



## Playing cat and mouse as cyber-threats intensify in 2022

May 11, 2022

**By Barbara Holmes**

In the news, it is hard to tell who is winning against the ever-growing threats posed by our information security vulnerabilities. We should be concerned not only with Russian or Chinese hackers. Serious threats can come from internal staff who find a flash drive in the parking lot and plug it into their networked workstation. That random flash drive could unleash a sleeping monster hiding in the network and collects data until it is ready to attack. These threats often steal sensitive data, then encrypt important files and backups.

More recently, attacks can exploit weaknesses in the very services we rely upon. The Log4JShell vulnerability sent web administrators scrambling to prevent malicious code from executing on web servers that use Apache logging. In the past year, [Microsoft's on-premises implementations](#) faced threats as did [Office365](#). Spam blocking software and services fail to block many threats that reach our end users.

Don't forget the coding staff! Often, a developer will build a "back door" into a custom application so that they can troubleshoot it in the future, bypassing security. Both users and bad actors may exploit this vulnerability, elevating privileges to get to sensitive data and network resources.

In one instance, a developer developed a custom captcha (that little set of floating letters that we must retype on certain web pages). However, the developer stored a table that converted the goofy letters to their typing equivalent on the same webserver that the captcha was supposed to protect. Consider how easy it would have been for a hacker to access and bypass the captcha just by writing a quick program against the thinly shielded conversion.

The sad part is that many issues could and would be addressed if both business and IT management knew what was happening and how to prevent and provide protection for the most important resources. Too often, we are afraid to address our own demons.

What is the remedy? An important first step is to perform an honest and impartial InfoSec/Cybersecurity assessment that would identify major information assets and their vulnerabilities so that real planning can occur. The old phrase “know your enemies” is never truer than creating plans for lowering risk and recovery/remediation.

Have you checked out NCSC's [cybersecurity webinar](#) as a good first step? Share with us at [Knowledge@ncsc.org](mailto:Knowledge@ncsc.org) or call 800-616-6164. Follow the National Center for State Courts on [Facebook](#), [Twitter](#), [LinkedIn](#), and [Vimeo](#).