melissaagnes.com

How to Develop a Cyber Security Crisis Management Plan

Melissa Agnes

9–11 minutes

I recently came across the below cyber security awareness video by Deloitte. This video is exceptionally well done. It watches like a thrilling trailer and is meant to get organizations thinking about their cyber security preparedness. Take a look:

Are you ready for a cyber security crisis?

Cyber security is a crisis scenario that is extremely top of mind these days – and rightfully so. Over the last few years, we've watched countless brands suffer cyber security incidents of mass destruction,

from Target to Ashley Madison, to the Panama Papers, and the list goes on.

The truth is that a cyber security incident is a crisis scenario that every organization is vulnerable to, which makes it one of the most important types of high-risk scenarios to include within your crisis preparedness program.

The trouble with cyber security crises is that they can occur in a multitude of different ways and detecting and assessing the scope and impact of an incident is often a challenging and time consuming process. However, just because it's a complex and multi-faceted type of crisis to prepare for, doesn't mean it can't be done. In fact, I've helped many organizations think through this risk and develop internal processes, protocols and a crisis management playbook that has provided them with an additional layer of protection and preparedness for this risk, which has proved to be highly beneficial.

If your organization hasn't yet done this, then it's time to start thinking about it. So to help get you

started, following are some helpful tips and considerations when setting out to become crisis-ready for a cyber security incident.

Step 1: Define the parameters of a cyber security crisis

The first step is to simply start at the beginning and define what a cyber security crisis is and means to your organization. As a high-level starting point, a cyber security incident can be defined as “a breach, compromise or disruption of the organization’s critical data and/or systems”.

Once you have this risk defined, you’ll need to determine how your organization – and the law – defines “critical data and systems”. For example, what types of data do you have access to and what are your most critical systems, whereby if either were breached, compromised or disrupted, it would present a crisis or potential crisis to your organization?

Step 2: Develop your internal escalation

process

Not every cyber security incident risks rising to crisis levels. In fact, depending on the size and nature of your business, your information security team probably detects issues and potential threats on a regular basis as part of their business as usual activities. So how do you determine whether or not a cyber security incident is a “business as usual issue” verses a potential crisis? Who will help your IT team make this determination and at what point do they get called in to do so?

A good way to approach this, in my experience, is to provide your IT team with a set of questions that they can answer as part of their initial assessment of any given incident. These questions should aim to help them assess the potential *business impact* of each incident. From there, I usually devise a protocol stating that if the IT team can answer “yes” or “maybe” to X amount of these questions, they are to escalate the incident to a dedicated cyber security assessment group. This group should include members of different departments that,

together, can assess the full potential impact of a given incident on the business and its stakeholders. From there, if this group deems the situation to be a potential crisis, the protocol should be to escalate the incident to senior management.

One of the main goals of this escalation process is to ensure that the right people have the tools they need to assess the full potential impact of a cyber security incident, while ensuring that as few “false alarms” as possible get escalated all the way up to senior management. It’s both an effective filtering process and a way to make sure that the right people are a part of the initial assessment process when needed.

Step 3: Understand the legal aspects of a cyber security crisis

One of the goals of crisis preparedness is to minimize the amount of tasks needed to be undertaken in the event of a crisis. This means that if there is work that can be done now that will prove to be beneficial to the team in the heat of the

moment, then that work should be outlined and completed.

As cyber security crises can come with a lot of legal obligations and ramifications, part of the preparedness process is to set out to understand your organization's legal responsibilities in the event of a breach. Depending on the jurisdiction(s) of where the incident happens, the type of data that gets compromised and the potential impact to your stakeholders, your organization will be subject to different legal requirements and timelines. It is your responsibility to understand and adhere to these requirements.

Even if you have a powerhouse of internal attorneys, it's a good idea to consult with outside counsel on this one. One advantage of doing this is that many of the big legal firms that provide this type of service to their clients already have most of the work done. For example, you'll find that many of them have created a matrix that details the different rules and laws within different jurisdictions, and that they're committed to keeping this

information current as laws change and evolve.

Equipping your team with the right third-party experts is an important part of being crisis-ready. In the event of a cyber security crisis, this list usually includes legal counsel, cyber forensic professionals, insurance providers and a specialized crisis management consultant.

Step 4: Draft your playbook and crisis communications handbook

I've written about this before *(read: 5 "must-include" items for your crisis management plan)*, so I won't go into too much detail here. But basically, the goal is to think through the required tasks and considerations for each member of your crisis team within the first 24-48 hours of a cyber security crisis. This should include task considerations, action items, contact lists, timelines and pre-approved crisis communications.

I find the best way to tackle drafting the pre-approved crisis communications for a complex crisis such as a cyber security incident, is to think

through the most likely types of scenarios that pertain to your organization and to draft talking points, stakeholder-specific written notifications and an FAQ to the most extent possible.

However, one of the challenges with this type of crisis is that you will have two main focuses when it comes to your crisis communications: one focus will be on relationship maintaining (in other words, trying not to lose the trust of your stakeholders), and the second will be your legally required notifications which are very case-specific. With these two focuses in mind, you can draft an outline of the different notifications you would want to use, including appropriate tone of voice and key message points, and then set parameters for guiding the flow and timelines for communicating with your stakeholders. This isn't an easy undertaking, but with the right help it's well worth the effort.

Step 5: Put your plan – and your team – to the test

Once you have your crisis preparedness program developed, it's important to test it. Testing the plan with a table top – or better yet, a crisis simulation – allows you to detect gaps and strengthen the plan before you actually need to put it to use. It also helps your team develop muscle memory and crisis management instincts that everybody will be very grateful to have in the event of a real crisis.

Remember: your plan is not complete unless it has been adequately tested. And you certainly don't want to test it in the midst of a breaking crisis.

Where to go from here

In my experience, cyber security is a high-risk crisis scenario that keeps many executives up at night. And while it's not a crisis scenario that you can ever fully prevent, there are ways to mitigate the long-term impact that this type of crisis threatens to have on your organization. Having the right IT structures and controls in place is the first step. But from there, you also want to think through and develop comprehensive crisis management

strategies and protocols for managing this type of crisis.

Do this work now and not only will you sleep easier at night, but you will be very grateful that you dedicated the time and resources to preparing for such an event when you find yourself in this type of compromised position – which is said to be a question of “when” rather than “if”.

Interested in hiring Melissa Agnes to speak to your team about cyber security crisis preparedness? Click here to learn more**.**

Author of *Crisis Ready: Building an Invincible Brand in an Uncertain World*, Melissa Agnes is a leading authority on crisis preparedness, reputation management, and brand protection. Agnes is a coveted keynote speaker, commentator, and advisor to some of today’s leading organizations faced with the greatest risks. Learn more about

Melissa and her work here.