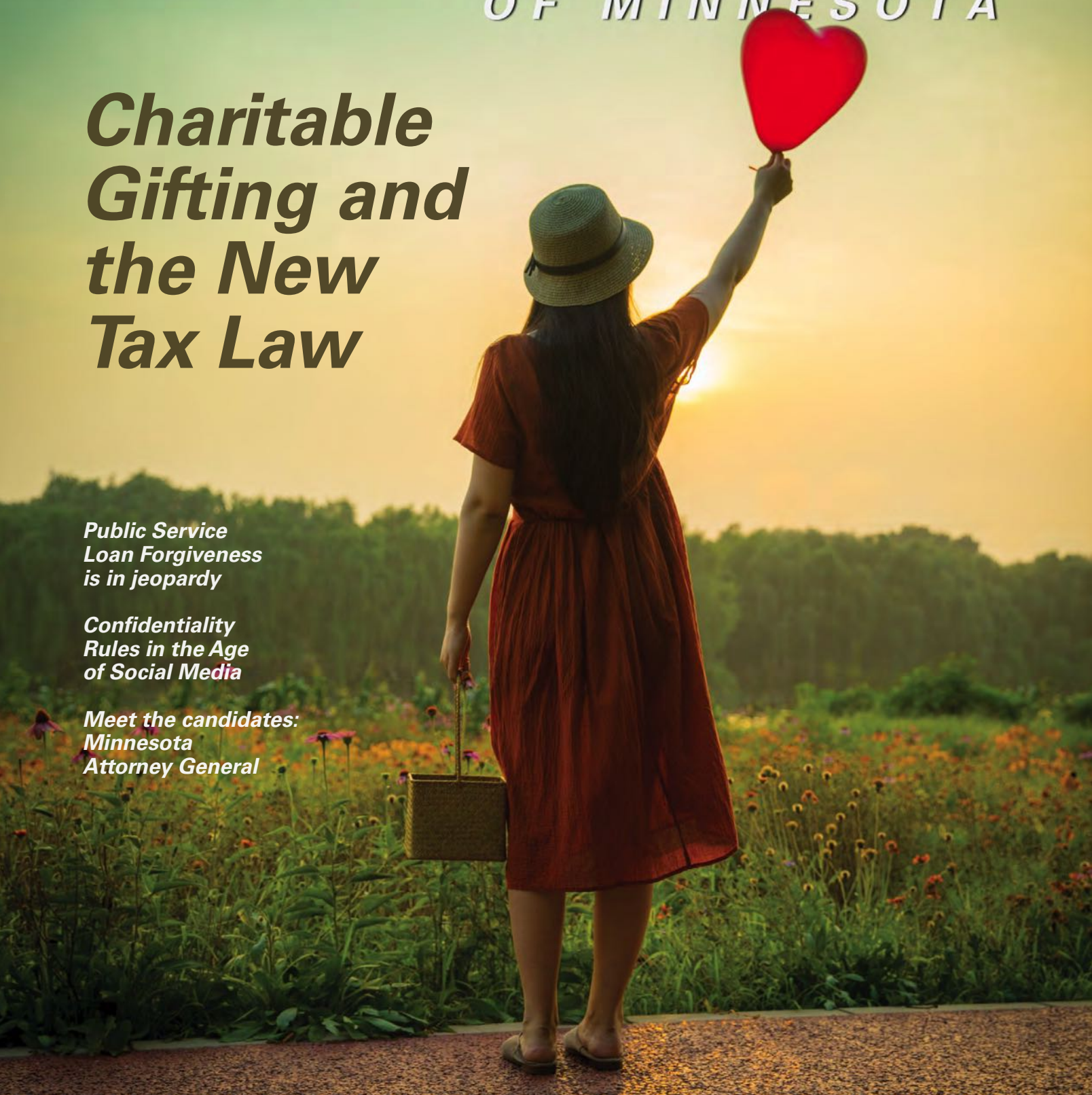
OFFICIAL PUBLICATION OF THE MINNESOTA STATE BAR ASSOCIATION

VOLUME LXXV NUMBER IX
OCTOBER 2018
www.mnbar.org

Bench & Bar OF MINNESOTA



Charitable Gifting and the New Tax Law

Public Service Loan Forgiveness is in jeopardy

Confidentiality Rules in the Age of Social Media

Meet the candidates: Minnesota Attorney General

Cyberattacks and the costs of reputational harm

Reputational damage is something that cyber insurance cannot accurately estimate. It accrues over the long term.

A few months ago, I wrote about cyber insurance and its place in an organization's cybersecurity plans ("Managing cyber risk: Is cyber liability insurance important for law firms?", June B&B). In my estimation, the most valuable aspect of cyber insurance lies in applying for it. Making organizations go through the paces to evaluate their cybersecurity postures, review security assessments, and implement ongoing procedures for proactive and reactive security measures is really what makes cyber insurance important.

Leaving aside the confusion over what this type of insurance actually covers, getting organizations to evaluate themselves is absolutely critical, especially as organizations are increasingly held to a high standard in protecting their data, networks, and critical assets. Cyber insurance often requires the organization applying for it to conduct a thorough risk assessment, vulnerability scanning, penetration testing, and simulated cyberattacks (including social engineering attacks, like email phishing). Third-party vendors the organization may work with are also scrutinized, as they often come into contact with critical assets and data. Though daunting to a lot of smaller organizations and firms, the cost of reaching this degree of preparation is fairly minimal compared to the potential cost of a data breach or cyberattack.

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 trials. He is a member of the MN Lawyers Professional Responsibility Board.

Damage potential beyond measure

When data breaches and cyberattacks do occur, calculating the financial damage is what we usually think of in considering the costs. But stolen assets are only one element to be reckoned with; in fact, one of the largest expenses is mediating the long-term reputational harm—including the inevitable legal and public relations expenses—that breaches today cause. This type of damage is something that cyber insurance cannot accurately estimate, especially since pinpointing the scope and severity of public response to a breach is not possible: It accrues over the long term.

Reputational harm is a primary risk associated with cybersecurity vulnerabilities, and organizations may never recover fully from the damage it causes. There is very little public forgiveness for victims of cybercrime, especially when it comes to the perception that personal data has been mishandled, stored insecurely, or collected without full disclosure or permission. With large-scale acts of cybercrime occurring every day, law firms especially are now held to a high standard of cybersecurity awareness and security program implementation. Anything short of perfect is often regarded with suspicion and distrust by current or potential clients.

Any time an organization gathers and stores information about employees, clients, patients, partners, or consumers, that organization is responsible for keeping the data secure. Organizations have to consider the cyber risk that corresponds with the cyber threats they face. Operational, legal, financial, and reputational costs are all elements of that risk and vary greatly depending on the sector, scope, and type of attack. A cyberattack could very well result in ongoing legal action, along with large financial settlements on behalf of those affected. With larger breaches, organizations now have a duty to alert people when they occur, adding to the pressure to have strong cybersecurity plans to protect the organization's reputation.

Weighing response costs

With reputational costs being a huge factor in data breaches, it is important for firms and organizations to consider the associated expenses required to start recovery. In addition to the types of services needed to recover the affected technology, organizations are sometimes advised to hire communications teams to control the scope of the damage. Today, these agencies often take to social media—both to ascertain the severity of the damage to the firm's public image and to begin rebuilding public trust. Before this can be done, however, organizations need to consider notification expenses. The EU's recently introduced General Data Protection Regulation (GDPR) poses new requirements for notifying the public about a breach, as do other recent laws and regulations governing cybersecurity.

Notifying the public is also one of the first critical steps in restoring public trust. Having complete information at the time of notification, working with the proper authorities, and providing mediation support (such as credit monitoring) for individuals are all elements of a thorough public response. Significant penalties can be incurred for non-compliance—but it should also be noted that perfect compliance does not necessarily equal perfect security. The best cybersecurity, mediation, and response practices need to be tailored to the firm or organization for optimal results.

Reputational damage is one of the many risks created by the cyber threats organizations face. Operational interruptions, financial costs, litigation, legal liability, and cybersecurity response only comprise part of the ultimate cost of having client data compromised. Developing cultures of security is no longer optional when it comes to maintaining the confidence of the public—and abiding by current compliance standards and regulations. Investing in cyber insurance may not be something your firm is eager to do, but evaluating your security posture and understanding the impact of reputational damage may encourage improvements to security postures, training programs, and in-house education. ▲