PUBLICATION

What You Need to Do Now: Responding to the Major Cybersecurity Attack Against Organizations

Authors: Alisa L. Chestler
May 15, 2017

Regardless of whether you have experienced any disruptions to date, you cannot ignore the major global cybersecurity attack that continues to plague organizations. A particularly destructive piece of malicious software, the WannaCry ransomware infection has hit more than 100 countries and brought thousands of organization to a grinding halt.

As we continue to assist clients with their current and ongoing issues, Baker Donelson offers some key thoughts and action plans for management, business teams and IT security personnel. First and foremost, as this attack was based upon a known vulnerability, please make sure that your IT team has installed the MS17-010 patch to the Microsoft Windows operating system. For more detailed information, we recommend your IT security personnel keep track of the recent information through the U.S. Computer Emergency Readiness Team (US-CERT), which is a division of the United States Department of Homeland Security. [Multiple Ransomware Infections Reported]

Recommended Steps:

- **Communicate**. Prepare and send an alert for employees and staff regarding their roles in preventing such attacks on your networks. For example, remind them to be on the lookout for phishing scams and to report them to the Help Desk immediately if they are making it through your spam filters. Further, remind employees that very few emails contain an "emergency." Even if an email appears to be from a known source, everyone should be thoughtful when opening email attachments. Please also make sure employees know how to get to the Help Desk 24 hours a day, seven days a week, as system incidents are not limited to a 9-5 workday.
- **Review Your Incident Response Plan**. Ensure communication lines among management, counsel and key IT personnel (IT Information Security Team) are open and ready to implement your incident response plan. Pull out the response plan and make sure it specifically anticipates a ransomware attack of this nature. If your plan does not, or if you do not have a written incident response plan, please contact your Baker Donelson counsel for assistance. Documented Incident Response Plans are an expected compliance obligation for all organizations regardless of the size, industry or kind of information maintained by the systems.
- **Know Your Patching Compliance**. Patch Management programs are the lifeblood of any IT security structure. Thousands of organizations were immune to this strain of ransomware because they were up-to-date with their patches. Management should ask (if they don't already know) whether critical patches are up to date. If they are not, initiate a plan to get your programs as current as possible.
- **Use This as an Opportunity**. Management, legal and IT security can no longer keep "kicking the can" when it comes to information security. Whether the systems include information on trade secrets or personal information of individuals (including employees), or the systems just keep the machinery up and running, computer systems and programs are the lifeblood of organization. Knowing your compliance and contractual obligations before an event is critical. This is also a good opportunity to revisit some prior decisions. For example, many organizations continue to delay implementing multi-factor authentication. Organizations continue to resist multi-factor authentication for a variety of

reasons, including employee morale. However, this tool is widely becoming one of the most important information security protocols.

If your organization has become infected with this (or any other) ransomware and a system is already encrypted, then swift action must be taken. Baker Donelson has an incident response team that can help you systematically address the most pressing issues quickly and efficiently.

Baker Donelson's Data Protection, Privacy and Cybersecurity Team was recently recognized as a member of the "Honor Roll of Cybersecurity Law Firms" in the United States as determined by The BTI Consulting Group. Recognition as a member of the Honor Roll reflects corporate counsel's view of the Baker Donelson team as strong cybersecurity performers. To link to the Baker Donelson series on ransomware, please click here.

If you have any questions regarding the topics in this alert, please contact Alisa Chestler, CIPP/US, or any member of the Firm's Data Protection, Privacy and Cybersecurity Group.