expel™

Aug 24, 2017 | Bruce Potter

A cheat sheet for managing your next security incident

Surviving the unexpected.

On the face of it, security is pretty straightforward. We're operating in one of two modes. In Mode A we're focused on keeping evildoers at bay (and other generally bad things from happening). In Mode B the bad things have happened and we're doing the best we can to manage them. For most people A > B. But we don't get to choose when the bad guys show up.

When they *do*, we're often out of practice because we have so much less experience *responding* to attacks than we do *preparing* for them. In a perfect world, there's a comprehensive incident response plan that involves legal, communications, the board, and technical response processes. In an even more perfect world, you've put that plan through a table-top exercise, refined it based on your learnings, and drilled it to the point of muscle memory.

But few of us live in that perfect world.

That's OK. All is not lost. If you haven't yet got that perfect incident plan in place you can still make the best of a bad situation and manage your organization back on level ground. Here are six things I recommend.

1. Control your emotions and the velocity

First and foremost, it's important not to freak out. Your job is to manage the incident in front of you and return the organization to "normal." Letting your emotions get the better of you will just get in the way of reaching that goal. It may be difficult to settle your emotions, but there are ways to help. First, **get organized by putting a set of facts and tasks together to help you focus on the event at hand rather than the emotions surrounding it.** Also, take care of yourself. Eat. Rest. Don't be afraid to take a step back (or a walk around the block) once in a while. It will help you maintain perspective and control your emotions.

Pace of response is also important. You need to drive response activities but – like Icarus – you'll only be successful if you stay away from the extremes. Move too fast and you'll have wasted work, missed opportunities and poor decisions that could make you look like the Keystone Cops. Move too slowly, and you'll jeopardize the integrity of your organization as attackers continue to have access and do damage. There's no

clear rule of thumb here, but as each meeting goes by and each day passes, make sure you're thinking about the velocity of activities and adjust tasking appropriately.

2. Build a team and assign roles

You can't respond to an incident all by yourself. No matter how big or small your organization is, you need help. **Build a team that's appropriate for the response and assign everyone discrete roles.** Without roles, you'll have people stepping on each other's toes and gaps where there should be work. You'll want to engage legal, communications, key executives, IT leaders and technical staff. Make sure each person knows what they're expected to do, the level of effort and the need for confidentiality.

But be careful. Don't bring in too many people – especially if you're dealing with an insider incident. Controlling information gets harder as more people get involved. So, think carefully about who you involve when insiders are involved.

3. Communication is key

Regular meetings are important to keep everyone on the same page. You'll be bringing together individuals from across the organization. They don't normally work together and they won't be familiar with each other's communication styles or skills. By meeting at least once or twice a day, you'll **help the team integrate rapidly and ensure your response activity doesn't suffer from lack of information sharing.**

And while internal communication is critical, make sure you're also looking beyond your own four walls to your customers, vendors, board, and the public at large. Controlling the message while an incident is unfolding is difficult. And it shouldn't be your responsibility – not just because you're busy, but because you are probably not good at it. Being transparent but also communicating facts externally in a way that is consistent with your brand is complicated. Educate your communications staff about the incident and hold them accountable to message with the appropriate parties.

4. Don't jump to conclusions

Nothing is worse than a public statement about an incident that later has to be completely changed because an organization made an assumption during an incident that turns out to be false. I was once pulled away from a vacation with my family because my corporate website was "under attack" according to our network operations center. We spent half a day working with that hypothesis, trying to shore up our DDoS defenses and control traffic. When we actually stepped back and looked at the facts, we discovered our marketing department had launched a new ad campaign without telling IT. It was swamping us with new users. Within a few minutes, we contacted marketing and had them turn the dial down to levels our infrastructure could handle.

Deal with the facts you have, not the facts you want or the assumptions you brought to the table. Jumping to conclusions without sufficient facts damages your creditability with stakeholders. More important, it can lead to poor assignment of resources and cause greater harm to your organization as attackers are allowed continued room to operate.

5. Save the post-mortem for the actual "post"

While you're figuring out "what" happened, it's often easy to drift into thinking about "why" it happened. Assigning blame and tracking down the root cause of an incident may seem like a good idea, but it can inflame emotions and distract you from the task at hand. If you see your teammates diving into the "why" of the

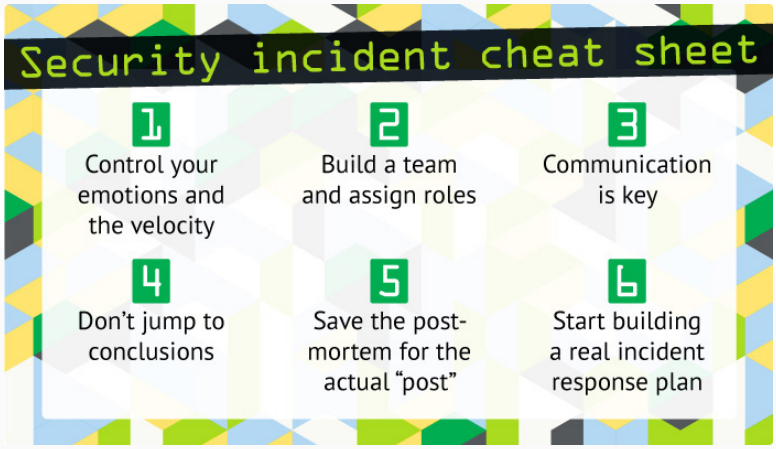
incident, remind them that the team will do a post-mortem after the incident and ask them to stay focused on their tasking. Usually, the promise of the post-mortem is enough to keep things on track.

Then, **once the incident is resolved, make sure you actually do the post-mortem analysis.** Addressing the root cause of an event is important to the long-term integrity of your organization. Give everyone a few days to rest and deal with their normal job functions, but try to have a post-mortem meeting within a week after the event.

6. Start building a real incident response plan

When the dust has settled, sit down with all your notes, emails, and random facts. Marvel that you were able to deal with such a complex situation with nothing but your wits and your skills. And vow to never, ever do it like that again. **Creating a solid incident response plan will ensure that when things go wrong again** (and they will go wrong) **that your organization is better prepared to deal with the event.**

Did you notice something? None of these recommendations are overly technical. In my experience, when incident response goes wrong it's not because there wasn't competent technical staff. It's because there was no clear leadership for the staff to follow.



So today, while you're still working on your full incident response plan (and before anything bad has happened) let me offer a three-minute plan and a three-hour plan that will leave you better prepared to manage your organization the next time you face an incident.

> **If you've only got three minutes:** get your phone out, make a list of the people across the organization that you'll need to work with if an incident happens and make sure you have them on speed dial.
>
> **If you've got three hours go a step further:** set up meetings with each of them and tell them what their role would be if an incident ever arises.

Trust me, the time you spend doing this will be paid back tenfold when that time is most valuable – during your next incident.

--

Visit the EXE blog for more articles like this at https://expel.io/blog