Collection

Users can Collect posts into a printable, sortable format. Collections are a good way to organize posts for quick reading. A Collection must be created to tag posts. More Help

Thread:	Handling Security Incidents	**Posted Date:**	October 6, 2019 10:21 PM
Post:	RE: Handling Security Incidents	**Status:**	Published
Author:	**LEAH DREW**	**Overall Rating:**	

Ron,

Personally I think it's extremely important to be cautious about who to seek help from. It's unlikely that an outside entity like that would be truly malicious, but they don't always have good security and might be more vulnerable to threats than your business is. If you're not careful, you might put your own organization at risk of suffering the consequences of an attack on the outside entity you trusted. Especially if you've given them access to your network or another direct way at getting at your information. You always should try to make conscious decisions before an incident even happens.

(Post is Read)

Thread:	Addressing Outside Entities	**Posted Date:**	October 6, 2019 10:08 PM
Post:	RE: Addressing Outside Entities	**Status:**	Published
Author:	**LEAH DREW**	**Overall Rating:**	

Jourdain,

I agree with you and Emeralde that contacting the vendor of the software to get a security hole patched is a good idea. It's interesting to hear a personal story about it too.

I also think it was beneficial to Microsoft that someone eventually decided to contact them, not just to your company. By telling them about a problem in their software you're not just protecting yourselves, you're also protecting them and anyone else who might have been affected by it. I also think the policy of contacting them within 1-2 days is crucial because as long as a hole is left open, there's a chance of someone malicious taking advantage of it.

(Post is Read)

Thread: Communication with Outside Entities		**Posted Date:**	October 6, 2019 9:46 PM
Post: Communication with Outside Entities		**Status:**	Published
Author:	**LEAH DREW**	**Overall Rating:**	

When a cybersecurity incident occurs, it's usually beneficial to communicate with certain outside parties. According to our reading, many organizations never contact law enforcement after an incident, resulting in the perpetrator never being caught and punished. Often this isn't because of neglect, but because the organization doesn't understand the proper procedures for contacting law enforcement, or even who to contact. Incident response teams should be taught who to contact and how before an incident happens, not after. The organization also should contact any other parties that may have been involved or affected by the incident. A concern when doing this is accidentally leaking private information to these outside parties who don't need this information. This can also happen when discussing the incident with the media, so the incident response team should be trained on how to communicate with them and what information should and shouldn't be given away.

When constructing an incident response team, many organizations may choose to partially or fully outsource, usually due to not having enough qualified employees. According to an article published by Infosec titled "The Advantages & Disadvantages of Outsourcing Incident Response," one major disadvantage of doing this is that allowing an outside entity to perform incident response functions gives that entity access to sensitive information. This means that if the entity suffers an attack, not only will they be affected, but the organization that outsourced may be too. When deciding whether or not to outsource, an organization should always take into account the reliability of the entity providing the service.

(Post is Read)

← **OK**