CARLTON FIELDS

Get Your House in Order: Four Steps to Take Now to Prepare for Ransomware

August 09, 2021

With ransomware attacks surging, companies should evaluate their cybersecurity posture and harden their defenses. This could include working with a third-party security firm to audit the company's security and then follow-up work to address any high-priority gaps. Apart from working with a security firm, there are myriad resources that could be consulted for this work, including the federal government's recently released website: StopRansomware.gov.

The work described above may help a company avoid becoming a victim in the first place. Of course, that is the best position for a company to be in. However, given the sophistication of attackers, this client alert highlights four other steps that can be taken now to help a company respond quickly and effectively should it nonetheless fall prey to a ransomware attack.

Know your data and where it resides.

Commonly referred to as "data mapping," this process involves understanding the company's data, the sensitivity of that data, and where it is stored. For example, does the company know on which servers it houses sensitive information regarding its customers? How about its employees? How about its contract partners? Is that data backed up and, if so, is the backup stored offline and separated from the main systems? In our experience, companies that have a handle on this information are better positioned to respond to a ransomware attack than companies that do not. For example, assume an attacker claims to have taken sensitive data from a specified server on a company's system. If the company knows that the particular server does not in fact house sensitive data, the company is in a better position to evaluate its bargaining position with the attacker and respond accordingly. That many state privacy laws also require a company to know the location and uses of its personal data is all the more reason to undertake a data mapping exercise now.

Develop an incident response plan, test it, and keep it updated.

An incident response plan is the company's "playbook" in the event of a ransomware attack or other cyber incident. The plan should list the team that will respond in the event of an attack (with updated contact information); the team members' respective roles and responsibilities; triage and escalation rules depending on the severity of the attack; and contact information for insurers, counsel, forensic advisers, and public relations professionals. Once the plan is drafted, the company should test it so that everyone is familiar with the plan and ready to act. The plan should be kept up to date, ideally through an annual revision process.

Develop contacts with law enforcement.

A company's counsel or internal security professionals may have relationships with the FBI, Secret Service, or local law enforcement, which should be fostered during "peacetime" to strengthen the company's crisis posture. As former federal cyber prosecutors, we have seen these relationships pay dividends in responding to an attack and even recover assets. The time to develop those relationships is before the company suffers an attack.

Evaluate your insurance program and work with your broker to address any gaps.

Depending on the incident, several insurance policies could be relevant, including cyber and fidelity/crime. Having a robust insurance program is helpful not only for the coverage it may provide but also because the underwriting process may itself help the company assess its cybersecurity posture and address any shortcomings. Also, many cyber policies provide access to or discounts on preferred advisers, including experienced outside counsel, forensic investigators, and public relations professionals, and it is important to understand these benefits before the compressed time frame of a ransomware attack or other cyber incident. If your usual broker contact is not conversant in cybersecurity insurance and its coverage options, request that your contact involve a cyber-product specialist within the brokerage, or consider working with a different insurance broker. Cybersecurity insurance plays a central role in mitigating the impacts of ransomware, and as a result, understanding its features is critical.

As recent events have shown, it may not be possible to eliminate all risk of a ransomware attack. But taking the steps outlined above should help companies ready themselves to respond to such an

attack.

Authored By

John E. Clabby

Related Practices

Cybersecurity and Privacy