Eight steps to a stronger cybersecurity strategy

November 9 2018, by Meredith Somers

Credit: CC0 Public Domain

If there's an attack on the country, the military mobilizes. When a natural disaster strikes, recovery plans go into effect. Should an infectious disease start to spread, health officials launch a containment strategy.

Response plans are critical to recovery in emergency situations, but when it comes to cybersecurity, a majority of industries are not paying

attention.

"The reality is no matter how amazing you are with your prevention capabilities, you're going to be hacked," said Mohammad Jalali, a research faculty member at MIT Sloan whose work is currently focused on public health and organizational cybersecurity. "Then what are you going to do? Do you already have a good response plan in place that is continuously updated? And communication channels are defined, and stakeholder responsibilities are defined? Typically the answer in most organizations is no."

To help address cybersecurity weaknesses in organizations, Jalali and fellow researchers Bethany Russell, Sabina Razak, and William Gordon, built an eight aggregated response strategies framework. They call it EARS.

Jalali and his team reviewed 13 journal articles involving cybersecurity and health care to develop EARS. While the cases are related to health care organizations, the strategies can apply to a variety of industries.

The EARS framework is divided into two halves: pre-incident and post-incident.

Pre-incident:

1—Construction of an incident response plan: This plan should include steps for detection, investigation, containment, eradication, and recovery.

"One of the common weaknesses that organizations have is they put together an incident response plan, but the problem is that documentation is usually very generic, it's not specific to the organization," Jalali said. "There is no clear, specific, actionable list of

items."

Make sure that everyone in the organization knows the plan, not just the employees in the IT department. Set clear channels of communication, and when assigning responsibilities, make sure they are clearly defined.

2—Construction of an information security policy to act as a deterrent: Clearly defined security steps establish and encourage compliance.

"Many companies think that compliance is security," Jalali said. "[That] if you just follow the information you'll be taken care of."

Don't set the bar so low that the organization is not secure. Regulations should ensure an understanding of cyber threats. Establish motivational reasons for the response teams to follow reporting policies. Compliance should go hand in hand with continuous improvement.

3—Involvement of key personnel within the organization: No matter the size of an organization, key leaders need to be educated on the importance of cybersecurity and be ready to act according to the response plan.

Leaders don't have to be cybersecurity experts, but they need to understand the impact an incident will have on their organization. The more informed they are, the more involved they can be in a response plan.

4—Regular mock testing of recovery plans: Recovery exercises help organizations stress-test plans and train employees on proper response protocols.

If the organization only tests its recovery plan during an actual emergency, it's likely to run into serious issues, which could increase the

amount of damage caused by the cyber incident.

The shift from a reactive to proactive stance can help an organization identify weaknesses or gaps in its recovery plan, and address them before an incident occurs.

Post-incident:

5—Containment of the incident: Containment involves both proactive and reactive measures.

It's easier to cut off infected devices from a network if they're already segmented from other devices and connections, prior to an incident.

The researchers concede that it's not always possible to segment networks, nor to immediately disconnect it from the whole system. At the very least, immediately report the infected device to the organization's IT team to contain the incident.

6—Embedded ethics and involvement of others beyond the organization: It's important to remember that all of an organization's stakeholders could be impacted by a cyber incident.

Promptly notify legal counsel and relevant regulatory and law enforcement agencies. Consider help from external resources and share information about the cyber threat.

7—Investigation and documentation of the incident: Be timely and thorough; every step of the pre- and post-incident reaction should be documented.

The investigation should aim to find the root technical cause of the issue, as well as weaknesses that could prevent future attacks. Proper

documentation is a necessity for this analysis.

8—Construction of a damage assessment and recovery algorithm: Organizations should self-evaluate after the incident.

While computers are where cyberattacks happen, they can also be used to help with recovery. Organizations can leverage the power of computers, especially artificial intelligence, for real-time detection and containment of incidents.

"The commonly used frameworks for incident response strategies often miss this essential step," Jalali said, "even though there are already AI-based products for this very purpose."

Provided by MIT Sloan School of Management

Citation: Eight steps to a stronger cybersecurity strategy (2018, November 9) retrieved 20 June 2024 from https://phys.org/news/2018-11-stronger-cybersecurity-strategy.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.