the follow-up?

Businesses should read their messaging through the eyes of consumers, customers and regulators. What questions would they ask, and what communication protocol can the business implement to address them now?

If notice is being provided during an ongoing investigation, it is likely there will be questions relating to containment and ongoing risk. For example, customers may question whether it is safe to resume business with the organization during an ongoing investigation.

Businesses should consider what assurances they can provide if the question comes up, and what can be done from a containment perspective to mitigate these concerns.

A layered-notice approach is one strategy to consider when notice is provided during an ongoing investigation. This strategy offers initial, high-level information about the incident suitable for a broader audience.

For consumers or customers with specific follow-up questions, a second notice is prepared in advance, providing

additional factual details. By having a second notice ready to go, businesses can quickly respond to any follow-up, allowing them to focus their efforts on where it is most needed — the ongoing investigation.

The second notice also provides the added benefit of making consumers and customers feel that businesses are being transparent about the incident, or that they are part of the solution.

If notice is being provided once the investigation is complete, consumers and customers may ask specific questions about the impact of the incident on their data and the resources that are being offered to assist.

This is typically when businesses will create FAQs and line up a dedicated call center to answer common questions. There should also be an established escalation plan — including escalation contact — to address those questions that were not covered by the FAQs.

Is the messaging factual, and does it avoid speculation?

As with forensic reports, messaging during incident response should be factual.

Businesses should avoid providing opinions or speculating as to the impact of the incident or its root cause, especially when an incident is still under investigation.

Often, speculation results in businesses needing to correct prior statements made. This keeps the incident fresh in consumers and customers' minds, making it difficult for the company to move past it.

While a company wants to minimize the impact of the incident, it is important the company does not describe the incident in a manner that would deter affected parties from taking certain precautionary steps.

For example, even if the business conducted dark web monitoring to ensure that data has not been leaked, this should not be stated in a way to suggest that there is no need to sign up for any credit monitoring being offered.

Ultimately, affected parties should always be encouraged to take steps to protect their data, and it should be up to them to decide whether there is no risk based on the facts, not opinions, provided.

Does the messaging provide sufficient context?

A central goal of messaging should be to minimize the impact of the incident on the business.

To help achieve that goal, a business should provide adequate context to any message. What constitutes sufficient context will of course depend on the specific situation, but there are certain questions a business can consider to help ensure the message provides sufficient context.

One question to consider is: Where did the incident occur?

Suppose the business is providing notice about an incident that affected one of its third-party service providers. In that case, explaining the relationship between the business and that third party is imperative.

Otherwise, message recipients may ignore the message, wrongly assuming it does not apply to them because they have never done business with that third party or fail to focus on the message contents. They will instead be too focused on trying to understand how the business and third party are related, or why the third party has their personal information.

Another question to consider is whether to explain the type of incident. Explaining to the message recipients the type of incident — a phishing campaign, a fraudulent wire transfer, a ransomware event — can help manage the recipients' expectations.

Knowing that the business fell victim to a phishing campaign during which an unauthorized party accessed the business's email environment to send out phishing links will likely elicit a different response than a message indicating that a business experienced a ransomware attack.

When relaying the nature of the incident, however, businesses should consider the demographics of their audience, including their ages and locale. For less technically savvy audiences, avoiding legal or technical jargon is important to ensure the message does not get lost in translation.

Businesses should also consider whether additional context is needed to explain any calls to action. For example, if a company asks customers to apply patches to their software, providing context as to why the patch is needed may be critical to ensure customers follow through quickly.

Likewise, if a company recommended individuals change their passwords for accounts unrelated to its system, explaining the concept of "password reuse" may quell consumers' fear of how far spread the impact of the incident is.

Can the business take additional steps to minimize potential risks and concerns?

Many businesses tend to wait until their investigation is finished before suggesting protective and preventive measures.

However, it may be beneficial to consider taking action or providing support during the investigation to reduce the negative impact of the incident on the company.

One scenario where this may be prudent is when an organization experiences a ransomware attack, and the business suspects that employee information has been affected. In such a scenario, offering employees and their dependents family credit monitoring while the incident investigation is ongoing may allay, if not altogether quell, employee concerns.

Consider also when an organization learns it has been the victim of wire fraud. The initial impulse may be to remain silent and only notify other businesses if those businesses sent payment to the fraudulent account.

It may behoove a business, however, to let all its customers know, while the investigation is pending, not to send any wire payments without first confirming the correct account information. Doing so may prevent another organization from sending payment to the wrong address.

Has the business considered the audience?

The above questions are important to consider before issuing any message about an incident.

While the focus has primarily been on the message itself — the timing, transparency and content — it is equally important to consider the intended, and unintended, recipients of the message.

If messaging internally, consider how employees will respond to the message. Are they likely to keep the information confidential, or is there a chance that it may be shared with a broader audience?

The answer to this question may dictate how much information is shared about the incident and when.

If messaging externally, consider how customers and clients will respond. Is the customer likely to be understanding and receptive to the situation? Or is it possible the customer will cease business operations until their demands are satisfied?

The answers to these questions may vary depending on the sophistication level of a company's customers. It may be prudent to prepare specific communications for the VIP customers who require more hand-holding than others.

It is important to keep in mind that if notice is given, the media may become involved. Therefore, it is essential to have a media statement prepared in advance that aligns with other communication efforts as part of a comprehensive communication strategy.

Lastly, keep in mind that a company's messages may be reviewed by regulators and plaintiffs lawyers at some point. It's important to review messages with this in mind to ensure that even well-intentioned statements won't be used against a company in the event of litigation or an investigation.

Kamran Salour, a partner and co-chair of the data privacy and cybersecurity practice at Lewis Brisbois Bisgaard & Smith LLP, co-authored this article.

RELATED INDUSTRIES + PRACTICES

- [Data + Privacy](#)
- [Privacy + Cyber](#)