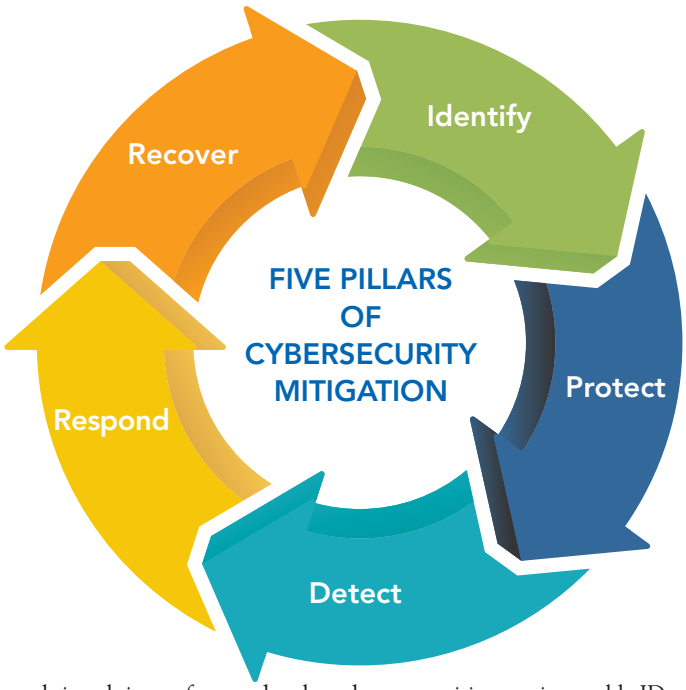
Response to "The Court Has Been Hacked!"

By Judge Herbert B. Dixon Jr. (Ret.)



After the publication of my previous technology column, "The Court Has Been Hacked!,"[1] several readers wrote me of their belief that they were reading a true account of an actual court hacking—until they reached the end of the article. Those remarks surprised me because I intended to write a fictional account of a court hacking as a wake-up call for those who had not thought about the disruptive effects on a court whose IT systems were completely compromised. Apparently, my readers don't believe I am capable of writing fiction. I can now sympathize with Orson Wells following the public outcry to his 1938 Halloween Eve Mercury Theater radio broadcast, "War of the Worlds," which sent communities of listeners into panic mode believing that Martians were invading the earth. Whether you classify my last technology article as a successful wake-up call or an unintended April Fools' joke, I now owe it to all who read that previous article to write about individual, commercial, and governmental efforts to avoid similar cybersecurity disasters.

Cybersecurity should be everyone's priority. The drastic increase in the number of employees working from home because of the COVID-19 pandemic has made the need for improved cybersecurity even more urgent. Cybercrime alerts to the Federal Bureau of Investigation have risen to 4,000 a day, compared to 1,000 pre-pandemic.[2] Attacks on virtual private networks (VPNs) are on the rise,[3] phishing attacks are increasing 200 percent each year,[4] and ransomware attacks have risen by 93 percent over the past 18 months.[5]

Closer to home, cyberattacks dramatically affecting court operations are in the news. A significant example occurred in January 2021 when we learned that a cyberattack involving software developed by the company SolarWinds had compromised the electronic filing system used by U.S. federal courts, likely revealing confidential information in sealed documents, including trade secrets, espionage targets, whistleblower reports, and arrest warrants. This incident compelled federal courts to issue standing orders directing the filing of highly sensitive documents only in paper form or by uploading to a stand-alone computer at the courthouse not connected to the internet or court network.[6] Other cyberattacks have targeted devices manufactured by Citrix Systems Inc., Cisco Systems Inc., and Microsoft Exchange Server—products used by many courts.[7]

Before discussing current strategies to combat cyberattacks, let's look at recent history. Most current computer users are familiar with antihacking efforts that have been in use and refined since the 1990s. These efforts were based on a "trusted user" model that focused on keeping the hacker out of the network. They include the use of IDs and passwords, VPNs, firewalls that reject suspicious emails and attachments, and more. These efforts have been modernized to some extent with the use of multifactor authentication, which adds an additional element to identify the user, e.g., a secret fact (the city in which you were born), a PIN (personal identification number) sent by text, facial or fingerprint recognition, an insertable ID card, and synchronized random number generators. Although multifactor authentication has been shown to reduce password-based cybercrime by 99 percent,[8] cybersecurity experts now operate under the assumption that, one way or another, unauthorized persons will eventually get into a network. A recent example of this inevitability is the breach of the Colonial Pipeline system that disrupted U.S. fuel supplies after the theft of a VPN password.[9] Today, IT professionals are not asking themselves what they should do *if* a cybersecurity attack occurs but what they will do *when* it happens.

Judge Herbert B. Dixon Jr. retired from the Superior Court of the District of Columbia after 30 years of service. He is chair of the *ABA Journal* Board of Editors, a former chair of both the National Conference of State Trial Judges and the ABA Standing Committee on the American Judicial System, and a former member of the Techshow Planning Board. You can reach him at Jhbdixon@gmail.com. Follow Judge Dixon on Twitter @Jhbdixon.

Among IT security professionals, there are five pillars of cybersecurity mitigation: *identify* the vulnerabilities, *protect* the network with the most effective defensive measures, *detect* the intrusion, *respond* with preplanned cybersecurity measures, and *recover* from a cybersecurity attack. These pillars are the essence of any cybersecurity mitigation strategy. Unfortunately, this technology column cannot comprehensively address the full range of mitigation strategies because of space limitations but will highlight a few well-known strategies.

Plan How to Respond to a Cyberattack

As implied by this subtopic, the premise under which IT security professionals work is what to do *when* a cyberattack occurs, not *if* such an attack occurs. To avoid some of the disarray described in the last article, "The Court Has Been Hacked!," courts should establish a Cybersecurity Incident Response Plan *before* a cyberattack incident is already underway.

In one instance, a cybersecurity attack forced Alaska state courts to go offline after their IT security staff detected malware on the courts' servers. The courts quickly switched to teleconferences or in-person proceedings because videoconferences were no longer possible.[10]

Another example of this is represented by the May 2020 compromise of the Texas state courts' computer systems by a ransomware attack that affected all devices connected to the state judiciary's network.[11] The ransomware essentially made all stored files unusable. Fortunately, the Texas judiciary previously had begun backing up network data both on-site and separately in cloud storage. Although the ransomware corrupted the on-site backups, the daily-occurring cloud backups were not affected, so most of the corrupted data could be restored. Nevertheless, it still took six weeks for most of the judiciary's network functionality to return because the extensive network intrusion and damage required the network to be almost entirely rebuilt.

Finally, consider the recent experience of Jackson Hospital, a 100-bed facility in Mariana, Florida. The hospital's emergency room personnel discovered that they could not access patients' medical histories, which were stored in a records database maintained by an outside vendor. It turned out that the external system was infected with ransomware designed to spread to any connecting system, which included the Jackson Hospital network. The hospital management reacted quickly and authorized the IT director to shut down the Jackson Hospital computers before the malware spread. The IT team physically disconnected the hospital's network from the outside vendor's health records system and began to check the hospital's systems one by one for malicious code, starting with the most critical systems. Despite IT's quick action, the entire hospital was forced to resort to its contingency plan—old-fashioned pen-and-paper records—to keep the hospital running and avoid any significant disruption to patient care in the interim. After a few days, the hospital's computers were entirely back online, aside from the emergency room charting system (however, the records were available from other parts of the hospital's network).[12]

The ransomware that Jackson Hospital was combatting was identified as "Mespinoza," a virus that has successfully infected nearly 200 entities worldwide. However, the actual number is unknown because many ransomware attacks are not reported. The organizations best prepared for a cyberattack will have in place defensive measures to discover bad actors during their reconnaissance stage, i.e., while the bad actors are covertly discovering and collecting information about a system, but before they attack.

Update and Upgrade Software Install Patches

According to the National Security Agency (NSA), software updates, upgrades, and patches should be installed immediately. This process should be automated to the extent possible using an update service directly from the vendor. Naturally, users may be concerned that a software update or upgrade might be released before the discovery of bugs or other imperfections in the update that might adversely affect the software's performance. It is for this reason that, before installation, IT staff at complex organizations will test updates in a controlled environment to ensure compatibility with the systems in that organization's network.

On the other hand, however, bad actors study these patches and seek ways to exploit the vulnerabilities when users have not patched their systems.[13] To try to avoid these issues, an organization's professional IT staff should regularly monitor online advisories such as the notices of vulnerabilities known to be exploited by bad actors against private and government entities issued by the U.S. Cybersecurity and Infrastructure Security Agency (CISA). CISA also issues binding directives ordering federal agencies to patch affected systems within specific timeframes. CISA's online catalog lists hundreds of vulnerabilities, with some as old as 2010, that are still being exploited against the unsuspecting public.[14]

Implement Periodic Employee Cybersecurity Training

Employee cybersecurity awareness training is critical for cybersecurity mitigation and protection of an organization's network. Employers and IT personnel must do more than provide a once-a-year slideshow to adequately educate employees about cybersecurity. For example, one effective strategy is to train employees not to fall for phishing attempts by actually attempting to phish them. Organizations with large enough IT staff may be able to run phishing simulations themselves, while smaller organizations may have to rely on contractors who can provide these services. With this approach, employees are first educated about common signs of a phishing email, such as an inconsistency in an email or web address (e.g., an email purportedly alerting you that someone has changed your Facebook password sent from an email address identified as "FB" is not from Facebookmail.com, but from CVVWK.EQYN@GLQOVQX.us upon inspection), an illegitimate web address (e.g., Linked1n.com rather than LinkedIn.com), a request for the recipient to provide personal or account information, a warning that the recipient must immediately act, or a message that you have won something or are otherwise

entitled to something that seems too good to be true. As a part of this type of training module, employees are informed they will be receiving fake phishing emails to test whether they fall victim to phishing attempts or whether they appropriately identify and report the emails as suspicious. Simply knowing that anonymous IT professionals randomly monitor employees' performance and might attempt to trick them with fake phishing emails may motivate employees to evaluate emails they receive more scrupulously.

Along the same lines, companies using innovative cybersecurity training programs have found that requiring employees to participate in game simulations of real-world threats can "train[] [employees'] brains to recognize suspicious messages immediately."[15] Other measures IT departments have employed are having emails that originate from outside an organization prominently display an "External" flag and adding a "report phishing" button to the shortcuts bar in employees' email inboxes for easy reporting of suspicious emails.

Employees should receive cybersecurity training periodically. One study found that employees began forgetting lessons from their cybersecurity training after six months had gone by,[16] meaning training ought to occur at least twice a year. Even twice a year may not suffice, however, as some security experts urge that training should take place more frequently because "in a rapidly evolving industry like cybersecurity, we can never stop learning."[17]

The Zero-Trust Approach

One highly touted model for cybersecurity mitigation is based on principles of "zero trust." This model assumes that any perimeter has already been breached and the bad actors are lurking within. One zero-trust approach premise is that no user is trusted simply because that user is within the network. Instead, the zero-trust system "relies on identity, and continuous verification of that identity, for permissions and access across all network resources."[18] As described by the NSA, the zero-trust security model assumes that a breach is inevitable or has likely already occurred. Accordingly, this approach limits access and looks for suspicious or malicious activity. In more concrete terms, this means that a user may access only the data, applications, or parts of the network necessary for the user to accomplish their work on a per-session basis. If a user is behaving unusually, e.g., by attempting to access files or applications not necessary for the user's work, access can be cut off or reauthentication required. While employees may prefer unfettered access to all their network's resources, restricting access limits a bad actor's ability to move laterally throughout a network. This means that any malicious activity within a network will be easier to trace, easier to quarantine, and less likely to bring an entire network crashing down.

Adopting a zero-trust approach means that an organization will first need to identify and classify sensitive data and resources, develop access policies, compile a list of users, determine what access privileges those users ought to have based upon their roles within the organization, and determine how to conduct continuous monitoring of users. Though the transition to a zero-trust security framework cannot occur overnight, the effort required will undoubtedly prove worthwhile as cyberattacks continue to increase.

Final Comments

There is no single panacea to the threat of cyberattacks. Rather than diving in blindly, an organization's first step should be to take stock of its existing security measures and conduct a risk assessment to identify vulnerabilities. Organizations should create or update a cybersecurity incident plan and implement a new or updated cybersecurity framework, considering both their technology infrastructure and human resources. Again, preparing for *when* the cyberattack occurs, not *if*, is your best bet to avoid the disaster described in my previous technology column. ■

Judge Dixon wishes to thank Amanda Purcell, Esquire, Superior Court of D.C. senior judges' law clerk, for research and writing assistance preparing this article, and David M. Simpson, chief information security officer (CISO), District of Columbia Courts, for his advice concerning current cybersecurity mitigation efforts.

Endnotes

1. Herbert Dixon, *The Court Has Been Hacked!*, 60 Judges' J., no. 4, Fall 2021, at 36, https://bit.ly/3ryihr5.

2. C.J. Haughey, *What Is Zero Trust? A Complete Guide for Security Professionals*, Sec. Intel. (Sept. 30, 2021), https://ibm.co/3FT77SR.

3. Jai Vijayan, *Attackers Heavily Targeting VPN Vulnerabilities*, Dark Reading (Apr. 21, 2021), https://bit.ly/33XPHqS.

4. Drew Rose, *Phishing Reports Show You There's a Problem, but What's Next?*, Infosecurity Mag. (Oct. 19, 2021), https://bit.ly/3AjYcsx.

5. Javvad Malik, *How Social Engineering Contributes to Successful Ransomware Attacks*, ITProPortal (Oct. 22, 2021), https://bit.ly/3rEapV4.

6. Maryclaire Dale, *Russian Hack Brings Changes, Uncertainty to US Court System*, Claims J. (Feb. 1, 2021), https://bit.ly/3rQCPeH.

7. Christopher Bing & Raphael Satter, *China-Linked Hackers Used VPN Flaws to Target U.S. Defense Industry*, Reuters (Apr. 20, 2021), https://reut.rs/32lPKwc.

8. Haughey, supra note 2.

9. Stephanie Kelly & Jessica Resnick-Ault, *One Password Allowed Hackers to Disrupt Colonial Pipeline, CEO Tells Senators*, Reuters (June 8, 2021), https://reut.rs/3nMUqCV.

10. Becky Bohrer, *Alaska Court System Offline After Cybersecurity Incident*, Associated Press (May 6, 2021), https://bit.ly/351OgYX.

11. David Slayton, *Contracting the Virus: Not If, but When*, Judicature, Fall/Winter 2020–21, at 52, https://bit.ly/3FL7zCA.

12. Sean Lyngaas, *'Lock It Down and Piss People Off': How Quick Thinking Stopped a Ransomware Attack from Crippling a Florida Hospital*, CNN (Jan. 16, 2022), https://cnn.it/3AgYz6V.

13. Nat'l Sec. Agency, U/OO/122630-18, NSA's Top Ten Cybersecurity Mitigation Strategies (Mar. 2018), https://bit.ly/3qIcGPO.

14. Catalin Cimpanu, *CISA Creates Catalog of Known Exploited Vulnerabilities, Orders Agencies to Patch*, The Record (Nov. 3, 2021), https://bit.ly/3GLugrw.

15. Rose, supra note 4.

16. Nick Bambulas, *How Often Should You Do Cybersecurity Awareness Training?*, Gordon Flesch Co. Cybersecurity Blog (Oct. 27, 2020), https://bit.ly/3AufdQL.

17. Mathieu Gorge, *Cybersecurity Is a Journey, Not a Destination*, Forbes (Oct. 11, 2021), https://bit.ly/3KymALH.

18. Matt Graves, *4 Stages of a Zero Trust Self-Assessment*, Sec. Mag. (Oct. 20, 2021), https://bit.ly/3IrCt4B.