Amii Barnard-Bahn
CW Columnist

Ask Amii mailbag

Amii Barnard-Bahn lays out four guidelines for tough conversations, and a guest expert weighs in on what to do if someone's holding your data hostage.

Breaking bad news to top brass

Q. I am a compliance department of one, and I'm afraid our company made some mistakes recently that I need to report. I haven't taken it to the board or the C-suite yet … what's the best way you have found to break bad news to important, powerful people? —Anonymous

Amii: How fortunate that your company has you to lead them through this compliance crisis. When breaking critical business news to the people who need to be looped in, it is imperative that you follow some important guidelines:

- **Give the headline first**—don't beat around the bush. Be clear and concise with the facts; Stick to what you know is true. It's OK not to have all the answers.
- **Allow venting.** Your leadership may be angry, disappointed, or anxious at the news. Provide support by showing gravitas—grace under pressure—and not turning away from any displays of emotion. It's not your job to try and make it better. If anger or blame is displayed, remember: it's not you that is causing these emotions—it's the bad news.
- **Help them move forward.** Tell them what they need to know, allow them to ask questions and propose next steps with a timeline. If they seem to be in denial and ignoring the gravity of the situation, outline consequences and impact of the situation.
- **Set a timeline for follow-up**—both for decisions on next steps and touch base meetings until the matter is resolved. Depending on the severity of the situation, consult outside experts (such as legal or regulatory counsel and PR).

Good luck and let me know how it goes.

Q. My company recently had a drill where we "experienced a cyber-attack": A group of "hackers" essentially froze our systems and demanded a "ransom" to get it back. We had a pretty good internal debate over whether to pay the ransom or not (I'm glad it wasn't a real-life scenario!). Where do you stand on a philosophical question like that? If systems critical to your business were shut down by hackers, would you ever consider paying a ransom? And across the industry is there a consensus on this question? —Anonymous

Amii: Excellent question. For this, I turned to my Hoya law school buddy, renowned data privacy and security expert Peter McLaughlin of Boston, who had this helpful advice to share:

Kudos to you and the team for having an incident response plan; practicing is such an important part of successfully dealing with the issues and stresses that invariably arise during a real event.

I'm not sure I'd worry about the philosophical question of whether it is "good" to make crime pay. I'd suggest an entirely practical approach: Precisely how much trouble are you in?

The questions you should initially focus on are: How recent are your backups and have those backups also been frozen? Which systems have been "frozen" and do you have a workaround? Have you a savvy cyber-security consultancy on call? And will your insurance help manage costs, including potentially the amount of any ransom payment?

These questions will help you assess how much of a bind you are in. If the "hackers" are less sophisticated and did not manage to also infect your backups, then the ransom question becomes moot. More sophisticated opponents will have been in your systems for some time, poking around in order to determine which files indeed are essential versus freezing the first database their ransomware happens upon. This is where your cyber-security consultancy is essential. The best of these firms can identify and unlock ransomware that may look impenetrable at first glance.

But let's assume the worst and address the not-quite-Shakespearian "to pay or not to pay." Your cy-

ber-advisors can help you with this decision. In particular, a good firm keeps track of which extortionists abide by some form of honor among thieves and will actually provide you the means to release your files. These cyber-advisor firms will often have pre-established cryptocurrency accounts (whether Bitcoin or some other currency) in order to facilitate payment. You should also speak with your insurer or your broker and see if your cyber-policy includes ransom payments.

While I agree that there is an interesting philosophical argument on whether to pay a ransom, you still have a business to run. Small- to medium-sized businesses are particularly at risk because they have not taken the preparatory steps of having an incident response plan, engaging a broker to help with a suitable package of insurance coverage, and making the time to practice that fire drill.

Q. We have a good compliance program on paper, but all we seem to do (and by "we" I mean the company) is pay it lip service. There are no consequences for missing compliance training, for example. Is the backing of senior management essential to making compliance more of a priority in practice (that's going to be tough to get), or is there a way to implement a truly effective program even if you're working against forces that might not see it as a high priority? —Tim

Amii: As you have implied, it is almost impossible to implement an effective compliance program without the backing of senior management. Most employees want to do the right thing—except when they don't. Organizational incentives—large and small, like the pressure to achieve tough sales quotas or get home on time to attend your kids' soccer game—can all be simple reasons people cut corners, which can lead to compliance issues.

Is there someone you can find that would be a sponsor for the compliance and ethics program? Perhaps it's not someone obvious. Perhaps it is your head of customer service or human resources. Take a step back and evaluate the business impact of a major reputation crisis on your organization.

In my prior work at an insurance company, the support of the head of claims was absolutely critical to gaining support for our very first compliance and ethics program at the company. He knew that the insurance industry had low trust as a whole, and he wanted our company to be the most highly trusted insurance company in the country. Happily, our general counsel agreed and the two of them spent a few years building a business case with the CEO and the rest of the C-Suite for a dedicated compliance and ethics program. It helped that we were able to tie compliance and ethics to increasing customer brand loyalty and retention.

Another option is to identify previous compliance failures in your industry. This is often a tried-and-true way to get senior management attention and to loosen up complacency. Use real examples in your marketplace, those demonstrating the value to the company of effectively managing threats to the achievement of business goals, shareholder value, company morale, and loss of competitive edge. Draw their attention to Facebook, Nissan, Theranos, and Wells Fargo, with particular focus on companies in your industry or with your risk profile. The more you can tie risk management to achievement of strategic objectives, the more likely you are to get deserved attention.

Q. Our compliance department has recently provided some training for our sales team that they've complained might lead them to miss some sales goals. I've taken it to management and they seem to be blowing it off, which is a problem. The way I see it, the way we want them to behave (ethically) is not lined up with how they are being incentivized (financially, on number of sales). How can I hammer home that message to bring about change? —Sherri

Amii: This is a difficult (and common) situation. I understand why you feel you need to use a hammer, but you're likely to get better results over time using softer influencing skills. If you only use a hammer, they will stop listening to you. You've got to build that relationship.

When sales incentives are not aligned with compliance and you need to build a case for change, you need to find a business sponsor who will champion this for you; it's tougher to go this alone.

If you truly have no organizational support, my advice would be to try to educate, educate, educate about why this is important and what the risks are of a major repetition fail due to legal or regulatory noncompliance. If there are any examples of competitors or others in your industry getting in trouble for the kinds of risks you're concerned about, use those as a case study to illustrate why they need to listen to you.

Express empathy for their sales goals. Remember this is the profit engine, and so it helps to appreciate the pressure sales people are under to deliver. Paint a vision of non-compliance. What could happen to the company, customers, and ultimately the sales person's job and reputation? People don't change unless they're uncomfortable with the status quo and inspired by a different future (or super scared of the consequences). ■

Looking for practical advice from a proven compliance leader?

Submit your questions for Amii at complianceweek.com/ask-amii-mailbag.