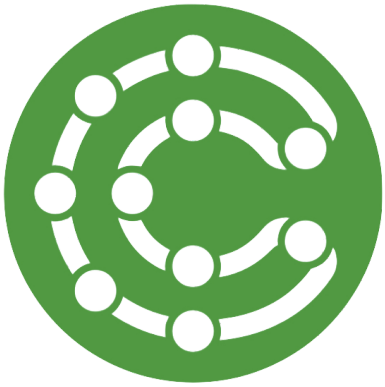

CISO TRACK

RSA 2020 Event

Session 4: Incident and Crisis Management

Problem Domain SME: Jen Ellis

(Sponsored by Rapid7)

Date: February 25th, 2020
Staff: Iftach Ian Amit and Chris Nickerson
Transcribed and Prepared by: Scott Lyons, MS.

CISO TRACK

Executive Session Summary

As Chief Information Security Officer (CISO), you may already have experience with crisis communication, have an incident plan in place, and have regularly practiced that plan; you've already thought about things like, "How do you build your plan? And how do you know what your legal requirements are? And, and how do you figure out stakeholder management and roles and responsibilities?" You may have a good relationship with your General Counsel (GC) and Legal team. As Jen points out in this panel, however, you might *not* have as strong of a relationship with the Head of Communications (Comms) or Marketing.

One of the biggest crisis communication issues that CISOs can encounter is the question about roles and responsibilities: Is it your job to figure out how to communicate in a crisis, or to present things to the Board all teed up for action and with a bow on top? Are you involved in the customer communication aspects, internal stakeholder management piece, external communications (press/social), or some combination across these three buckets? What is your role, "what are your responsibilities; where do they begin and end?"

One CISO reported feeling like their job was tied to the "three envelopes" and being able to get information from the employee whose actions led to the incident at hand so that they can communicate, to their "CEO, in language that they understand,

> What we think has happened, what are we doing to identify (and address) 'Why?' and what things do we need to do to try to ensure that this doesn't happen again (or, if it does, [what to do so that] it's less of an impact to the business and our brand reputation)?"

Another participant agreed:

> "As the CISO for my organization, I believe it's my role to 'translate' the technical ins and outs of an incident to the impact on our customers and the impact on our business so that our comms teams and that our internal folks can provide accurate, up-to-date information in non-intimidating, easy-to-understand way."

In addition to internal stakeholder management with an upward focus (i.e., informing executive management, Board members) and external communications with the press/social and your customer base, Jen argues that crisis communications should include considerations for a fourth group: your general employee base. She argues:

> "You should never forget that they are your frontline; they are your army. If you don't arm them appropriately, they are your greatest potential liability. Because they will freak out. They will know that something's going on; they won't know how to

> interpret it, they'll start gossiping with each other. And that's a huge potential challenge."

This internal communications strategy will likely be broken into sections: there will be some level of communication for the entire internal audience (your workforce), and a different level of communication for the employees who are working/engaged with customers and prospects. This could mean working with the Communications Team, Human Resources, People Strategy, and other stakeholders associated with the incident (e.g., Security, Head of Products, Platform Delivery Leads) to develop internal memos and a list of Frequently Asked Questions. These FAQs can anticipate what customers, prospects, journalists, people on social media, and other concerned individuals might ask when they call in for information about the incident so that the "front line" knows how to handle these requests. While the appropriate response to these third parties is likely to have those requests directed to designated spokespeople, the employees taking those calls need to have enough knowledge and understanding that they aren't tempted to mutter under their breath that they don't know what's going on either, gossip with friends from other companies that, "Hey, something's blowing up here, and we're all going to get laid off," or otherwise jumping to crazy conclusions that can impact the public message you're trying to craft for your organization.

The crisis communications plan has to be adaptive: Jen compared it to fighting a fire, where your specific response will depend on the circumstances on the ground, regardless of the extensive training and preparation beforehand. When you're practicing your communications plan, it's not all about rehearsing a template; it's about building relationships, figuring out roles and responsibilities, making sure there isn't a misalignment in expectations regarding who "owns" a particular thing, and identifying each other's triggers - what do they care about, and why? When that comms plan has to be activated, not all of your team members may be immediately available, but if you know those triggers ahead of time then you can still proactively address the issues that concern them the most. It's very common to find out that different stakeholders will have strong, drastically different opinions on how a certain thing should be handled, particularly if they are focused on different types of risk. For example, the CISO's recommendations are based on security risks, the comms person's recommendations are intended to manage reputational risks, and the Head of Legal/ Data Protection Officer will make recommendations to manage legal risks, so they may all bash heads as a result.

Jen suggests that the CISO's role isn't just to manage security risks though; the CISO is also supposed to be the voice of the customer internally within your organization, giving advice by coming at the issue like, "'As a security professional, this is how this thing would affect me, and this is how I would want my vendor to behave towards me." If the CISO can give the comms people a baseline understanding of cybersecurity, including training on what really matters and how customers or prospects might view different issues, that makes it a lot easier for everyone to be on the same page; the comms people aren't living and breathing

cybersecurity and aren't immersed in that field the way the CISO and employees in a security company are.

Aligning these different inputs during the communications planning process will help ensure everyone is on the same page when it comes time to respond to an incident. Every compromise, data leak, and security incident will be heavily context-dependent and cannot be templated out in full. Some of these decisions will be guided by the company's values regarding transparency, including:

- **How much information do you give people?** Should it be highly-detailed, transparent communications that show every single step that was taken? Should it just cover the minimum legal requirements from the GC? Or should it be somewhere in the middle, where some pertinent information is relayed but we don't overwhelm them? And should this be across-the-board, or tailored to the specific recipient?
- **Should you contact individual customers directly, or put out a public notice?** If you know exactly who was affected, is it appropriate to just reach out to those individuals? Can you reserve public notice for situations where you don't know exactly who was affected and/or where the weight of communicating to each one individually is too high (e.g., if it's a large percentage)?
- **When is the right time to reach out?** If you ping customers every time you get an alert, you might just be wasting everyone's time. But if your press release is a few minutes late and a TechCrunch article goes out before you can make a statement, you can't contact each blog that picks it up and ask them to update their story.

As one CISO noted,

> "It's actually a triangle between timeliness, accuracy, and transparency. Because transparency doesn't necessarily help your customers; *accuracy* does. So when you have data and you're not 100% sure, or you see that there's still reason why it might change, sometimes transparency isn't a good thing. And it can be more important to just be accurate and timely, and then afterwards be more transparent after you complete the post mortem."

The response strategy will likely differ between Business-to-Business (B2B) and Business-to-Consumer (B2C) models: If your customers are other companies who have legal liabilities of their own (e.g., as data recipients), then you might have "aligned incentives" and will both want to handle things quickly and quietly. If you contact individual consumers about an incident and they turn around and post about that notification on social media, there may be greater public backlash as people might think that there's been a larger compromise than what actually occurred; it might be better to just go public so you can control the message.

It's important to know the audience: one CISO described an incident where they contacted a small group of professors within their university who had been targeted by a nation-state's phishing attack and gave them the basic information they needed (without compromising

an ongoing law enforcement investigation) and let them know that they needed to change their passwords; it didn't affect their loyalty to the university, they didn't need to panic, and they knew exactly what steps they needed to take. Another CISO described an incident where email addresses and passwords were leaked from a marketing press site and, by treating it as a "black-and-white" decision (full transparency) rather than "grayish" (just the basics) like they might have done with regular consumer notifications, the press didn't report on the incident as they might have if they viewed it as a potential scandal.

Well-executed, timely, transparent incident/breach notifications with sufficient detail can help build consumers' trust in a company. By demonstrating accountability throughout the crisis, the company shows how they recognize the responsibility that comes with that consumer trust, which can influence consumers' buying decisions moving forward.

However, detailed transparent notifications are not always a blessing, particularly if the message is perceived as tone-deaf. The example discussed was Facebook: why was it that Facebook's detailed report about Russian interference faced massive scrutiny while other platforms who faced similar levels of interference were able to hide? Jen suggested that this was likely a combination of two factors: (1) it wasn't presented as an industry-wide issue where the industry came out as a united front; this report was only about Facebook, and (2) Facebook is an organization that is perceived as having too much power and has previously faced a *lot* of criticism for being slow to respond, so it was pretty tone-deaf when their detailed report came across as very self-congratulatory — the *tone* in crisis communications can really affect how the messages are received.

Media response is another important factor; everyone is competing for clicks so there may be a tendency to throw people under the bus over botched notifications (because "negative stories sell more") rather than commending organizations who do have good response efforts. Jen highlighted that there are generally three groups who cover cybersecurity issues and companies' responses: (1) press who write the tech titles, are part of the tech community, and cover security every day; (2) the mainstream media who are trying to get clicks but don't cover security all the time; and (3) the bloggers from the security community who aren't reporters at all but have a very active social media presence. The first group, because security reporting is their bread-and-butter, are well aware of the issues that information security professionals face, recognize the odds of a breach, and are interested in seeing advances in security rather than beating up on people unnecessarily. If companies are taking responsibility and handling incidents in the right way, these tech reporters will cover the story "in the most minimal way possible"; but they *will* go after companies that are behaving "slimily" really hard because they genuinely care about security. The mainstream media, on the other hand, will play up the fear, uncertainty, and doubt (FUD) by putting out salacious stories that may be more hyperbolic since their audience isn't immersed in security every day. If the mainstream press notices that tech reporters are acting like it isn't a big deal then they might follow that cue. However, Jen pointed out that the security bloggers who like to pick apart press releases about response/recovery activities "can often be the most harmful" since they're "the ones who create all of that social media

hysteria and who provide the comments that then get picked up by those mainstream press that are looking for the negative angle." Jen suggested that CISOs could work with their press teams to navigate security reporting, such as guide them towards tech reporters with reliable coverage and away from reporters who don't seem to understand the issues or have misquoted them previously.

A large part of crisis communications is figuring out how to de-escalate: when you cause a problem, be the first person to raise your hand; you call out the issue - "I caused it" - and give specifics as soon as possible.. If your organization's culture and values incorporate that type of accountability and transparency, it can help people understand what's going on and empathize, and can de-escalate because it shows you're doing the right thing for your clients.