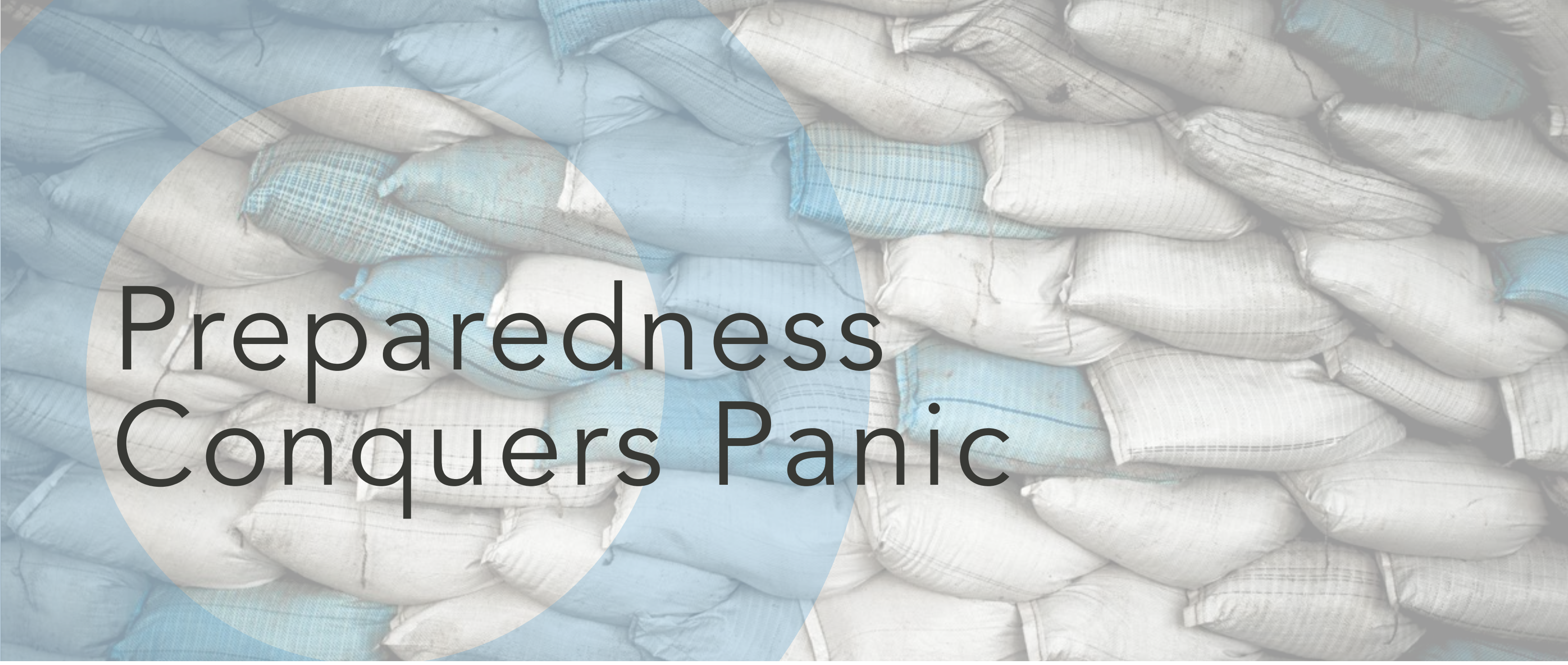

Preparedness Conquers Panic

KEY ISSUE:

The media widely sensationalizes the consequences of large data breaches, yet lacks a real focus on the role of incident management preparation. In the age of the "mega breach,"' organizations must concentrate on facilitating an effective strategy versus a last-minute reaction to help ensure that the media reports facts, not fiction.

In the past year, multiple companies have suffered a now common level of breach known as a **mega breach**, where the number of affected records surpasses 10 million.

- LinkedIn identified a mega breach of more than 117 million customer accounts in May 2016. Further review and investigation indicated the compromise actually began in early 2012. The outward facing company response was to force a mandatory password reset for the entire customer population. [3]
- Yahoo disclosed a mega breach of nearly half a billion user accounts in September 2016; updated disclosures later indicated the initial compromise occurred in late 2014. More recent reports show another separate breach of a billion user accounts in December 2016. [1,2]

The timing of this was unfortunate, as Yahoo was in the middle of acquisition negotiations with Verizon. [1,2]

When reviewing the parallels between these breaches, the media could have directed its response toward the preventative measures taken by these companies. Instead, the focus was based largely on wild speculation and victim shaming. In the absence of a planned, practiced and executed incident management strategy, speculation and sensational reporting take over the narrative. In today's competitive business climate, many organizations cannot afford to risk the chance of loss in consumer trust, reputational damage and the impact on value in the eyes of the shareholders due to this unconstrained media response.

CHALLENGES:

When the media gets the scent of a breach, their version of "how many, how bad and how expensive" can be detrimental to reputation. Consumers rarely see what preventative and protective measures the company had in place – only that something bad happened. The reason behind this is a combination of more and more companies reporting breaches, thus decreasing public sensitivity, and a continued escalating focus on negative coverage to draw clicks and views. In lieu of facts, the media seizes control of the narrative, leading to speculation of the worst-case scenario. This is truly the "failure to plan, is a plan to fail" scenario. By the time the victim company brings the facts to light, the public has already made up their minds based on pseudo-facts and hearsay of pundits.

There is still a significant amount of enterprises that have not developed and deployed an enterprise security incident management strategy. Companies have been focused on meeting increasingly complex compliance requirements. However, the race to acquire cyber insurance is prompting many to focus on their enterprise incident management programs as a precondition. Consequently, both of those examples make excellent business cases for developing an enterprise security incident management program and operational framework.

Now, perhaps more than ever, it is crucial for enterprises experiencing a breach to have a pragmatic, practiced security incident management plan. Don't let planning, training and testing with the various stakeholders of an incident management program take a back seat.

OPPORTUNITIES

Companies must learn to own the public narratives of their breaches and security incidents. With sufficient planning, preparedness and practice, this is possible. **Transparency matters. Timeliness matters. Facts matter.** Combat victim shaming by leveraging the facts. Though we cannot predict what the media will focus on, getting ahead of it during even the worst times provides customers and stakeholders with a clear and calm picture. For example, implementing an advanced media plan is a positive component to incident response planning by allowing a breach victim to focus on recovering, rather than scurrying to develop that plan on-the-fly. Focus on giving the power back to the victim organization to not only drive its own narrative when the time comes, but reassure its customers that information security is an enterprise priority.

Companies that appear disorganized and unprepared – such as waiting too long to notify customers and law enforcement during an investigation – are routinely the subject of attack and negative media coverage. Additionally, a lack of transparency adversely impacts trust with customers and business partners. The take away here is to have a planned approach to notifying customers and any appropriate parties to avoid these types of consequences and long term costs.

Shawn Tuma, a cyber security and data privacy partner at Scheef & Stone, LLP, describes the risk of not prioritizing incident response planning, especially about a company's media presence:

> *"Legal and public relations are crucial components of incident response. Two of the greatest harms that can befall companies following a data breach are to make mistakes that put them in legal jeopardy, such as making inaccurate statements that are later used against them in court, or mishandling how incidents are disclosed to the public and doing it in a way that jeopardizes the company's future business. It is almost always better for the company to be the one to make the initial disclosure rather than have the public find out from another source. The important thing for companies to learn now is that the key to their being able to handle these situations after a breach is to start planning ahead now."*

Prioritizing a programmatic approach to enterprise security incident management helps promote a strategic approach to enterprise defense. Developing a business-aligned enterprise incident management strategy and testing it in a simulated scenario helps facilitate a calm and cool reaction in the event of a real breach. It allows employees and stakeholders alike to understand not only the risk but the reaction – all of which help drive a calm and focused narrative in the media.

THE PATH FORWARD

"Not if, but when" is the new normal. Focus on a strategic effort to develop a game plan with leadership and the security team for incident management that includes communications and technical response.

- Advanced media planning is valuable because it gives the organization a chance to communicate its statement of investing in cyber security. It can also project calmness and order, deterring the media from potentially destructively embellishing a story.

- Work with legal and PR teams directly to promote cyber security for the organization. Training all key members of the incident response team can be the most important part of a proactive breach plan.

- Dedicate time to dissect current incident management program and processes. If one does not exist, capitalize on current resources and invest in a program-focused transformation.

CALL TO ACTION

Most organizations are aware of the targets and the techniques, so why haven't they modified how they operate? Guidance on how to calmly navigate through the data breach minefield can be the difference between simply surviving a data breach and thriving in the face of one. Preparation is key to taking control of the public narrative in the event of a breach. Organizations that take the time to strategize, prepare and practice project a more organized image to the public. This outward sense of calm and order minimizes the erosion of trust.

How prepared is your organization? Do you have a strategy? Do you practice response? Even if you do, take Optiv's free online self-assessment to determine your program maturity level. If you haven't thought about preparedness, Optiv can help.

MacKenzie Brown
Associate Research Principal
Solutions and Program Insight, Optiv

References:

1 Vindu Goel, http://www.nytimes.com/2016/10/19/technology/yahoo-says-traffic-rose-despite-hacking-that-could-alter-verizon-deal.html?_r=0

2 Hannah Kuchler, https://www.ft.com/content/dc044df6-956c-11e6-a1dc-bdf38d484582

3 Evan Schuman, http://www.computerworld.com/article/3077478/security/linkedin-s-disturbing-breach-notice.html

OPTIV

1125 17th Street, Suite 1700
Denver, CO 80202

800.574.0896 | www.optiv.com