Team: Team 3

Inject Number: 32

Inject Duration: 60 Minutes

Inject Start Date/Time: Sat, 24 Mar 2018 10:38:19 -0500

From: Chief Information Officer

To: Infrastructure Team

Subject: [F-230] Update Incident Response Policy

Our legal team and internal auditors have reviewed the Incident Response policy recently created and found some minor deficiencies as well as one major gap. While the minor deficiencies can be addressed at a later time, the major gap requires immediate action. Under the notification section of the policy, the review determined that a detailed subsection on proper mechanisms in communicating the incident with media, law enforcement, internet service providers, partners, and customers is critical. Apparently, there have been past mis-steps in these areas during a prior incidents and they insist we document a process that prevents similar mistakes and legal ramifications.

Provide an updated version of the policy with the updates in a different font color from the original incidence response plan. The additions must address the handling of those five external organizations: media, law enforcement, internet service providers, partners, and customers. It must also discuss the following:

1) who is authorized to speak with the external organization, if that requires higher approval, who provides that approval
2) when is the communication to take place
3) what components can be included (this gets to what details can be shared - who, what, why, when, how, where)
4) what mechanisms are used for communication
5) preparation/training for this section of the policy

References - NIST 800-61 (particularly section 2.3.4)

Thank you.

Chief Information Officer