THE EXPERTS | LEADERSHIP

Why Companies Need to Start Sharing More Information About Cyberattacks

Details on how long an organization was impacted and what it did to recover could be among the most helpful details that companies reveal

New regulations are being proposed or enacted in the U.S. and elsewhere to increase the quality and quantity of cyberattack reporting..

PHOTO: GETTY IMAGES/ISTOCKPHOTO

By

Stuart Madnick Follow

Sept. 8, 2022 1:00 pm ET

Stuart Madnick is the John Norris Maguire Professor of Information Technologies, Emeritus, at the MIT Sloan School of Management and the founding director of the Cybersecurity at MIT Sloan (CAMS) research consortium.

***

It's conventional wisdom that cyberattacks are a big and growing problem for institutions. But here's the truth about that conventional wisdom: We really have no idea

how big the problem is. We don't know how many attacks take place in any given day, month or year. And we don't know who is being attacked.

That's because until recently the only cyberattacks that had to be reported were those involving the theft of personal information such as names and credit-card numbers. People may be surprised to learn that before the ransomware attack on Colonial Pipeline in 2021, which shut down a big portion of fuel deliveries to the U.S. East Coast, pipeline operators weren't required to report breaches to any authority.

It has become clear that through laws or regulations, we need to increase the quantity, quality and timeliness of cyberattack reporting. Only by having more detailed information on who is getting attacked, how they are getting attacked and what is being stolen can everybody begin to arm themselves with the right defenses.

WSJ

To that end, there are various new regulations being proposed or enacted in the U.S. by the White House, Congress, state governments and agencies such as the Securities and Exchange Commission, as well as by authorities around the world, to increase the quantity and quality of cyberattack reporting.

Here is a look at the types of cyber-attack information that would be most helpful to reveal and why. Obviously, the faster organizations report data on cyber incidents the better, but the timing will depend on what information is being reported. For example, the date that an incident is discovered is immediately known, but the date the organization fully recovers from the incident could be many weeks away.

Types of Attacks: Cyberattacks can range from personal information being exposed, to money being stolen, to computer systems being held hostage due to ransomware. Knowing the types of attacks that are being launched can help organizations better prepare for what is likely coming their way. This information is usually known rather quickly by the impacted company.

Methods Used: This kind of detailed information is crucial for organizations that want to be ready for an attack. For example, how did the intruder get into your system? Was it due to a link in a phishing email that some employee clicked on, or was it due to a known vulnerability in your system that hadn't been patched. In most cases, there are multiple steps that an intruder must go through to complete the crime. Sharing this information will help other companies identify their own vulnerabilities.

Impact: For many reasons, but especially for shareholders, it's important that organizations quantify the impact of the attack on their business. Were normal business operations disrupted or actual money lost, such as through ransom payment? Shareholders require transparency, and hiding significant business impact only reduces the trust between shareholders and management.

Current Status and Recovery Methods: In many ways, what may be of most value to other companies is what can be learned about how to recover as rapidly and thoroughly as possible. Often the news about a cyberattack drops from the headlines quickly. But learning how long the organization was impacted and the methods that were used to recover from the disruption could be of great value in preparing other companies to be more resilient in the face of a cyberattack.

Increasing the amount and quality of cyberattack reports would be one of the most effective ways to improve the cybersecurity of our organizations. The cybercriminals do a great job in sharing information on the Dark Web. The "good guys" (that is, us) need to get to be at least as good.

Write to Dr. Madnick at reports@wsj.com.

MORE IN EXPERTS

- Four Traps to Avoid After Getting Promoted
- What Top Executives Can Learn From Their Junior Employees
- It's Time to Change the Cybersecurity Metaphors We Use
- Why Small Cybersecurity Decisions Can Expose Companies to Cyberattacks
- How Small Businesses Can Tell If They're Underpricing Their Offerings