KAUFMAN | DOLOWICH

Mansfield Rule Certified 2022-2023

Let’s Check Our Cybersecurity Before We Wreck Ourselves

By Avery A. Dial, Partner and Co-Chair, Data Privacy & Cybersecurity Practice Group,
and Nicole Christman, Attorney

Microsoft released its annual Digital Defense Report this past month, which shows an increased sophistication of cyber threats. This annual report, initially launched in 2005, continues to contribute to a community approach to better improve the security of our shared digital ecosystem. This year’s eighty-eight (88) page report covers cybersecurity trends throughout the past year and recommends that est in professionals and technology to help stop attacks.

Recent attacks are showing a trend in certain techniques such as credentialed harvesting, the use of compromised username/password information to gain access to sensitive information; ransomware, a type of malware that blocks access or threatens the use of the victim’s sensitive information unless the victim pays a ransom; and an increased focus on the Internet of Things (IoT), given the interconnection of our phones, devices, etc. Also, attack campaigns are morphing to avoid detection, changing use from domains to email addresses to content templates and URL domains. In the past years, cybercriminals focused on malware attacks. However, more recently, cybercriminals have shifted their focus to a more direct means of phishing attacks (~70% increase), such as sending emails pretending to be reputable companies to induce a victim to reveal passwords, personal and financial information. Further, nation-state actors have shifted their targets this year to COVID-themed attacks, luring victims with crisis themes, and targeting nongovernmental organizations (NGOs), government health care organizations, among others. Some of these actors are even targeting vaccine research organizations. Most of these attacks originate from groups in Russia, Iran, China, and North Korea. Ransomware continues to grow as a significant threat, and many government officials have warned against the potential use to disrupt the 2020 elections.

Moreover, working from home has presented new challenges and vulnerabilities. As more organizations move applications to a cloud, there is an increase in distributed denial of service (DDoS) attacks, which causes harmful infiltration of an organization. Social engineer is also being used to psychologically manipulate victims into performing actions or divulging confidential information. All organizations, businesses, industries, and even individuals should work with the government, IT, and legal professionals to help stop attacks through regular security updates and comprehensive backup policies, enabling multi-factor authentication (MFA). MFAs alone have prevented the majority of attacks, and we recommend you ensure your organization implements them today.