



**GOVERNOR ERIC J. HOLCOMB'S
INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY**
302 West Washington Street, IGC-South, Room E208
Indianapolis, IN 46204

Author: Goldfarb, Joshua

Title: "20 Questions to Ask During a Real (or Manufactured) Security Crisis"

Website: darkreading.com

Organization: Dark Reading

Date: 03 July 2019

URL: [https://www.darkreading.com/vulnerabilities---threats/20-questions-to-ask-during-a-real-\(or-manufactured\)-security-crisis/a/d-id/1335079](https://www.darkreading.com/vulnerabilities---threats/20-questions-to-ask-during-a-real-(or-manufactured)-security-crisis/a/d-id/1335079)

Accessed: 21 Oct 2019

Synopsis: There are important lessons to be learned from a crisis, even the ones that are more fiction than fact.

I've heard the statement "society doesn't deal with problems until they become a crisis" many times. Unfortunately, this is often the case in information security, but it doesn't need to be this way. As security practitioners, we can't fix the ills of society. We can, however, learn how to distinguish a real security crisis from a manufactured one. Furthermore, from each crisis (real or manufactured) that we go through, we can learn how to avert them all together.

In this spirit, I offer 20 questions to ask during a real or manufactured security crisis.

20 Questions to Ask During a Real (or Manufactured) Security Crisis

Joshua Goldfarb Commentary

There are important lessons to be learned from a crisis, even the ones that are more fiction than fact.

I've heard the statement "society doesn't deal with problems until they become a crisis" many times. Unfortunately, this is often the case in information security, but it doesn't need to be this way. As security practitioners, we can't fix the ills of society. We can, however, learn how to distinguish a real security crisis from a manufactured one. Furthermore, from each crisis (real or manufactured) that we go through, we can learn how to avert them all together.

In this spirit, I offer 20 questions to ask during a real or manufactured security crisis.



Image Credit: DuMont Television/Rosen Studios. Public domain, via Wikimedia

1. What is the threat that the issue at hand poses? Regardless of the noise surrounding a given situation, you need to understand the actual threat you're dealing with. Conjecture and hype won't help. Rather, you need to objectively understand how the threat could manifest itself as a risk to the organization.

2. What is the organization's exposure to the threat? Once you understand the threat, you can evaluate your exposure to that threat. This needs to be done in order to fully understand the gravity of the situation.

3. What risk does this threat pose to the organization? Once you understand

the organization's exposure, you can assess the *risk* posed to the organization. This is where you really begin to understand how seriously to consider the threat and how aggressively to respond.

4. Is the hype surrounding this threat justified? Separating fact from fiction is important. If the facts support the hype surrounding a given threat, then it needs to be dealt with as such. However, if the facts tell a different story, it's time to spin this one down.

5. Does the hype surrounding the threat translate to a real risk for the organization? If the risk is real, then it's time to respond appropriately. That includes the communication necessary to keep the right stakeholders informed.

6. When did we first become aware of the issue? Were you just made aware of this, or have you been aware of it for quite some time? The difference is important. If you knew about a significant risk to the organization and didn't act on it or escalate appropriately, that's a fairly significant lapse in security.

7. Why wasn't this raised earlier? If there is a reason, it can be addressed as part of continual process improvement. If there is no reason, it's important to understand why.

8. Could we have avoided this issue? In many cases, issues can be avoided if risk assessment were done more proactively, or if the attack surface had been reduced significantly. Not in all cases, of course, but it's good to ask the question.

9. Why didn't we avoid this issue? Once you understand *how* you could have avoided an issue, you need to ask why you didn't.

10. Has any damage to the organization occurred? This is, of course, the quintessential question. If no damage occurred, you need to remediate the risk, learn from your mistakes, and be thankful. If damage has occurred, then you still need to remediate the risk, learn from your mistakes, and, of course, perform incident response.

11. What are the steps required to remediate the issue? If you need to respond and remediate, the first step is to map out the steps required to do so properly. Taking a few moments to get organized and ensure all bases are covered yields a higher-quality result and saves time down the line.

12. What are the lessons learned from this issue? After any issue is dealt with, lessons need to be extracted and studied. This allows the security organization to improve and mature.

13. Can we apply those lessons to avoid a similar situation in the future? Obviously, crisis mode is a last resort. If you can apply lessons learned, you can avoid making the same mistake.

14. What other potential crises might we encounter? Post-crisis is a great time to think outside of the box and do some analysis. Understanding what other pitfalls you may encounter allows you to mitigate those risks ahead of time and improve the security posture of the organization.

15. What else can we tighten up to avoid future issues? You may have

patched, tightened controls, or improved monitoring after the crisis, but what else can you do to keep from having to relive this or a similar experience?

16. How can we ensure that our remediation of the issue will be effective?

Your plan may sound good on paper, but to be more certain, map the technologies and applications the issue affects, then conduct a sanity check to see whether it will achieve your desired goals.

17. Have we verified that remediation was effective? If you've already remediated, have you tested to ensure that the remediation was effective? If not, you could be exposed to a recurrence.

18. What steps have we taken to avoid a similar situation in the future?

You need to ensure that whatever remediation you've done, whatever lessons you've learned, and whatever improvements you've made are lasting and not a one-time fix.

19. Have we precisely and effectively communicated actions to

management and executives? Regardless of whether or not you had a real crisis, whether or not you handled it appropriately, and whether or not you've made improvements to the security organization, your actions need to be documented and communicated to management and executives. This builds confidence in the security team's ability and avoids excessive spin-up when the next issue arises.

20. Have we taken steps to avoid future damage? In the end, it all comes down to whether or not you avoid or minimize damage to the organization. This is perhaps the hardest question to answer. But it is likely the most important.

Related Content:

- [Sensory Overload: Filtering Out Cybersecurity's Noise](#)
- [The Fine Line of Feedback: 6 Tips for Talking to Security Pros](#)
- [KISS, Cyber & the Humble but Nourishing Chickpea](#)



Black Hat USA returns to Las Vegas with hands-on technical Trainings, cutting-edge Briefings, Arsenal open-source tool demonstrations, top-tier security solutions, and service providers in the Business Hall. Click for information on the [conference](#) and [to register](#).

Josh (Twitter: @ananalytical) is an experienced information security leader who works with enterprises to mature and improve their enterprise security programs. Previously, Josh served as VP, CTO - Emerging Technologies at FireEye and as Chief Security Officer for ... [View Full Bio](#)

More Insights