The Five Stages of Grief, the ARIAS•U.S. Guide to Data Security in Arbitrations, and You

A new guide to information security has some ARIAS members in denial, but many are accepting it.

By David Winters

In 1969, Swiss psychiatrist Elisabeth Kubler-Ross introduced a model identifying a set of five emotions experienced by people facing traumatic experiences. The so-called "five stages of grief" are: (1) denial, (2) anger, (3) bargaining, (4) depression, and (5) acceptance. The five stages of grief are not a linear series of emotional experiences; some people go through all of the stages in order, some experience only a few, and some experience none at all. The "five stages of grief" model was originally intended to describe emotions experienced by people anticipating a serious and traumatic future event. I've noticed that it is also common to see people experiencing the same emotions when dealing with information security issues.

The anticipated traumatic experiences relating to information security are twofold. First, there is the actual threat of a breach of confidential information, whether by hacking, a lost laptop, a rogue employee, or any number of threats that exist today. Second, and perhaps equally as concerning, there is the stress of mandatory compliance with the legal and regulatory regimes that require individuals and organizations to take particular steps to protect against breaches of confidential information.

Having been involved with efforts to improve information security in various different contexts, I can say that the most difficult challenge does not lie in figuring out what the ethical and regulatory regimes require, writing new rules and guidelines, or even ensuring that the proper structural protections are in place, but, rather, in selling the effort to the people within an organization. The difficulty of "selling" better information security is compounded by the emotional reactions of those people.

I've seen people go through the five stages of grief when dealing with any push to improve information security. One common reaction is denial—manifesting as a refusal to believe that information security requires the affected individual to do things differently

I've seen instances in organizations where people who were initially skeptics later professed to be happy about the focus on information security.

than previously. ("I don't work with personal health information, so none of this applies to me, right?") Anger is another common reaction—very common, in fact. It always amazed me how frequently people took offense at proposed new information security protocols. I have seen grown-ups resort to name-calling with respect to perfectly reasonable rule proposals ("That rule is stupid."), and I've seen people get annoyed at being told that they have to regularly change their passwords. Still others use bargaining as a coping mechanism. For example, I worked with an organization that mandated that a locking screen saver, which activated after five minutes, be installed on all employees' computers, and which required entry of the password to continue work. When the organization rolled out the new "locking" screen saver, one senior employee actually tried to negotiate that his screen saver would only lock after an hour. And yes, there is depression—I know, because I've experienced it. At my own law firm, I was part of a team charged with designing and implementing new information security protocols, and it was depressing to me that people seemed to like me less because I was associated with the those protocols.

The good news is that one generally sees an "acceptance" phase as well, and that shift happens relatively quickly. A few exceptional folks get there on day one, but most people do not. To be clear, no organization can ever "finish" the job of securing information—information security is a dynamic process that is ever-evolving as technology changes and new challenges arise. But once you have people on board with the concept of information security, facing future challenges becomes easier. I've seen instances in organizations where people who were initially skeptics later professed to be happy about the focus on information security and felt that learning more about information security and applying that knowledge was "the right thing to do."

The ARIAS•U.S. 'Guidance for Data Security in Arbitrations' and the Fall 2016 ARIAS•U.S. Conference

Now that I've talked about the five stages of grief, it's time to introduce the ARIAS•U.S. "Guidance for Data Security in Arbitrations." A draft version of the guidance and the broader topic of information security were among the focuses of the 2016 Fall ARIAS•U.S. Conference in New York.

The reaction to the guidanceat the Conference was not unusual. There was a small level of denial. ("Information security is only a problem for arbitrations that involve the exchange of personal information, right?") And there was anger. ("You propose to do what to the 'hold harmless' forms?") There was bargaining. ("Can't this problem be solved using internet deal rooms?") There was evidence of depression (but, again, this was mostly me). But most of all, and on a far more accelerated timetable than I have seen within other types of organizations, there was acceptance. I was struck by how most attendees, including arbitrators, outside counsel, and company representatives, understood that information security was something that needed to be addressed, that the problem was not going away, and that the best thing to do was to take reasonable and prudent steps to address the threat of confidential information.

The drafters of the "Guidance for Data Security," myself included, are particularly grateful for the insightful comments and suggestions for improvement offered by attendees at the conference. The revised document, which is posted on the ARIAS•U.S. website, incorporates those comments and suggestions. As Dan FitzMaurice stated in his article, "Cybersecurity and Data Security: What are the Risks for Insurance and Reinsurance Arbitration?," the document does not "dictate behaviors," but "offers many helpful suggestions for the parties and arbitrators to evaluate and possibly adopt."

You

It all comes back to you, of course. Whether you are an arbitrator, outside counsel, or a corporate representative, please review the "Guidance for Data Security." Think about the steps that you can take to improve information security in any arbitrations in which you are involved. Consider whether there are additional or different steps that might be required given the unique circumstances of any arbitrations in which you are involved. Be a skeptic if you must. Get angry if it helps. Bargain. Cry out in despair. But when you are done, accept that we must change with the times, read the document, and do your part to make arbitrations more secure. •