OFFICIAL PUBLICATION OF THE MINNESOTA STATE BAR ASSOCIATION

VOLUME LXXVII NUMBER IV
APRIL 2020
www.mnbar.org

Bench&Bar OF MINNESOTA

New Lawyers Spotlight

PLUS
An interview with retiring MN Court of Appeals Chief Judge Edward Cleary

Being a lawyer is hard. Don't make it harder.

New lawyers need a mentor and a sponsor

Moving from private practice to government

Inflexible leave policy litigation

Whistleblowers after Friedlander

Responding to COVID-19
mnbar.org/covid-19-resources

Cybersecurity in pandemic times

A week ago I wrote on the importance of business continuity in planning for the coronavirus ("Business continuity and coronavirus planning," B&B Online 3/12). In partnership with Mike Olson, CEO of 360 Security Services, I proposed a four-tier approach to aid organizations in implementing a remote work program led by a dedicated team of key personnel responsible for communication, monitoring, and the coordination of procedures. Under that system, many within Minnesota would be at tier 2 or 3 as I write this—meaning an almost complete reliance on remote work given the spread of the virus and the government-ordered shutdowns of public gathering spaces. As we continue to manage this novel threat, maintaining organizational security while accommodating high volumes of remote work is imperative.

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.

In this crisis, reprioritization is occurring on a number of far-reaching levels. Communities are faced with the prospect of being quarantined for extended periods in order to stay healthy and protect vulnerable populations from becoming ill. Schools, venues, and events are closing or canceling for the same reasons. Families canceled spring break trips and vacations. Organizations are being encouraged to focus on remote work capabilities and business continuity. Throughout this upheaval, one thing is clear: Technology is the thread holding all of us together—allowing many of us to continue to work, to communicate, to live as normally as possible, and to find answers when uncertainty seems to be lurking around every corner. The reality of instant communication has made the response to this pandemic unlike any other in history.

> The very tools that are upholding business operations during this pandemic also open up a wider range of vulnerabilities and potential cyberattacks. The fact is, hackers are being quarantined, too—and now have all the time in the world to take advantage of organizations with weakened security postures.

But even in a pandemic it remains true that the price of all this technology-bred convenience is weakened security. The very tools that are upholding business operations during this pandemic also open up a wider range of vulnerabilities and potential cyberattacks. The fact is, hackers are being quarantined, too—and now have all the time in the world to take advantage of organizations with weakened security postures.

Unfortunately, the health sector may be especially at risk. "The U.S. Health and Human Services Department suffered a cyberattack on its computer system Sunday night during the nation's response to the coronavirus pandemic," Bloomberg News reported on March 16. "HHS officials assume that it was a hostile foreign actor." Given the current climate it's possible that hacktivist attacks, especially those fueled by political or nationalist motives, will prove a particularly dangerous threat during this time. No sooner was the pandemic declared than the scammers, fraudsters, and hackers opened for business, recognizing new attack vectors and preying on the heightened feelings and fears of many of us. Phishing scams exploiting fear of this pandemic are on the rise, many purporting to contain information regarding the COVID-19 virus.

Some of the best hackers operate within the circles of organized crime and/or nation state bad actors. Much like a corporation with an effective enterprise security team, they evaluate all the potential avenues of attack. If they have conducted the proper planning and intelligence work, they have already targeted certain organizations for their vulnerable networks and lax security. Mike Olson stresses the need for crisis communication plans that let employees know who should be communicating to them from within and stay apprised of developing cyberthreats. "Employees should be avoiding personal email crossover onto work-issued computers and devices," he notes. "Your designated team should be monitoring emerging threats on a regular basis and providing concise awareness to your employees. Not all employees will be regularly tuned in to new cyber threats as they work to balance their work-from-home responsibilities while caring for their own families, children out of school, or other personal concerns as a result of this pandemic."

As many organizations race to put together viable remote work plans, it is crucial that cultures of security continue to thrive remotely just as they would in the physical office space. A holistic security approach takes into account all areas of potential vulnerability, including those at off-site locations as employees begin to remotely access critical business systems and networks. Security training for employees should be conducted by security and IT departments immediately. Instructing on best practices is imperative for supporting the efficiency and safety of remote work. These best practices include the use of VPNs, avoidance of open wifi networks, email encryption, securing endpoints, and phishing/social engineering attack awareness. Relevant remote work policies and procedures should be reviewed (and updated if necessary) and provided to every employee.

As you are continually communicating these best practices to your employees, it is critical to acknowledge the value of intelligence or information gathering. This includes information gathered from any remote employees who observe suspicious activity in relation to their work (such as phishing schemes, social-engineering attempts, or unusual phone calls seeking information). It also includes ensuring you are effectively logging or capturing activity in your network and retaining this information should an attacker exploit your employees or network.

Cyber and traditional criminal activity will rise as a result of this crisis. As during other recent crises, such as the 9/11 attacks or the housing collapse of 2008, fraudsters and hackers will seek ways to exploit vulnerabilities and monetize their crimes. Organizations and law enforcement will not be able to investigate these crimes until the immediate crisis and triaging associated with the pandemic subside. It is then that we will be left to clean up and investigate potential attacks that occurred. You will need a good collection of data to use in deciding to investigate, mitigate, respond to, and recover from any attacks that may have slipped past your defenses.

As we work through these challenging times, the role of digital communication and the conveniences enabled by the Internet of Things cannot be diminished. Our digital landscape has allowed for a degree of preparedness and information-sharing that did not exist in past pandemics. In many ways, it is the only thing preserving our capacity to carry out a semblance of "business as usual." But we must heed the heightened threat climate, too. Cybersecurity must be prioritized as much as the technologies making business operations possible. Though we may feel safer as we leave our physical offices, we face a greater number of threats in the cyber world. Now is the time to double down on your efforts to bolster your security posture and conduct the regular security assessments needed to optimize your organization's ability to respond to the cyberthreats we now encounter. In a society struggling to protect itself from a novel virus while maintaining some degree of normalcy, we truly are hanging by a Web. ▲