ROPES & GRAY

ALERT

Privacy & Data Security

May 19, 2017

Don't WannaCry: Ten Questions Boards and Company Management Can Ask in the Wake of Recent Ransomware Attacks

Attorneys
Heather Egan Sussman
Deborah L. Gersh
Timothy M. McCrystal
Douglas H. Meal
James S. DeGraw
Seth C. Harrington
Mark P. Szpak
Michelle Visser
Elizabeth McCann
Jessica L. Alfano

The WannaCry ransomware attack that hit computers around the world last week is yet another reminder that computers play key roles in most enterprises, and that it does not take much to disable those computers. Questions remain about who was behind the WannaCry attack and whether it even was that sophisticated. But even the most robust of systems can be susceptible to attack, regardless of the attacker's level of sophistication. Here are ten questions that Boards and senior management can ask their information security and business teams to assess how prepared they are to respond to and recover from future attacks.

1. Do we have a patch management program in place?

WannaCry is a ransomware variant; ransomware has been around for a while, but this was a particularly virulent version, hitting and encrypting data on an estimated 230,000 devices in over 150 countries in just days. The attack appears to have taken advantage of known in dated versions of the Windows operating system, reportedly hitting companies using Windows XP and Windows 2003 particularly hard. Victims without readily available backups of their data could find themselves paying a bitcoin ransom to hopefully obtain a key to allow them to unlock their files.

Software providers routinely discover vulnerabilities in their software and often distribute patches to their products to address them. Vulnerabilities can range from simple performance issues to significant security holes, and patches from routine to critical. Even though Microsoft stopped supporting certain of the impacted products some time ago, it released a patch to address a vulnerability associated with WannaCry two months ago.

One way to help address this issue is to have a program in place to address patching – for example, a policy that provides for installing routine software patches on a scheduled basis and critical patches on an expedited basis, taking into account relevant business and technology considerations. For example, in many cases, patches need to be tested before deployment. A patch management program can help to maximize resiliency while minimizing business interruption.

2. Can users install their own software, and how do we manage admin-level access?

Users who are permitted to install software can introduce vulnerabilities into an otherwise secure system. One way to help address this risk is by restricting user rights to download software. Administrator-level user accounts are another area of focus because they have broad access privileges and are permitted to perform a wide spectrum of functions. These credentials, if compromised, can possibly allow a hacker to install malicious tools on local machines or, in some instances, move through the company's network with greater ease and, potentially even to cover its tracks to avoid detection. Controls that can help address this issue include limiting the use of elevated, administrative user accounts throughout the enterprise. They also include enhanced password complexity and a regular changes in user account credentials. Companies can also deploy privileged account management software to monitor administrator accounts, detect unusual activity and take action to quarantine an attack.

3. Have we considered multi-factor authentication?

Multi-factor authentication involves a log-in process that requires multiple means of authentication, such as a password plus a temporary token generated by a separate device at the time of user log-in, each of which is required to be entered by the user before network access is granted. This multi-step process can provide a layer of protection particularly where a user's password has been compromised, because an attacker cannot get into the network remotely using the password alone. Context is key, in that multi-factor authentication can be impractical or more than is needed for various implementations. But more regulators are showing an interest in exploring where multi-factor authentication has or has not been adopted as a control for remote access points into parts of an enterprise's network.

4. Will our back-ups be available to us, on an acceptable timeframe, if we are attacked?

A back-up system that allows for quick, seamless recovery of critical systems and data can bolster resiliency in the wake of an unexpected system outage or loss of data, whether caused by a ransomware attack or non-malicious means such as a natural disaster. Attackers know this, and according to security researchers, ransomware attackers are more and more looking to target back-up servers as well as main servers in their attacks. Understanding whether backup systems can withstand a ransomware or other attack on company systems is therefore important. Having procedures in place for regular back-ups can help minimize the impact of an outage or attack. Additionally, back-up systems can be further enhanced by maintaining them on separate networks or having tightly controlled write access to those devices, and by procedures for testing the efficacy of those controls.

5. Have we tested our systems to determine susceptibility and have we tabletop exercised our incident response plan?

The primary goal of testing information systems is to identify vulnerabilities before the attackers exploit them. Companies can retain experienced cybersecurity firms through legal counsel to provide a robust assessment, under privilege, of what may need to be improved so they can meet their legal obligations to protect information. These firms can work to identify vulnerabilities just as a hacker would and determine how well a company's cybersecurity program is functioning.

Periodic testing of the incident response plan also can help a company prepare for an attack. Tabletop exercises involve practice drills of a "real world" incident simulation. These exercises can often identify flaws in a company's incident response plan and help team members learn the incident response process so they are prepared to respond when a real life incident occurs. A tabletop exercise can involve all members of the incident response team, including IT, legal and compliance, and provide other stakeholders like business teams, HR and corporate communications with an opportunity to practice coordinating and communicating effectively with each other across a range of possible scenarios.

Companies can also practice analyzing incidents against applicable notification statutes and industry-specific laws, as well as contractual commitments to notify business partners or other third parties. In the health care industry context, for example, ransomware attacks have been known to target hospitals, health care providers and other health industry entities because they tend to have rich repositories of personal and sensitive data. In practicing an incident response plan, healthcare providers who use, disclose or access electronic identifiable healthcare information can review and rehearse how they are meeting their obligations under relevant laws, including the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as well as various state privacy and data security laws. In addition, the U.S. Department of Health and Human Services Office of Civil Rights has indicated that a ransomware attack involving health care information often results in a breach under the HIPAA Breach Notification Rule, unless the entity can demonstrate, after conducting a risk assessment, that there is a low probability that protected health information has been compromised.

6. What kind of security detection and monitoring capabilities do we have?

When a ransomware attack occurs, a company may learn almost immediately that its systems have been compromised because the ransomware is designed to lock a system, and then display an instruction for how to pay the ransom to secure the key to unlock the files. This is often not true, however, for other types of attacks. In its 2016 Trends Report, cybersecurity firm Mandiant reported that the median time from compromise to eventual discovery of the incident by the company was 146 days. One potential option that may help here involves the use of security information and event management (SIEM) technologies that help to detect and respond to suspicious behavior, potentially allowing a company to isolate impacted devices or systems until the issue can be investigated and resolved. In some cases, companies may elect to retain an outside security services firm to help triage alerts.

7. What type of security training do our employees receive and how frequently?

Employee training on information security can play a part in reducing information security risk. Depending on the business, its level of risk and the particular job function, training topics can include:

- Good information security hygiene;
- How to recognize and avoid falling victim to attacks, like spoofing and phishing; and
- Company processes for responding to a security threat, including reporting the incident to the correct contact persons within the organization.

This training can occur upon hire and periodically thereafter.

8. What is our information security budget, and have we allocated the right resources?

An effective information security program requires appropriate budget and staffing. Boards and management may want to evaluate what their company spends on security and identify security requests that have been made but that may remain unfunded. It is helpful to consult directly with IT and information security leadership within the company to solicit input on gaps in resources. These inquiries can help determine whether the company has allocated the correct amount of funding and number of personnel to security, taking into account the size and scope of the organization and the level of sensitivity of the information and systems to be protected.

9. Who is responsible for what aspects of our information security?

Information security is not just an IT function. Many organizations appoint a cross-functional team to consider and manage the overall enterprise risks that information security present. On this front, gaining a basic understanding of the high-level principles of the NIST Cybersecurity Framework and how to apply them can help an organization develop, maintain and evolve proper administrative, technical and physical controls designed to protect the network.

10. Have we reviewed our cyber-insurance coverage lately, and does it appropriately address the risks we face, including ransomware attacks?

As cybersecurity attacks become more frequent, companies that depend on the Internet may want to consider obtaining cyber-insurance or reviewing existing coverage to ensure it appropriately addresses the risk profile of the company. Working with a qualified professional, companies can review policies to assure coverage is appropriate for their business in light of its risk profile and that any policies issued do not contain exclusions that would render the policies ineffective for the major risks a company faces. Companies may want to consider whether the policies cover ransomware attacks. Coverage limits should be selected based on a realistic analysis of a company's exposure, keeping in mind that certain laws may impact the amount of coverage a company should seek. For example, Europe's General Data Protection Regulation, which goes into effect in May 2018, dramatically increases a company's liability exposure to the extent it is covered by that law, and this exposure increase may warrant obtaining additional coverage.

Closing Thoughts

If a ransomware or other security incident happens, affected organizations should work closely with legal counsel, forensic specialists, IT professionals and others to determine an appropriate response, including whether a breach notification is required by law (such as HIPAA or any other applicable law) or by any contract into which the company may have entered.

With appropriate planning and resource deployment, companies can ensure they have the necessary information security infrastructure in place to maximize protection against ransomware and other cybersecurity attacks, and to quickly and effectively respond to attacks if and when they occur.