



Legal Alert

‘SHIELDS UP’ ON CYBERSECURITY IN WAKE OF UKRAINE CONFLICT

March 02, 2022

CONTACTS

Dawn M. Russell

Consultant

D: (585) 419-8708

Alan M. Winchester

Member

D: (212) 313-5403

Fears of cybersecurity attacks are mounting in the wake of the Russian invasion of Ukraine. From the war itself, a number of malware variants have been created and are circulating on the internet.

In addition, with the stiff economic sanctions, Russian state-sponsored criminal organizations are seeking to accumulate more Bitcoin or other cryptocurrencies using techniques such as

ransomware.

In the past, these crime syndicates generally tried to avoid critical infrastructure, for fear of reprisals, but it is no longer certain if that forbearance is still being practiced or if we are entering a new phase in cybercrime.

The U.S. government's Cybersecurity & Infrastructure Security Agency (CISA) is urging greater vigilance, advising organizations to put their “shields up” while the war continues and taking their message to local communities. On Wednesday, CISA Region II leaders joined Congressman Joe Morelle in briefing business leaders during a session of the Rochester TRENDS series of the Greater Rochester Chamber of Commerce.

[Click here](#) to download a one-page summary of their recommendations for reducing your risk of cyberattack, or visit the CISA Shields Up website. CISA is also requesting all organizations to report signs of an attack to either their office or to the FBI.

We are advising all our clients to visit the CISA website to take advantage of their recommendations and threat intelligence reporting. Based on this heightened guidance, we at Harris Beach are reviewing our own cyber-defenses and can assure you we have a program in place to keep your information safe.

If your organization does nothing else, these are some of the basic steps it could take to reduce the likelihood of being hit with ransomware:

- Enable full logging for all critical systems that contain sensitive information. Data privacy laws have very strict reporting requirements and generally presume data exfiltration and acquisition when there is unauthorized access to a system. Further, ransomware syndicates often exfiltrate sensitive information with a promise to later delete it after the ransom is paid. Without complete logging, it can be nearly impossible to determine which files, emails, systems or computers were

accessed. There is usually an additional cost associated with heightened monitoring, but given the current wartime environment, it is certainly worth considering.

- Enable multifactor authentication for all remote access to your systems. We know that employees will complain that this makes remote access too hard, but it is time to move past this and enable the feature. It can be configured to only require it once for known computers or mobile devices or once every month or every time depending on the nature of the data your organization is holding. So while it could add an extra two seconds to logging into a system, the fallibility of passwords alone is so great that this extra level of protection is critical to any cybersecurity program.
- Make sure your backups are both complete and separate from your network. If system defenses fail and ransomware is deployed, a working backup is a strong protection against having to consider paying the ransom. The criminals know this as well and therefore try to encrypt the backup before anything else. So they should be separate or partitioned from the main network. Further, it is a good idea to test the backup/restore process to make sure it works.
- Patch and update all your software to its most current version. Software companies patch their software frequently to counter weaknesses and bugs in their security design. The criminals can find and assault the system that is not patched. It is not good enough to patch most of the systems in your organization. All of them need to be patched. This should be done according to a schedule and with a checklist from a system inventory or, if possible, automatically with systems capable of this feature. Doing patches on an ad-hoc basis will inevitably lead to omissions and cracks in the security program.
- Supply chain resiliency has become an area of intense focus. With so many systems now controlled and operated by third-party service providers or cloud platforms, organizations are dependent on these external systems for their own operation. In some cases, there may not be any reasonable alternative if they were to go down. However, in other instances, it may be possible to stand up a substitute process or system should that provider fall victim to an attack or disaster. Roundtable exercises where these key systems are both identified and work-around processes are explored are highly valuable and productive.
- Review your disaster response plan. After an attack has happened is never a great time to be either drafting or reviewing your organization's disaster plan for the first time. Ensure that the plan authorizes the necessary parties to act; that all the required stakeholders are included and identified; legal and technical assets are identified, under retainer (and done so with proper privilege protections) and prepared to engage when called; and that communication pathways exist in the event systems are not available. Consider if ransomware is included in the response plan and determine the organization's appetite for paying a ransom (and arguably supporting evil organizations) or relying on restoration efforts which could make the decryption process more difficult should the restoration efforts fail. This alone is a difficult discussion that is best to be had in less volatile circumstances.

We are experiencing a situation in Europe that did not seem possible only a short time ago. As with all things in cybersecurity, the threat landscape is continually changing and organizations need to adapt and adjust accordingly to reduce their risk.

If your organization is concerned about the adequacy of its cybersecurity program and would like to discuss it with one of our cyber risk counselors, contact Alan Winchester at 212.313.5403 or awinchester@harrisbeach.com, or the attorney you usually work with, to arrange a meeting.