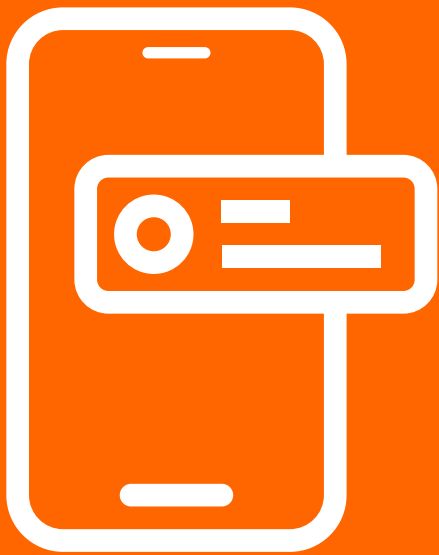


# When a Leaked Chat Becomes the Crisis



## In crisis, communication matters. It matters a lot.

When communication fails, so does crisis response. That not only goes for external communications to the press and public, but also for internal communications within crisis teams.


But while many teams understand the value of external communication, practitioners tend to feel that their teams still underestimate the value of internal communication to crisis<sup>i</sup>.

Perhaps, the problem is teams resist thinking of crises as extended events. But the fact is before the trigger event, there are usually warning signs to be read, identified, and disseminated among team members, especially during the following two stages:

- 1 Signal detection.**  
When warning signs are identified and acted upon to prevent crisis.
- 2 Probing and prevention.**  
When teams are searching known crisis risk factors and working to reduce potential harm<sup>ii</sup>.







At these stages, in particular, crisis teams will often exchange clues, hunches, and premonitions in an informal manner. They often do so via software like chat, which has surged in popularity, not just in crisis management but also in the culture more broadly.

Case in point: three quarters of mobile users now prefer instant messaging over other forms of communication, like email<sup>iii</sup>. The free messaging services, WhatsApp, WeChat, and Facebook Messenger, each command around a billion active users, spread out across advanced and emerging markets alike<sup>iv</sup>.

 **3/4** of mobile users now prefer instant messaging over other of communication, like email.

 The free messaging services each command around **1b** active users, spread out across advanced & emerging markets alike.

Chat has also rocked the enterprise space. From Slack to Chatter to Yammer to Microsoft Teams to Facebook at Work, dedicated enterprise chat services are also flourishing<sup>v</sup>. The trend towards the mass adoption of chat and instant messaging shows no end in sight. And that's in part because the business benefits of chat are so evident; whether teams are using WhatsApp or Slack, chat can:

-  Encourage interactivity
-  Boost collaboration
-  Foster openness
-  Help build up team support
-  Inspire connectedness
-  Remove the perception of hierarchy

However, it would be a mistake to suggest that team chat has been an unalloyed good for businesses. Some of the polling data has been mixed: 40 percent of respondents to a Chartered Institute of Personnel and Development survey in the U.K., for instance, said that chat services like WhatsApp actually undermine corporate culture<sup>vi</sup>.

Besides corroding corporate culture, the predominance of online chat in business has had other downsides. These unintended consequences are especially relevant for crisis teams reliant on the efficient flow of information before, during, and after crisis.

For one, chat makes even office gossip public and searchable for anyone who knows where to find it. Furthermore, the popularity of online chat has, in many respects, made it harder for crisis teams to handle internal communications efficiently, already a serious problem in critical issues and crisis management<sup>vii</sup>.

For crisis teams, the answer isn't clamping down on information sources, like chat. An outright ban would only hurt crisis decision making. Instead, teams should routinize the way information flows at every stage of the crisis lifecycle. And that means being fully aware of the ways chat disrupt efficient information flows:



#### Teams are overloaded with information.

The volume of chat and chat services are increasing apace. Too much chat on too many chat streams, without even factoring email and paper logs, simply overwhelms crisis practitioners, especially during an active crisis.



#### Relevant information gets ignored.

The fact that we conduct so many disparate conversations on so many disparate chat services only increases the chance that valuable pieces of information won't be adequately considered or even seen at all.



#### Sensitive data is leaked.

Here's the kicker. Plenty of chat services, especially the free ones, fall short when it comes to maintaining enterprise-grade privacy and security standards<sup>viii</sup>. That means that private conversations over them are liable to be hacked and leaked. Those conversations about critical issues often include senior stakeholders at an organization. And when their informal, out-of-context chats are leaked, those chats can trigger major reputational crises.



**Plenty of chat services, especially the free ones, fall short when it comes to maintaining enterprise-grade privacy & security standards.**



The New York Times's Opinion Section is perhaps the paper's most iconic property. In February of this year, Bari Weiss, a new contributor to the section, landed herself in hot water for what some saw as a culturally insensitive Tweet. While controversy raged on social media, management at the Times sought to show a united front. It was largely successful until a private Slack conversation, featuring a number of rank-and-file Times employees leaked to the media. In it, the employees criticize Weiss's original tweet, management's inadequate response to it, and the paper's lack of resolve to uphold its own diversity standards<sup>ix</sup>.



In 2016, a Rhode Island-based high school teacher was hacked. In the compromised account were the private Slack chats of fellow instructors. And in those leaked chats, teachers can be read bashing students and parents. After the leaked chats surfaced, several teachers were forced to resign in disgrace<sup>x</sup>.



WhatsApp has seen its share of leaks, especially as politicians around the world turn to the free service to communicate confidentially with their staffs and colleagues. Although the communications themselves are meant to remain private, many have eventually leaked to the press. Last year, for instance, U.K. Foreign Secretary, Boris Johnson, saw that his private message of support for embattled Prime Minister, Theresa May, was leaked to the press<sup>xi</sup>. Another government official, Labor MP, Lucy Powell, had to formally apologize after she inadvertently sent an angry WhatsApp message to the wrong WhatsApp group, containing a group of fellow parliamentarians<sup>xii</sup>.

The wide popularity of chat suggests that crisis leaders won't be able to simply turn back time to the pre-chat era.

And given how chat can actually enable quick collaboration and foster more open communication within crisis teams, crisis leaders shouldn't be so quick to tamp down on the practice either.

## Should chat be more accountable in the enterprise?

Crisis leaders can (and should) do a lot more to regulate relevant chat streams, with the aim of facilitating the efficient flow of information and mitigating the potential for leaks over unsecured services.

Enterprise chat is not a new concept, Yammer, the “Facebook for the Enterprise,” was launched a decade ago. Also, Hangouts is pervasive in organizations who use the Google suite of enterprise products. The temptation is very much still there for teams to bypass their procurement or IT procedures and use unsanctioned chat tools.

Falling into the temptation of using unsanctioned chat tools can be a dangerous thing, as they can prove a slippery slope towards further, unsanctioned critical issues and crisis processes. Fortunately, crisis teams can achieve the goals of expediting information flows and mitigating leaks with critical issues and crisis management technology that integrates chat functionality within the service itself. If teams need help finding the right solution, they should consider the following:



### Messages should be deletable.

When it comes to protecting sensitive data, always ensure that integrated chat comes with a feature which would allow you to turn off chat history.



### Multiple layers of security.

Crisis leaders should find a service that is secure at both the mobile app and infrastructure levels. Remember, standards and certifications matter here. For instance, the latest standard in transport layer security – that’s what provides communications security, privacy, and data integrity over a network – is TLSv1.2.



### Data centers should also be in compliance.

In this day and age, plenty of technology vendors have migrated to the cloud, and that means your sensitive data is now more likely to be housed in data centers. So make sure your critical issues and crisis management vendor’s data centers are certified to ISO27001 and fully complying with the legal and regulatory strictures of the region they’re in.

Of course, it helps if crisis chat can be blended with more structured information in a secure environment related to the crisis information flow. That’s because maintaining a secure record of chat can be extremely valuable when trying to understand the chronology of events for a post incident report.

By now, it’s clear that chat can help boost productivity and increase collaboration on your crisis team. But when unsanctioned chat tools are used in the enterprise, they can just as easily get you into trouble, lots of trouble; that is unless you integrate chat within a secure, critical issues and crisis management solution.



## Citations

- i Dr. W. Timothy Coombs, *Institute for Public Relations: Crisis Management and Communications*. Available at <https://instituteforpr.org/crisis-management-communications/>.
- ii Crisis lifecycle stages identified by crisis management specialist, Ian Mitroff.
- iii Dmytro Brovkin, *Medium: How To Develop a Chat App Like Whatsapp*. Available at <https://medium.com/swlh/how-to-develop-a-chat-app-like-whatsapp-e695257320f4>.
- iv Facebook, who by the way owns WhatsApp, reports that it has nearly as many active users on its Messenger product as does WhatsApp.
- v Alex Wilhelm and Ron Miller, *Tech Crunch: The great enterprise chat race*. Available at <https://techcrunch.com/2017/03/18/the-great-enterprise-chat-race/>.
- vi Emma Jacobs, *Financial Times: The perils of using WhatsApp at work*. Available at <https://www.ft.com/content/4fbf6c18-a501-11e7-b797-b61809486fe2>.
- vii In Denmark, for instance, researchers found that only 31 percent of organizations had crisis communication policies for their internal audiences. Dr. W. Timothy Coombs, *Institute for Public Relations: Crisis Management and Communications*. Available at <https://instituteforpr.org/crisis-management-communications/>.
- viii Examples include: Telegram, Amazon, WhatsApp, and Android messenger.
- ix Ashley Feinberg, *HuffPost: Leaked Chat Transcripts: New York Times Employees Are Pissed About Bari Weiss*. Available at [https://www.huffingtonpost.com/entry/new-york-times-diversity-bari-weiss-tweet\\_us\\_5a833d4ee4b0cf06751f3f44](https://www.huffingtonpost.com/entry/new-york-times-diversity-bari-weiss-tweet_us_5a833d4ee4b0cf06751f3f44).
- x Sarah Larimer, *The Washington Post: Teachers insulted students in private Slack chats*. Available at [https://www.washingtonpost.com/news/education/wp/2016/06/24/teachers-insulted-students-in-private-slack-chats-after-a-hack-they-resigned-in-disgrace/?nid&utm\\_term=.067bbb2618ef](https://www.washingtonpost.com/news/education/wp/2016/06/24/teachers-insulted-students-in-private-slack-chats-after-a-hack-they-resigned-in-disgrace/?nid&utm_term=.067bbb2618ef).
- xi Jessica Elgot, *The Guardian: WhatsApp: the go-to messaging tool for parliamentary plotting*. Available at <https://www.theguardian.com/politics/2017/jun/12/whatsapp-the-go-to-tool-for-parliamentary-plotting>.
- xii John Ashmore, *Politics Home: Labour MP apologises after 'bollocks position' WhatsApp message*. Available at <https://www.politicshome.com/news/uk/political-parties/labour-party/news/82828/labour-mp-apologises-after-bollocks-position>.

Like what you read?  
Follow Noggin on social media



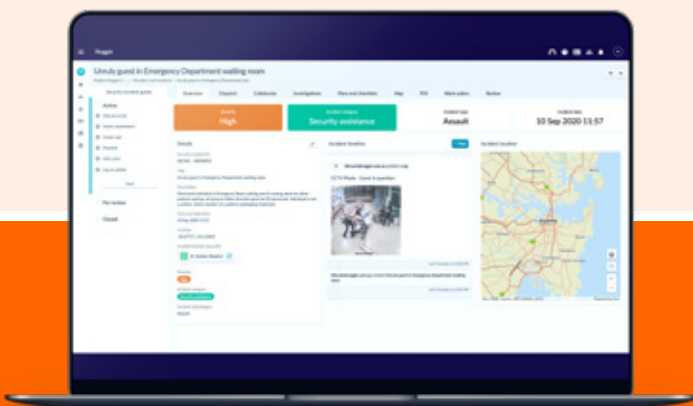
@teamnoggin



facebook.com/teamnoggin



linkedin.com/company/noggin-it



# noggin

for Crisis

Meet the next-generation tool for corporate crisis and business continuity management teams to collaborate, plan, track their response, and share information. Built on the Noggin Core platform, Noggin Crisis gives response teams and decision makers the tools to know what's happening, collaborate quickly and effectively, make better decisions, and enact the right plans to take action when it counts the most.

The Noggin Crisis solution pack is backed by the Noggin Library with hundreds of plans and best-practice workflows, out of the box, and installed in minutes.

To learn more,  
visit: [www.noggin.io](http://www.noggin.io)  
or contact: [sales@noggin.io](mailto:sales@noggin.io)