Avoiding the Cybersecurity Chopping Block

Can You Mitigate Your Company's Security Risks Before an Attack?

BY LORI S. NUGENT

BIGSTOCK

IF IT WERE EASY TO AVOID CYBERSECURITY incidents like data breaches and ransomware attacks, most organizations happily would apply whatever the solution and protect the sensitive information in their care. Unfortunately, no solution to protect data from all attacks exists, and it is unlikely that such a solution can be developed. When one form of attack is thwarted, attackers develop new forms of attack. An attacker only has to succeed once to gain access to an organization's data, but an organization trying to protect its data needs to beat every attack 365 days every year. Inevitably, at some point in time, an attacker will find a way to beat an organization's best efforts to protect its data.

A significant cybersecurity incident is a tipping point. An organization that is facing a significant cybersecurity incident may never be the same again. This situation creates an opportunity to weather the storm well, which may enhance the organization's reputation because its good character is highly visible. If handled poorly, however, the cybersecurity incident may damage the organization's reputation.

WHEN A CYBERSECURITY INCIDENT HAPPENS STAKEHOLDERS WANT ANSWERS

When an organization is significantly impacted by a cybersecurity incident, stakeholders and regulators want answers. They want to know what happened, why it happened and what is being done to keep it from happening again. A spotlight is brought to bear on everything that the organization did or did not do that contributed to the cybersecurity incident. Regulatory investigations often follow significant incidents, as does class action litigation asserting that the organization did not reasonably protect the data in its care, and that its board breached its fiduciary duty before and during the breach.

As answers are provided to a variety of internal and external stakeholders, executives and board members may face a lack of confidence from disgruntled stakeholders. When a cybersecurity incident erodes confidence, change may be sought both within the executive team and at the board level. For example, it has been widely reported that, in the aftermath of the Target breach, its CEO and CIO resigned, and shareholders were encouraged to replace board members (but ultimately retained the board members).

PRACTICAL WAYS TO RESPOND WELL WHEN A CYBERSECURITY INCIDENT HAPPENS

Executives and board members can prepare now, so that they are better able to retain others' confidence when a significant cybersecurity incident happens. There are several steps that can be taken to prepare to respond confidently and well when a serious cybersecurity incident happens. The three steps discussed below provide a good starting point. Taking these steps will help executives and board members highlight the reasonableness of the organization's actions and inspire confidence when the inevitable cybersecurity situation happens.

1. UNDERSTAND YOUR ORGANIZATION'S CYBERSECURITY RISKS

Each organization is different. Network architecture, software and hardware choices vary significantly, even among organizations of similar size in a specific industry sector. Additionally, the amount of legally protected data that is gathered, stored and retained varies. Take some time before an incident happens to understand your organization's unique cybersecurity posture. What are your organization's risks and what mitigation steps are taken? It is hard to inspire confidence if you don't know what data is collected, why it is collected, and what happens to it from the time it is collected until it is decommissioned and no longer accessible.

2. DETERMINE WHAT SECURITY IS REASONABLE FOR YOUR ORGANIZATION

The only way to avoid a cyber attack on data kept in your system is to disconnect the data from any system connected to the internet. Since your organization likely needs to have its data readily accessible to authorized individuals, disconnecting the data from internet accessibility probably will not be a reasonable solution. What is the right balance between the legitimate business need to access data and the need to secure data from unauthorized use? How does your organization strike this balance? Why do the people responsible for the data's security believe that the organization's balance is prudent? How do the steps your organization takes compare to steps others take? To inspire confidence when a cybersecurity situation happens, you need to be comfortable with your organization's choices in balancing authorized access with securing data from attack.

MAKE SURE THAT YOUR ORGANIZATION HAS A WRITTEN INCIDENT RESPONSE PLAN THAT INCLUDES THE ENTIRE ENTERPRISE.

Keep in mind that, in the aftermath of a breach or other serious attack, the people analyzing the organization's choices will view the situation with 20/20 hindsight—they will know what happened and look for "obvious" things that could have been done to prevent the specific incident. Your decisions, however, will be taken without knowing which of the numerous attack vectors that are known, and those that may be developed in the near future, ultimately will succeed in accessing data in your organization's care. Taking steps now to ensure that you are able to explain the reasonableness of your organization's choices can make a meaningful impact on the outcome.

3. TEST YOUR ORGANIZATION'S RESPONSE PLAN

Make sure that your organization has a written incident response plan that includes the entire enterprise. Your IT team can structure the organization's systems to take reasonable steps to protect data, but a substantial portion of cybersecurity incidents happen because of human mistakes. Everyone in your organization needs to know how to protect data in their care and what to do when a cybersecurity incident may have happened. Make sure that you have a written plan and that it is tested—not just with IT. This will make it much easier to respond well, making it easier for you to inspire confidence when a serious cybersecurity incident happens.

Responding well to a significant cybersecurity incident depends on preparation. There are many steps that executives and board members can take to better prepare to respond confidently. Cybersecurity is complex, and responding well to a serious incident can be a minefield. Some of the best responsive steps in a live situation are counterintuitive, even to lawyers and technologists who are skilled in other areas. To ensure that your organization is prepared to respond well when a serious cybersecurity incident happens, make sure that you understand the choices that have been taken, and how your organization plans to respond.

The most important step to be prepared to respond well is the first one. Get started now, and find partners who can add their expertise to your organization's to help you respond well with confidence.

Lori S. Nugent is a shareholder with the Dallas office of Greenberg Traurig.