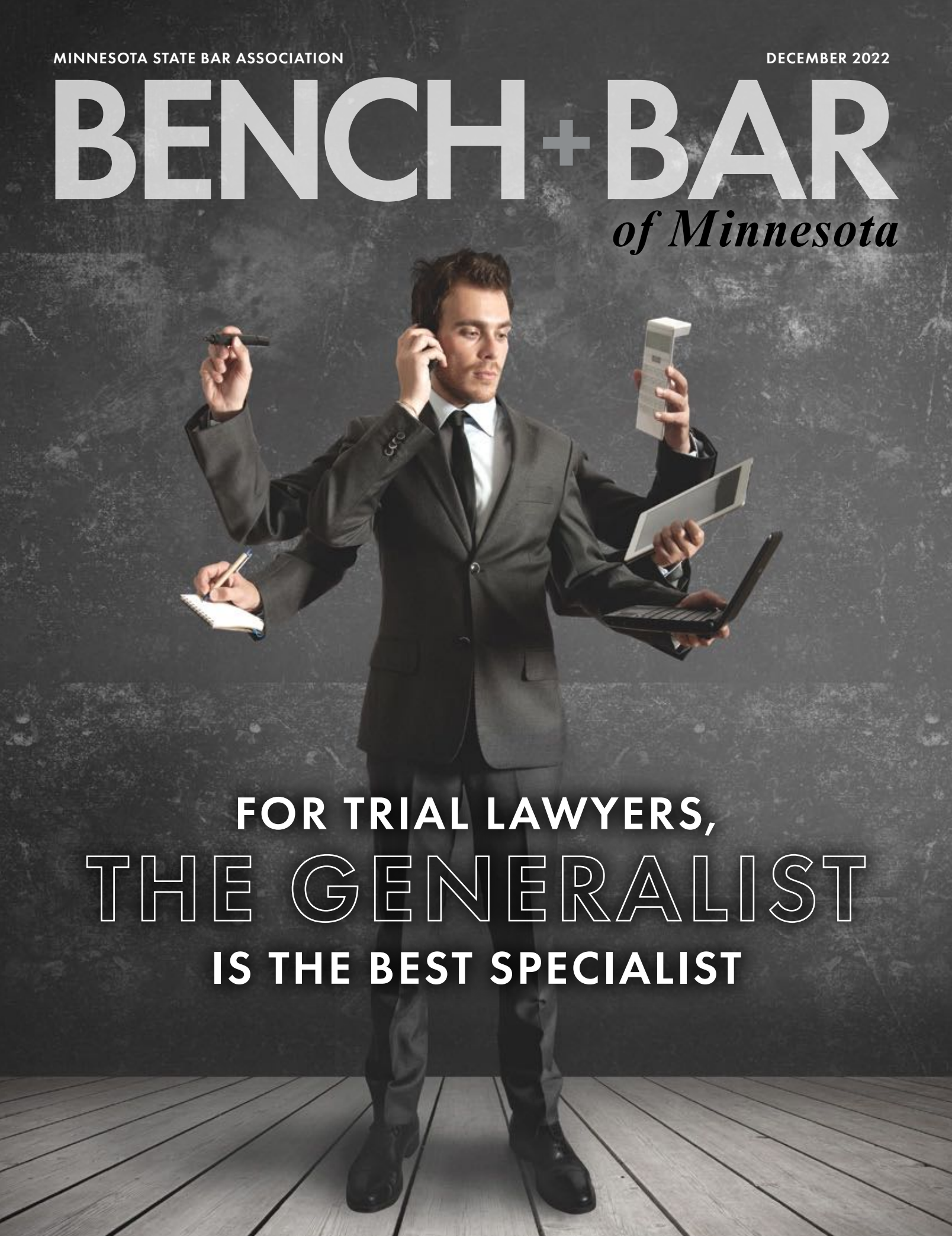
MINNESOTA STATE BAR ASSOCIATION

DECEMBER 2022

BENCH+BAR of Minnesota



FOR TRIAL LAWYERS,

THE GENERALIST

IS THE BEST SPECIALIST

RANSOMWARE *and counteracting the interconnected risks of the IoT*

BY MARK LANTERMAN ✉ *mlanterman@compforensics.com*

MARK LANTERMAN is CTO of Computer Forensic Services. A former member of the U.S. Secret Service Electronic Crimes Taskforce, Mark has 28 years of security/forensic experience and has testified in over 2,000 matters. He is a member of the MN Lawyers Professional Responsibility Board.

This past fall, Crystal Valley, a farming co-op in southern Minnesota, was targeted by a ransomware attack that left its employees using paper tickets to take orders.[1] The attack was one of many this year that have targeted critical infrastructure, with the agriculture sector being particularly at risk. Legacy technologies, apathetic leadership, and a lack of cybersecurity training and best practices can create a perfect storm. In fact, the FBI issued a warning this past spring, urging the agriculture sector to be aware of ransomware groups timing their attacks for maximum gain: "ransomware actors may be more likely to attack agricultural cooperatives during critical planting and harvest seasons, disrupting operations, causing financial loss, and negatively impacting the food supply chain."[2] Nevertheless, the agriculture sector is not unique in its heightened risk for ransomware, as attacks against critical infrastructure and organizations have continued to cause damage across the nation.

In all sectors, utilizing the internet of things (IoT) is a business requirement. Yet despite its ubiquitous nature, IoT cybersecurity is not always regarded as a top priority. Outside of organizations and companies, the average consumer often encounters roadblocks to both controlling how their personal information is protected and being assured of the basic security of their devices. Notifications are received in the mail when our private information has been part of a breach, we hear about largescale cyberattacks in the news, and there's the hope that the devices we purchase are as secure as possible. For organizations and individuals alike, it requires diligence to keep up with best practices and stay aware of current threats—but even the best of efforts do not create a perfect security posture when managing IoT devices.

To begin moving toward standardization and improved transparency for consumers, the White House has recently provided details on a new labeling initiative it expects to roll out in the spring of 2023, noting that "A labeling program to secure such devices would provide American consumers with the peace of mind that the technology being brought into their homes is safe, and incentivize manufacturers to meet higher cybersecurity standards and retailers to market secure devices."

According to the White House, "Government and industry leaders discussed the importance of a trusted program to increase security across consumer devices that connect to the Internet by equipping devices with easily recognized labels to help consumers make more informed cybersecurity choices (e.g., an 'EnergyStar' for cyber). These conversations build on the foundational work that has been pioneered by the private sector and the National Institute of Standards and Technology (NIST)."[3] Creating a labeling system standardizes basic cybersecurity needs and streamlines the buying process for consumers, recognizing security as a basic necessity.

The program further signifies a growing emphasis on information-sharing and cooperation between the private and public sectors and serves as an actionable step toward implementing the Biden administration's goals for cybersecurity on a national level—one goal being to combat the types of ransomware campaigns that target critical infrastructure internationally.

In October, The International Counter Ransomware Initiative (CRI) met in Washington, DC to reestablish its commitment to counteracting the worldwide threat of ransomware. Quoting again from a White House release: "CRI members are

committed to taking action, in line with national law and policy, to disrupt and degrade the ransomware ecosystem and hold accountable criminal ransomware actors based on our collective knowledge, expertise, authorities, and capabilities."[4] This initiative is tasked with better understanding the tactics of cybercriminals, and the circumstances that allow for their successful attack campaigns. From enforcing laws against financial crimes and holding cybercriminals accountable to organizing effective collaboration between nations, the members have adopted a global perspective on reducing the impact of ransomware.

As ransomware campaigns and the risks to critical infrastructure and organizations proliferate, it is encouraging to see that the objectives set forth in President Biden's 2021 Executive Order[5] are beginning to materialize. President Biden recently reiterated the importance of reaching these goals at the beginning of Critical Infrastructure Security and Resilience Month: "cyberattacks... have ripple effects, threatening global stability and disrupting supply chains everywhere."[6] Improving the security postures of government agencies, creating a labeling system to prioritize cybersecurity in technology, and launching international efforts to combat the growing dangers of ransomware are all positive signs. Within our own organizations, security is everyone's responsibility. Given the far-reaching potential for damage caused by cyberattacks, such as supply chain disruptions and dire business continuity problems, the same can be said on a national and even global scale. Cybersecurity measures are still sometimes seen as "optional," especially when convenience is impacted. The human element of security, from strong leadership to the proper management of legacy technologies, is a critical component of mitigating risk. ▲

NOTES

[1] *https://www.keyc.com/2021/09/27/business-resumes-crystal-valley-co-op-following-ransomware-attack/*

[2] *https://www.ic3.gov/Media/News/2022/220420-2.pdf*

[3] *https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/20/statement-by-nsc-spokesperson-adrienne-watson-on-the-biden-harris-administrations-effort-to-secure-household-internet-enabled-devices/*

[4] *https://www.whitehouse.gov/briefing-room/statements-releases/2022/11/01/international-counter-ransomware-initiative-2022-joint-statement/*

[5] *https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/*

[6] *https://www.whitehouse.gov/briefing-room/presidential-actions/2022/10/31/a-proclamation-on-critical-infrastructure-security-and-resilience-month-2022/*