OFFICIAL PUBLICATION OF THE MINNESOTA STATE BAR ASSOCIATION

VOLUME LXXVII NUMBER V
MAY/JUNE 2020
www.mnbar.org

Bench&Bar OF MINNESOTA

LAWYERS, INTERRUPTED

Learning to practice in a pandemic

Working from home and protecting client data

In recent days, remote work has become the norm in the legal community. Teleconferencing, email, and myriad digital communication methods are even more important now than they were before the covid-19 pandemic. This abrupt shift requires consideration of ethical obligations when sending and receiving client data and personal information electronically. It's especially critical now, since many organizations had to rush to get proper remote work infrastructure in place, emphasizing convenience and operationality over security protocols. The legal community is held to a particularly high standard when it comes to protecting client information, and is therefore required to stay apprised of best practices in cybersecurity. Referring to the CIA triad—a security model that focuses on the confidentiality, integrity, and availability of data—is helpful as we work to optimize security and efficiency in our remote work environments.

According to the ABA Standing Committee on Ethics and Professional Responsibility's Formal Opinion 477R:

> A lawyer generally may transmit information relating to the representation of a client over the Internet without violating the Model Rules of Professional Conduct where the lawyer has undertaken reasonable efforts to prevent inadvertent or unauthorized access. However, a lawyer may be required to take special security precautions to protect against the inadvertent or unauthorized disclosure of client information when required by an agreement with the client or by law, or when the nature of the information requires a higher degree of security.

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 requirement acknowledges that using technology is imperative for efficiency and ease of communication with clients. But it also maintains that lawyers must have a degree of technical proficiency and knowledge of cybersecurity best practices. Lawyers must do everything in their power to protect the confidentiality of client data, and to make sure that in the event of a compromise, data would still be accessible. The confidentiality, integrity, and accessibility of client data is paramount as the legal community continues to work at offsite locations.

Though the situation is challenging, now is not the time to shrug off poor security practices. Relying on email disclaimers such as "If you are not the intended recipient of this email, please delete" is not enough to ensure the confidentiality of client data. Shifting blame from the sender to the unintended recipient is not an acceptable security strategy. Instead, standard email encryption policies protect client data by making data unreadable until it is "unlocked" via a decryption key. Use of VPNs, strong passwords and multi-factor authentication, avoiding public wifi, and securing endpoints are all a few ways that remotely working attorneys can protect their clients. Other important steps in securing remote work environments: avoiding suspicious websites or links, updating software when necessary, and making sure to only use approved technologies (such as known USB devices or hard drives). Each remote device in your network is essentially another gateway, another potential access point for an attacker; the covid-19 pandemic has brought about a number of nasty attack campaigns for which we should all be on the lookout.

Training on phishing scams and social engineering attacks helps to mitigate some of the threat, as these attacks are regularly conducted through email. As cyberattackers continue to take advantage of covid-19, staying apprised of potential cyber threats is an element of cybersecurity awareness that is required of attorneys. Slowing down can make all the difference when it comes to becoming a victim or spotting an attack. If an email seems strange, unexpected, or urges you to act quickly in a way that violates standard procedures, think twice. Communicating any suspicious activity while working remotely helps to prevent breaches; it also helps to inform clients of when they can expect communications and what they will contain.

Just as client data must remain confidential, ensuring its integrity and availability are top priorities. Managing access controls in-house lessens the risk that client data will be inadvertently (or purposefully) altered or destroyed. Make sure that the IT department is performing regular backups in a sound manner, and that system upgrades are being conducted when necessary. This pandemic has brought about a high number of cyberattacks, especially against those organizations that were underprepared for remote work and are now even more vulnerable. Denial-of-service and ransomware attacks can leave an organization unable to operate for an extended period of time. Having a backup plan protects against the financial, reputational, legal, and operational risks that come with a cyber event.

In many ways, cybersecurity is now more important than ever. Given their reliance on digital devices and communication, attorneys should take special note of their ethical obligations in dealing with client data. Remote work security strategies should be communicated to clients, as well as how they should expect to be contacted during covid-19 (establishing, for example, what types of information will be transmitted via email). Moving out of our physical work spaces does not mean that we can ignore the security protocols governing how we use technology in the office. If anything, additional layers of diligence and information-sharing should be added to account for the complex threats we now face.

Going above and beyond those "reasonable efforts" is necessitated by the extraordinary working situation in which many of us find ourselves. Maintaining a strong personal cybersecurity posture may help to ease some of the risks that a reliance on remote work introduces; it may also ease the minds of clients during a time when many things seem uncertain. ▲

OFFICIAL PUBLICATION OF THE MINNESOTA STATE BAR ASSOCIATION

VOLUME LXXVII NUMBER VII
AUGUST 2020
www.mnbar.org

Bench&Bar OF MINNESOTA

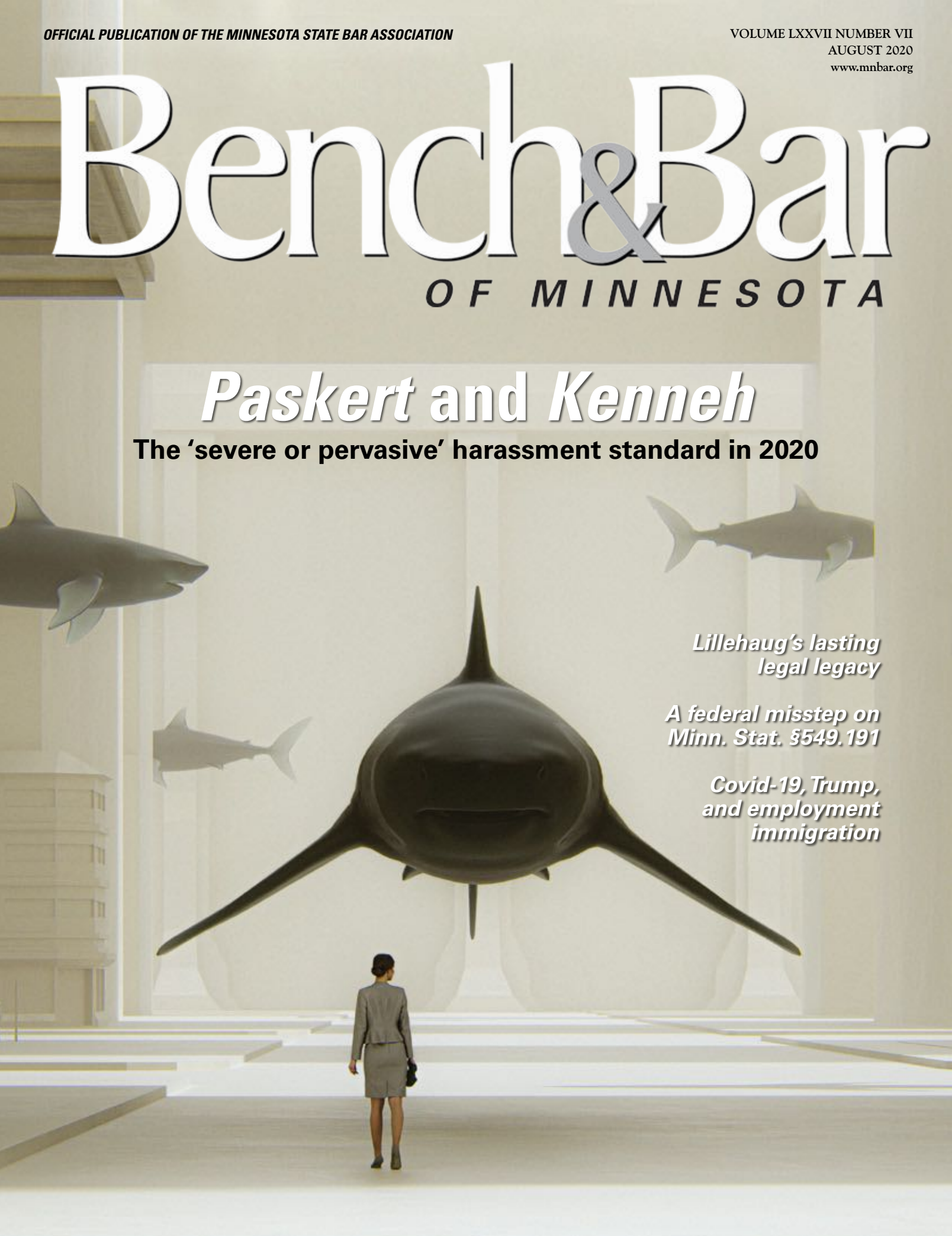
Paskert and *Kenneh*

The 'severe or pervasive' harassment standard in 2020

Lillehaug's lasting legal legacy

A federal misstep on Minn. Stat. §549.191

Covid-19, Trump, and employment immigration



Cyber risk:

Is your data retention policy helping or hurting?

This past June, several U.S. law enforcement agencies were the victims of a largescale data breach resulting in 296 GB of data being stolen. The National Fusion Center Association stated that "dates of the files in the leak actually span nearly 24 years—from August 1996 through June 19, 2020." The statement went on to say that personally identifying information was leaked along with other types of files.[1] The incident was an act of hacktivism and purportedly sought to reveal internal government workings to the public, including details relating to its covid-19 response.

This incident reveals a critical piece of cybersecurity strategizing that sometimes gets overlooked—the value of the data retention policies. Data retention policies outline what types of data are actively being stored, how long that data should be stored, and how it should be destroyed or relocated at the end of that time. Part of the severity of this attack stems from the fact that these agencies were retaining so much old data—data that should have been periodically audited and reviewed. While data is a critical asset, only retaining what is absolutely necessary mitigates the risks associated with a breach.

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.

Within the legal community, attorneys are held to a high standard when it comes to protecting client data. And one size does not fit all: It's complicated knowing when it is appropriate to discard old client files, especially given ethical requirements and the possibility you'll need certain case files in the future. Depending on the jurisdiction, retention policies—and the length of time attorneys are required to hold on to files—may vary. Furthermore, different types of cases and circumstances require different approaches to file retention. A records retention schedule may spark fears that files will be deleted or discarded before it's appropriate to do so. But law firms are also likely to run the risk of holding on to more information than necessary, and for an indefinite period of time.

Creating a legally sound records retention and destruction policy better protects clients from having their information compromised. Essentially, the less data a law firm houses on its servers (or in their storerooms, in the case of paper copies), the more able they are to manage and secure that data. Communicating the records retention policy to clients helps to protect against prematurely deleting client information. In the File Retention booklet distributed by Minnesota Lawyers Mutual, it is recommended that a letter notifying the client be sent prior to its scheduled deletion or destruction date: "The letter should tell the client they are welcome to pick up their file, in its entirety, before a certain date and that failure to do so will result in the file being destroyed. It is also a good practice to include a 'consent to destroy' form."[2] This measure provides an added layer of caution in executing a firm's data retention policy while still working to minimize the amount of data that a firm retains on behalf of its clients.

It should also be noted that the digital destruction of files is more complex than pressing the 'delete' button. Best practices should be followed in forensically destroying data, and any files that are deleted should be recorded for future reference.

While regularly reviewing stored data and creating a record retention policy is important in mitigating the risks associated with data breaches, it remains true that firms are often required to store large amounts of data even for cases that have closed. The key steps in creating a cybersecurity culture focused on protecting client data include: access controls to sensitive data; encryption; and employee education and training about social engineering and the threats associated with the Internet of Things. Appropriate physical security measures should be enacted to best secure physical files and storerooms. While data is a critical asset in any organization, the legal community is especially tasked with safeguarding its data and managing it with the utmost care. Implementing a data retention policy is an important part of that effort. ▲

Notes

[1] *https://thehackernews.com/2020/06/law-enforcement-data-breach.html*

[2] *https://www.mlmins.com/Library/File%20Retention%20Booklet.pdf*

OFFICIAL PUBLICATION OF THE MINNESOTA STATE BAR ASSOCIATION

VOLUME LXXVII NUMBER VIII
SEPTEMBER 2020
www.mnbar.org

Bench&Bar OF MINNESOTA

Covid-19 liability legislation

Force majeure *Hitz* home, excuses rent obligation

***Bostock v. Clayton County* and the future of the MHRA**

One Size Does Not Fit All

Estate planning for blended and nontraditional families

The Twitter breach and the dangers of social engineering

This past July, Twitter fell victim to a wide-scale cyberattack that compromised the accounts of some of its highest-profile users. It was soon determined that the attack was largely orchestrated by a 17-year-old boy, who apparently had a history of online scams—including some perpetrated on Minecraft—that amassed him a huge bitcoin fortune.[1] Twitter posted details about the attack on its blog: "The social engineering that occurred on July 15, 2020, targeted a small number of employees through a phone spear phishing attack… Not all of the employees that were initially targeted had permissions to use account management tools, but the attacks used their credentials to access our internal systems and gain information about our processes."[2] The post goes on to say that the attack focused on exploiting the human vulnerabilities that contributed to its success.

This episode underlines a simple truth that most cybersecurity experts acknowledge: The human element is what ultimately determines the strength of an organization's security posture. No degree of compliance or security budgeting can eliminate the potential for an attack on employees or staff themselves. As in the case of Twitter, once credentials were willingly offered up, the cybercriminals were able to access critical assets and compromise accounts.

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.

Human vulnerabilities are always going to be much easier to hack than technology. In this instance, a 17-year-old boy was able to trick a number of employees at one of the largest tech companies in the world. And the scary thing about it is that it was relatively easy to do. So how do we mitigate some of this continuing, inescapable human risk?

One step that Twitter is taking is to more carefully manage access controls. Twitter has pledged that the company will be improving its procedures and policies to better monitor and restrict access to internal assets. Access controls are a critical piece of an organization's overall security posture. Limiting access to critical data, systems, and networks is a surefire way to mitigate some of the potential risk. The more an employee is able to access, the greater the liability that employee poses in the event of a compromise. Restricting and auditing access controls do not make employees immune to spear phishing attacks, but these measures definitely limit the damage if and when employees become victims.

Second, training and education are always going to strengthen organizational security, but in particular, employees should be reminded that avoiding hastiness is always important when dealing with digital communications. The Twitter hackers conducted their social engineering attack via phone, by convincing an employee that they were calling from the technology department and required their credentials to access a customer service portal.[3] It is important to communicate to employees how personal information will be requested, and to establish that following up in person is encouraged (or required) when a request for personal information has been received. While email is the standard phishing method, it is important to remember that phone calls and texting can also be used to gather information. If anything appears suspect or out of the ordinary, make sure that reporting procedures are in place and that all employees know the designated communication channels. Taking a moment to slow down before acting on a request may make all the difference.

Like all high-profile breaches and cyber events, the Twitter breach should inspire organizations, firms, and companies to take a closer look at their own security postures and implement positive change. Security cultures thrive with top-down management support and a company-wide awareness that security is everyone's responsibility. ▲

Notes

[1] *https://www.businessinsider.com/twitter-hacker-florida-teen-past-minecraft-bitcoin-scams-2020-8*

[2] *https://blog.twitter.com/en_us/topics/company/2020/an-update-on-our-security-incident.html*

[3] *https://www.nytimes.com/2020/07/31/technology/twitter-hack-arrest.html*

OFFICIAL PUBLICATION OF THE MINNESOTA STATE BAR ASSOCIATION

VOLUME LXXVI NUMBER III
MARCH 2019
www.mnbar.org

Bench&Bar OF MINNESOTA

ABA Formal Opinion No. 483, data breaches, and you

Substantial completion and liquidated damages

An interview with Justice Paul Thissen of the Minnesota Supreme Court

The Music Modernization Act, explained

Third-party vendors and risk management

It's always scary to think that sometimes data breaches aren't the result of "hacking" so much as user error. Rubrik, a security and cloud management firm, recently learned this the hard way, when a misconfigured server exposed data belonging to major clients.[1] As organizations use increasingly complex technology to handle increasingly vast amounts of client data, it is becoming more and more difficult to keep up with security demands.

As Rubrik was recently reminded, security demands include proper configuration and hardware setup as well as more advanced security measures of the sort I have mentioned in previous articles. Many organizations overlook the fact that third-party vendors can cause just as much damage in the event of a breach as an internal cybersecurity event. Reputationally, operationally, and financially, where the breach originated doesn't matter as much as who the breach is going to impact most. If the answer is an organization's major clients, I am willing to bet those clients won't care either.

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.

Managing third parties

Most organizations have some degree of third-party involvement in managing internal systems and cloud services, or in helping conduct some operational function. When entering into agreements for these services, it's advisable to have a designated person who is responsible for overseeing the agreement process and guiding the management and review of third-party risk. All third-party vendor relationships come with a degree of risk, regardless of the service they are providing. In the massive Target data breach of 2013, it was a third-party that compromised Target's data, affecting millions of its customers. Keep in mind that this third party provided HVAC and refrigeration services.[2] It goes to show that regardless of the company, third-party involvement always comes with dangers and requires continuing oversight past the initial stages of the agreement. Cyber risk management calls for separate ownership of different levels of risk, including third-party relationships.

Once a responsible person or group is designated for the management and overview of third-party relationships, one key task is to keep track of where organizational data resides. Record where the data is being stored, what type of data it is (especially if it's highly confidential or protected), and how the data is being protected by each vendor. Try to limit which vendors have access to sensitive data and incorporate ongoing reviews and audits as part of continued due diligence. Prior to entering into any new agreements, thoroughly research the prospective party's stance on cybersecurity issues and how they have handled any past incidents. What controls are used for sensitive data and who has access to systems? Do they audit their third-party subcontractors? Do they have an incident response plan? Is it readily available for review? Does it comply with the standards of the internal response plan in place? Asking the right questions can help determine whether the value of a third-party agreement is worth the risk from the outset.

Assessing risk

Service-level agreements should be created in compliance with the same security protocols and policies that regulate internal operations. When an organization trusts an outside source with its data or allows it access to the organization's networks, that source is now an element of its risk profile. If that vendor is vulnerable, so are you. If that vendor has a weak security posture, so do you, no matter how stringent your internal policies are. In addition to the reputational, financial, and operational risks that may be incurred from a third-party security incident, legal risks must also be taken into account—especially in light of HIPAA and GDPR regulations. Transparency about reporting data breaches is critical when it comes to working with third-party vendors; immediate notification of cyber events should be a stipulation of any agreement. Contractual considerations should include access requirements, reputation of the third party, liability, audit procedures, and termination of access to data when the agreement is cancelled or expires.

It is impossible to ensure perfect security, but organizations can take measures to mitigate the risks associated with advanced technology systems and growing volumes of data. Whether it's ensuring proper configuration of systems or controlling access, third-party vendor agreements introduce another element of risk to your organization that may be difficult to fully account for or control. Considering each level of risk, including legal obligations, and promoting regular audits under the supervision of a single responsible individual within the organization can assist in identifying and mitigating the risks associated with third-party involvement. That also includes trying to ensure that the third party has the same dedication to developing cultures of security that your organization does. ▲

Notes

[1] Kelly Sheridan, "Rubrik data leak is another cloud misconfiguration horror story," Dark Reading (1/30/2019). *https://www.darkreading.com/cloud/rubrik-data-leak-is-another-cloud-misconfiguration-horror-story/d/d-id/1333767*

[2] Brian Krebs, "Target hackers broke in via HVAC company," Krebs on Security (2/14/2014). *https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/*

OFFICIAL PUBLICATION OF THE MINNESOTA STATE BAR ASSOCIATION

VOLUME LXXVII NUMBER VI
JULY 2020
www.mnbar.org

Bench&Bar NESOTA

MSBA President 2020-21

DYAN EBERT

Steady as she goes

The big question: Back to the office?

The business interruption pandemic

Ethics wake-up calls for supervisory responsibilities

Child safety first: Reporting child abuse and neglect

Minnesota legislative session recap

Cyber riots and hacktivism

As the calendar turned to June and the nation continued to cope with the aftermath of the killing of George Floyd, the Minnesota Senate allegedly fell victim to the international hacktivist group Anonymous. On June 2, the Senate's servers were breached and passwords used by senators and staff were accessed, resulting in web pages going down. As noted in the Pioneer Press, "In a tweet, the hacking movement Anonymous highlighted the hack, which appears to have included a defacement of a Senate web page showing an Anonymous calling card and saying 'Justice for George Floyd.'"[1] While it cannot be definitively determined whether this was really an Anonymous attack, it comes in the midst of a number of distributed denial of service (DDoS) attacks against Minnesota government web pages. Even as rioting recedes in the streets of Minneapolis and throughout the nation, cyber rioting and hacktivism will continue to be of concern.

'Hacktivism' can be defined as acts of cybercrime motivated by political or social causes. Anonymous is an international, decentralized hacktivist group that is being reenergized by the recent protests.[2] Since there is no clear leader to this group, new factions can be created very quickly and work together to enact largescale attacks. The social upheaval and widespread anger washing over our world fuels this group and makes it attractive to those who want to protest and riot from a distance, "anonymously."

Threat actors tend to have financial gain as their primary motivator. Ransomware and phishing attacks are typically examples of money-driven cybercrime. Hacktivism is more personal, and the mindset of a hacker with a social or political agenda may have an impact on how an attack is conducted. Apart from the team effort that groups like Anonymous are able to marshal, hacktivist attacks may be more tenacious than your average cybercrime venture, and government entities may be particularly targeted.

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.

The risks of a hacktivist attack are largely operational, as is evident by the recent attacks perpetrated in Minnesota. DDoS attacks seek to make a system or network unusable for a period of time by disrupting services to users. Government websites and data will most likely continue to be threatened by hacktivist groups, in addition to law enforcement agencies. Companies and organizations with government clients or contracts and individuals related to those involved in the tragic death of George Floyd may also encounter a greater number of cyber events.

As we continue to struggle with the ongoing limitations spawned by the coronavirus pandemic and compounded by the recent events calling for social reform and justice, it is important to consider how our clients and colleagues may be affected digitally as well as in "real time." Staying apprised of best cybersecurity practices and keeping up with the current cyber landscape is important to ensuring the safety and efficiency of our digital spaces, especially as many of us continue to work remotely.

In closing, a lesson from the Minnesota Senate hacking: It is always wise to avoid having a "Passwords File." Passwords stored in text files on network-connected devices contributed to the scope and severity of this breach. Regular backup policies, VPNS, avoiding public WiFi, and the general advice to "slow down" online in an effort to reduce the risk of falling prey to phishing attacks are all simple ways to mitigate cyberthreats. ▲

[1] *https://www.twincities.com/2020/06/02/minnesota-senate-computers-hacked-passwords-file-accessed-web-pages-down/*

[2] *https://www.reuters.com/article/us-minneapolis-protests-anonymous/hackers-and-hucksters-reinvigorate-anonymous-brand-amid-protests-idUSKBN23A06I*

Compliance & Ethics Professional®

April 2016

A PUBLICATION OF THE SOCIETY OF CORPORATE COMPLIANCE AND ETHICS

www.corporatecompliance.org

Meet Mark Lanterman

Chief Technology Officer
Computer Forensic Services
Minnetonka, MN

See page **14**

an interview by Adam Turteltaub

Meet Mark Lanterman

Mark Lanterman (mlanterman@compforensics.com) was interviewed in January of 2016 by **Adam Turteltaub** (adam.turteltaub@corporatecompliance.org) VP Membership Development at SCCE/HCCA.

AT: Cybersecurity is a bit of a nightmare issue. We just did a survey among compliance professionals, and they named it one of their top areas of concern for 2016. It's not surprising, given the headlines. I also well remember a couple of years ago at the Compliance and Ethics Institute when the Director of the FBI gave a scary talk on the topic. Is the risk getting greater or smaller?

ML: That's a good question. The best answer I can give is this—it's all proportional. By that I mean, the threats are no doubt growing in size and scope. As we come to rely more and more on technology, the bad guys are seeing more and more potential to steal and line their own pockets. By its nature, cyber threat intelligence is always a step behind the bad guys. Therefore, the risk is definitely one that is growing and will persist well into the future. Luckily, though, awareness and the market for digital security are also growing.

AT: One of the things that I find most troubling about this issue is that there are so many potential intruders. You could have a hacker wanting to access your system for fun or malicious reasons, state actors and competitors looking for trade secrets, and let's not forget employees with a grudge or who are just careless. How would you prioritize the risks among these and other potential sources of breach?

ML: Motive is important in analyzing and understanding cyber breaches in order to prevent them. However, I don't think it should matter what a hacker's motive may be. Every breach should be treated as a malicious, serious, and potentially damaging threat. That said, the nature of different threats, and consequently, the potential damage of a breach, is really dependent on an organization's digital infrastructure. Thus, organizations are really in the best position to rank these threats for themselves. We have certainly seen that different organizations are in different spots on the spectrum.

Our primary observation over the years has been that data breaches occur because of a simple lapse of judgement. The single most important aspect of security is people.

AT: Are there specific strategies that companies should employ to counter each of these threats? If so, what would they be?

ML: While there are specific measures that organizations can take, it is highly dependent upon the variables in a given organization. In other words, there is no "one size fits all" for a strong digital security plan. Furthermore, the technology changes on a daily basis. The most secure companies are the ones that do not let their security plans grow stagnant. The best are those that account for changes in the technology, educate employees, and audit consistently.

AT: What do the strategies all have in common? Put another way, what should every company be doing right now?

ML: Our primary observation over the years has been that data breaches occur because of a simple lapse of judgement. The single most important aspect of security is people. The human element of technology is just as, if not more, important than the tech itself. It can only ever be achieved through education and strong implementation of written digital use policy. I like to refer to this as fostering a "culture of security." Therefore, I think that companies should be educating their employees on a regular basis about the realities of digital attacks, how to recognize them, and what to do in the case that something does happen. Such education programs should cover everything within the company's digital security policies—from mobile devices, to social media, to passwords and encryption and backups.

AT: What are some of the common mistakes you see companies making when it comes to shoring up their cyber defenses?

ML: I think the biggest mistake I have seen is over-confidence. Many organizations believe that they have done all they can to prevent a breach, and are thus absolved from putting in place any sort of contingency plan should a breach occur. These organizations adopt a posture of: "Something like that cannot possibly happen to me." When breaches

happen, too often the C-suite executives are caught looking like deer in the headlights. As the old adage goes, "Hope for the best, but prepare for the worst." Therefore, I recommend that an organization take the time to delegate roles and responsibilities and have a plan of action should its worst fears be realized.

AT: Compliance officers are increasingly getting involved, if not taking charge, of this aspect of IT. What's the first thing a compliance officer should look for when assessing the risk of cyber attacks, and their company's defenses?

ML: Compliance officers have an interdisciplinary job. They need to educate themselves not only about how the different technologies within their organization's network, but more importantly, they need to understand how those technologies are being used. I advise compliance officers to remember one key fact: No hacker (unless you have been breached already) knows more about your organizations digital infrastructure than you. Compliance officers have the potential to learn everything there is to know about an organization's digital and non-digital assets. I recommend that compliance folks take the time to not only learn the tech, but also use their discretion to prioritize which assets need the most protection.

AT: How much does a compliance officer need to "get into the weeds" of security protocols and other technical factors? Is it time to get some training, or best to leave the technology decisions to the experts?

I advise compliance officers to remember one key fact: No hacker (unless you have been breached already) knows more about your organizations digital infrastructure than you.

ML: In order to effectively manage and audit digital security, compliance officers should absolutely have a general understanding of the technology to a point where they would feel comfortable with the jargon between Legal and IT in the event of a breach. It is important to know about what happened in order to report it and prevent it moving forward. As far as "getting into the weeds" or minutiae of the technologies, I don't think that is necessary. I think the best compliance officers know that when it comes to digital security, outside vendors and digital security contacts are absolutely necessary in most cases, no matter how many details a compliance officer knows about the tech.

AT: You do a lot of computer forensic work, which leads to another area of cybersecurity: making sure you aren't holding onto documents longer than you should. Are companies getting better about their document retention practices? Or do they still have policies and haven't gotten to the real putting-them-into-practice stage?

ML: That is an excellent point. Document retention practices are actually a key aspect of digital security. Keep too much for too long, and you have that much more information that can potentially fall into the wrong hands. Keep too little, and there may be serious inconvenience factors, costs, and other issues. A good security plan always accounts for the volume and type of data that is available. More importantly, it also addresses where the most important digital assets are located,

so that the proper resources can be diverted to an organization's "crown jewels." But this question is really dependent on the policy choices an organization and, perhaps in some cases, what an industry's standard dictates.

AT: I remember a few years ago there was a lot of press about companies getting rid of old photocopiers and not realizing that thousands of their documents might be stored on them. I imagine most have gotten better about that, but should compliance officers be worried about all the old laptops and smartphones hanging around? Are they being disposed of properly?

ML: As much as the industry should be concerned about external attacks, it is important to not forget about the smaller, seemingly innocuous security lapses. Data exfiltration from negligence happens all the time, which is a shame, given how easy it is to prevent. Think about a breach in the form physical device theft. For instance, as you know in the healthcare industry, data breaches that affect 500 patients or more must be reported to the U.S. Department of Health. Hundreds of reported incidents involve stolen laptops and phones. With theft, there is clear evidence that data has been stolen. In the case of disposal, companies often fail to securely wipe data before selling or recycling. Failing to recognize this, these types of breaches would never be reported, as no one would expect anything to be wrong.

AT: That leads to one last area to explore: smartphones. These days most everything is kept on them. How secure are they? What should compliance officers be asking their IT teams to make sure that they truly are secure?

ML: Mobile devices have changed how work gets done. While they are often secure, it all depends on how they are used. There are always threats that are unique to mobile computing. For example, like public restrooms, public Wi-Fi should never be trusted like your own. Public Wi-Fi networks are very useful, but there is always a risk in using them, because they can be a portal for cyber criminals to steal your valuable data, including usernames and passwords. This alarming trend is what is known as a "man-in-the-middle" attack. Essentially, this kind of attack enables a hacker to eavesdrop on your Internet connection, intercept your communications, and in some cases, reroute your connections to their own malicious webservers and material. For many websites you may visit regularly, a hacker can remove the encryption from the websites' secure login pages. Again, there is always the persistent and very real increased risk of device theft, not just of smartphones, but all mobile devices. Considering all this, I would suggest that compliance officers ask IT about public Wi-Fi use prevention and data encryption. With encryption, data on mobile devices is rendered inaccessible to a thief.

There are always threats that are unique to mobile computing. For example, like public restrooms, public Wi-Fi should never be trusted like your own.

AT: So, once the company-issued devices are covered, that's only halfway there. There are still the personal devices that employees are using. What protocols should be in place if a company has a "bring-your-own-device" policy?

ML: Unfortunately, in most instances, bring-your-own-device (BYOD) relinquishes some defined, universal security strategy, and inherently gives an organization less in the way of data control, because standard mobile device management tools are not used with employee's personal devices. Many smartphones also offer device tethering, whereby the phone's cellular data connection is shared with other devices. This type of network activity is not monitored. Before simply accepting BYOD as a cost effective and desired approach, ensure that policy is clear and consequences are clearer. Also consider with Legal whether there are special regulatory concerns particular to a certain industry. In some industries, like healthcare for example, such a lack opens up serious liability.

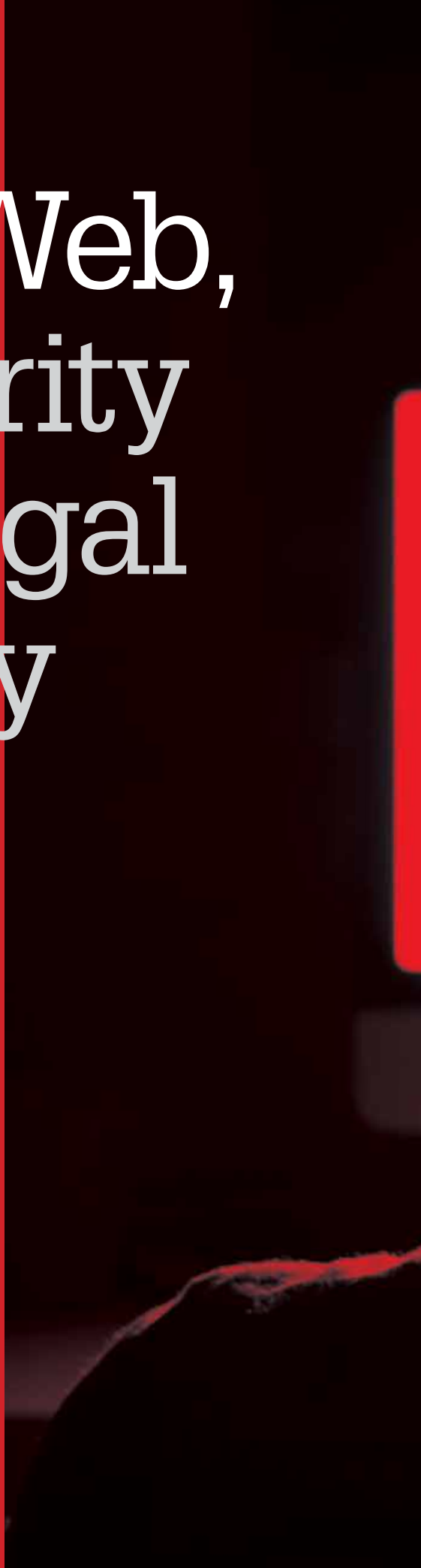
Beyond BYOD, I also urge compliance professionals think about BYOC (bring your own Cloud). The risk with BYOC is two-fold. First, it can be an avenue for disgruntled employees to easily take information with them after leaving. Second, they also pose unique mobile security risks. Interestingly, rather than stealing a username and password, cybercriminals have found a way to steal and use password "tokens" that are stored with a Cloud application on a user's mobile device. These tokens store a user's credentials for convenient access from a trusted device, making it so a user does not have to re-enter a username and password each time they access the app. By using other types of attacks, such as Wi-Fi exploits or a phishing attack, this credential token can be stolen and used to authenticate another untrusted device. Since this token is unique to a legitimate "login" session, it makes detection difficult, and even the service providers will have a hard time detecting the compromise.

AT: Finally, given the threats out there, is it time to start asking a very hard question: Should some of our data NOT be available through our network? Is there some data that's safer if we keep it offline on a desk somewhere?

ML: That is a very hard question and not one I can answer for everyone. It is all about finding that magic recipe that balances convenience with security. It is important to remember that there is no such thing as perfect security, no matter where or how data is stored (whether digitally or on paper). Just because it's not connected to a network does not mean it cannot be stolen. In many ways, storing information digitally allows for greater control of access privileges.

AT: Thank you, Mark for sharing your insights with us.✳

The Dark Web, Cybersecurity and the Legal Community



As technology advances and capabilities grow, so does the number of evolving threats.

By Mark Lanterman

From lightbulbs, cardiac devices and washing machines to the instant communication our smart devices offer, the internet of things (IoT) has impacted nearly every facet of our personal and professional lives. These capabilities offer us unprecedented levels of convenience but also an unprecedented number of evolving threats and a complicated interplay of risks that require constant diligence and attention.

As IoT continues to pervade how organizations operate, the legal community must adapt to uphold the highest standards in protecting client data and operational integrity. With tasks ranging from considering cyber liability insurance policies to budgeting appropriately in reactive and proactive cybersecurity practices, counteracting the magnitude and variety of cyber threats that the average firm faces can seem like a daunting task.

THE RISE OF THE DARK WEB

Often considered to be a "far away" threat, the risks associated with the dark web are often underestimated. The internet that most of us know—Amazon, email, retail websites, news sites and social media—only accounts for a small fraction of the entire internet. The dangers lurking in the dark web are like the deepest parts of an expansive and mostly unknown ocean, with regular internet browsing patterns represented by a clearly visible and accessible shoreline.

For the legal community, the dark web presents several risks, many of which aid a cybercriminal in executing attacks. From information gathering in the wake of a breach to opening credit accounts using purchased card numbers, cybercriminals rely on the dark web.

Clients expect the utmost care in ensuring the confidentiality of their data. Law firms are prime targets of cybercriminals because of the value of the data they collect and store. In this article, I will discuss some of the primary threats that a firm may encounter, the types of risk associated with these threats, and steps to both prevent and mitigate damages in the event of an attack.

ADDRESSING MALWARE

One significant risk for law firms is the installation of malware via social engineering attacks. "Malware" is bad software that is installed by bad actors with the intention to exploit vulnerabilities in code, which allows for other forms of software on the targeted systems to act the way the cybercriminals want it to. Once malware is installed, data exfiltration, operational dysfunction, control of the device by the cybercriminal or ransomware attacks can all ensue. Viruses, worms, rootkits, ransomware and spyware are all types of malware that can be installed in a variety of ways, and all pose significant risks to a law firm. However, the primary method that cybercriminals tend to utilize in disseminating malware is social engineering.

Social engineering attacks take advantage of the all-too-forgotten "human" element of security. Instead of compromising technological weaknesses, cybercriminals will go for a route that typically takes a lot less work. Phishing emails are probably the most common social engineering tactic. A typical phishing email appears to be sent from someone we know, maybe a boss or co-worker. The email will often request a confidential task that needs to be done right away. "I am busy right now and can't talk on the phone. I need a $50,000 wire transfer. This needs to be done immediately, so don't tell anyone about it. Thx." When the request seems urgent and especially if it appears to be coming from upper management, an employee may feel pressured to follow through without double-checking or ensuring the validity of the demand. These emails can often appear legitimate, including details that would at face value seem to only be known by the sender.

Social engineering attacks are often strengthened and personalized by a method known as doxxing. Doxxing is the act of publicly identifying or publishing private information about a person, often with malicious intent. To strengthen an attack by personalizing it to the target, a cybercriminal will frequently visit personal information reseller websites to gather as much information possible. The dark web may also be a source of information.

Perhaps more damaging though is information willingly put out on the internet by the targets themselves. Social media can be a cybercriminal's best source of information. Posting personal information, even something as innocuous as when you are going to be out of the office on vacation, can be used to bolster a social engineering attack and result in data exfiltration, financial damage or reputational

Law firms are prime targets of cybercriminals because of the value of the data they collect and store.

harm. Legal consequences can also ensue, as well as operational dysfunction.

THE RISK TO LAW FIRMS

The risks associated with cyberthreats are both immediate and ongoing and extend far beyond a firm's financial strength. An attack that compromises the confidential data of a firm's clients can severely impact that firm's reputation and overall success. In our digital age, the legal community has the huge responsibility of ensuring the confidentiality of its clients' digital information. Any breach in this trust is going to have immediate and long-lasting repercussions.

Cyber attacks also pose significant financial and operational risks. Responding to an attack, especially if a firm has no pre-existing plans or protocol in place, can be incredibly expensive and time-consuming. A ransomware attack that requires financial payments to regain access to client data can cost a firm thousands of dollars.

Operationally, an attacker may gain access to a firm's devices, making day-to-day operations impossible to conduct for a period of time. The ongoing legal risk associated with an attack, especially in the event of client data being compromised, can further contribute to a firm's financial losses and reputational damage.

PLANNING AHEAD

To counteract these threats and mitigate the associated risks, thinking ahead is a firm's best approach. Combining proactive and reactive cybersecurity strategies is critical, as well as designating in-house parties responsible for cybersecurity and ensuring top-down management support of security protocols and procedures. Proactive cybersecurity strategies include the development of a cybersecurity team responsible for ensuring the development and implementation of cybersecurity standards, and the establishment of clear communication channels in the event of a cyber attack.

Moving beyond the IT department, creating a culture of security requires interdepartmental support, especially from upper management. If an employee receives a phishing email, he or she should know how to (or not to) respond and how to report the incident to appropriate parties.

Proactive solutions should also consider best practices in regard to email encryption, fortifying networks, implementing controls, the security of third-party vendors, physical security, the institution of regularly scheduled security assessments that include vulnerability scanning as well as penetration testing and employee training and awareness programs.

Part of a proactive cybersecurity approach is that a firm knows how it will respond in-house and publicly if it is made victim to an attack. Having a third-party security vendor on hand for assessment and mitigation is often a necessary first step; gathering accurate information about the scope and damages of a breach is important in addressing the public and mitigating ongoing damage. Reporting procedures and requirements should also be understood prior to an incident occurring.

Our interconnected world has made things easier but also more complex. When technology works in our favor, it makes everything better. Data can be collected and stored easily and in huge amounts, communication is instant and the operations of our organizations are made possible. Credit freezes and good "cyber hygiene" may prevent some of the dangers associated with the dark web and the personal information that may be readily available there. When cybercriminals take advantage of technology, the results can be disastrous, especially within the legal community. Acknowledging the ever-evolving threat landscape, as well as its associated risks, can help keep a firm one step ahead. **LP**

Mark Lanterman is the founder and chief technology officer of Computer Forensic Services. Before entering the private sector, Mark was a member of the U.S. Secret Service Electronic Crimes Taskforce. He has testified in over 2,000 cases. **info@compforensics.com**