n|u

null - The Open Security Community

Guidelines for communications in a data breach response

Security and privacy discussions have moved from the backroom to the boardroom in the organizations. Data breaches and privacy incidents now regularly make headlines in the news. These are becoming the focal point for social media discussions worldwide.

Failure to communicate with all stakeholders on these critical issues can damage business by damaging market reputation, losing stock value, eroding customer trust.

We at null – The Open Security Community have analyzed a few data breaches and their crisis communication plan and made an extensive list of guidelines for organizations to minimize and plan for this risk.

If a data breach occurs, get your crisis communication team together with top-level executives from management and legal, security, IT and any other relevant departments, and hold a meeting to establish what you know.

1. Communicate

Communicate directly, not only through the media but also with the affected customers. Setting up a particular website or an easily accessible page on your current company website gives customers and journalists a location to obtain accurate information and your official response.

Use simplified language to communicate: Cybersecurity is full of technical jargons. Simple and straightforward language is best to speak with the public and journalists.

Few questions to ask when preparing a data breach communication plan:

- Who are the stakeholders that need to be informed of a breach? (customers, employees, investors, media, law enforcement)
- How is the communication going to be different for each stakeholder?
- Who is involved in the data breach communications program?
- How will customers be notified of the breach [channels of communication: email, SMS text, Newspaper Ad, etc.]?
- Who will manage to educate internal stakeholders and employees on the details of the breach?
- Who is the public face/spokesperson for breach communication?
- How will legal concerns be balanced against reputational damage?

2. Pick a spokesperson

The best way to handle a breach is to step up to own the problem. A spokesperson for the company, they communicate to the media and customers. By taking responsibility for the violation, they look at the company and help regain customers' trust, minimizing reputation damage.

3. Be ethical, be responsible

Apologize for the inconvenience and disruption. Sincerely and without excuses. To regain trust, the best apologies include an indication of steps being taken to protect affected individuals, resolve the issue, and prevent further problems.

Promptly and honestly disclose what you know. If you're still searching for answers, say it.

4. Be specific

When they're not given enough detail, people tend to speculate. When disclosing an incident, say precisely what happened, how it affects customers and partners, and what you're doing about it.

5. Be ready with official statements

6. Equip and train your social and online media team with the situation

Link your official statements from your social media accounts. Equip your social media team with official, human, factual responses.

7. Keep all the stakeholders continuously informed evolving situation

In conclusion, effectively planned communication channels can assist in easing the operational, reputational risks imposed by data breaches and may even be critical in minimizing damage.

About null – The Open Security Community:

null is one of the most active, open security communities. Registered as a non-profit society in 2010. One of the main objectives for null is spreading information security awareness. In a calendar year, null chapters host about 100+ events across security domains and impact about 8000-10000 security professionals, enthusiasts, and beginners with their initiatives. null is open, professional, inclusive, responsible, and most importantly, completely volunteer-driven.