PUBLICATION

Cyber Criminals Now Have the Keys to Your "House"

Authors: Alisa L. Chestler
December 10, 2020

On Tuesday, December 8 one of the nation's leading cyber defense vendors (FireEye) announced it suffered a recent cyber-attack from a "highly sophisticated threat actor, one whose discipline, operational security lead us to believe this was a state-sponsored attack." While cyber-attacks have been plaguing organizations for years, the threats have grown increasingly more sophisticated and the level of criminal operation is unprecedented. The Advanced Persistent Threat (APT) groups are focused on larger organizations, however many times their targets are not specific and they end up infiltrating even the smallest of organizations. Unfortunately even some of our smaller clients have suffered cyber attacks which can have devastating and long term consequences.

The FireEye cyber-attack is a signal to all organizations that delay of critical resources toward information technology infrastructure and planning can no longer wait. The FireEye event will shift the cyber-attacks into overdrive, and 2021 will end with numerus organizations not only suffering a cyber-attack, but potentially suffering an attack that will mean the termination of operations. All hope should not be lost. There are several actions organizations can take now to add a line of defense in an effort to reduce the risk facing all organizations:

- Understand and practice the incident response plan (IRP) with disaster recovery and business continuity specifics. Have these documents downloaded to paper in case the systems are unavailable. Make sure the IRP has contact information on cyber coverage, internal incident response team members, and key outside vendor contacts, including outside counsel.

- Ensure your IT security professionals are monitoring the specific countermeasures published and recommended by FireEye and other cyber firms. Staying on top of these issues and concerns is of critical importance. There are threats evolving every day and it is important to understand how the models are pivoting. The ransoms are no longer small or insignificant. The ransom demands have expanded significantly and are, many times, crafted with knowledge about the organization. In the past year the threat model has been enhanced to perform significant reconnaissance and exfiltration of information prior to unleashing the ransom. Once the organization's files are encrypted and the ransom note is released, it is too late – the damage has largely been done. This should be of grave concern to organizations with confidential information and trade secrets, personal information for customers or employees, and certainly for those who rely on systems for executing their business, whether it be supply chain, e-commerce, health care or technology. In other words, every organization, large or small, can be subject to a devastating cyber-attack.

- Use this event as an opportunity to continue the risk discussion within your organization. Management should be gathering key department leads to understand the issues and develop a culture of risk management and planning. Operations leads should be key players with the management team and IT to develop a robust understanding and program.

If you do not have an IRP or have not practiced your IRP, we stand ready to help you. Please contact one of our Baker Donelson Data Protection Team members.