MITIGATING CYBER RISK DURING THE COVID-19 NEW NORMAL

By Craig R. Blackman, Peter Bogdasarian and Rachel Ortiz

**Stradley Ronon hosted Rachel Ortiz as a 2020 summer associate in the firm's Philadelphia, PA, office.*

COVID-19 is driving tremendous uncertainty in the professional workspace, particularly concerning where workers will physically perform their job. When the pandemic first struck, CEOs were impressed with workers' ability to adapt to remote working environments. Some companies quickly embraced the efficiencies and cost-cutting opportunities that resulted from pandemic-driven telework and committed to long term remote work.[1]

However, cracks are beginning to emerge as workers continue to telework long after most expected a return to their physical workplaces. Some businesses are noticing that projects are taking longer, training is more difficult, hiring and integrating new employees is more complicated, and younger professionals are not having the same opportunities for development as they would have in the typical in-office environment.[2]

Some of the initial efficiencies recognized are now being attributed to the fear that employees felt when the pandemic began, of losing their job if they failed to perform at the same level as in-person operations. Such fear-driven productivity is proving unsustainable.[3]

The Bureau of Labor Statistics reports that only 29% of Americans were able to work from home pre-pandemic.[4] Surveys show that post-COVID-19, most workers want the option to work from home at least part-time.[5] Thus, many companies are now envisioning a hybrid future where employees can work remotely part of the time and work from the office for the remainder of their workweek.[6]

SIGN UP FOR THE FREE WEBINAR!

We will be hosting an interactive webinar in February or March with a more comprehensive discussion on Mitigating Cyber Risk. Please send your questions about Mitigating Cyber Risk to cblackman@stradley.com and pbogdasarian@stradley.com, and we will try to address them during the webinar. ***If you are interested in attending, please visit Stradley.com and click the event page for registration details and more information.***

Whatever the new normal looks like, it is widely accepted that teleworking is inherently less secure than working from the office.[7] Further, a hybrid approach could prove even riskier as far as cybersecurity and cyber-risk are concerned.

As we approach this new normal, there will be a learning curve. Unforeseen security challenges will pop up, just as they did when workers first shifted to remote work at the beginning of the coronavirus shutdown. For example, the shutdown drove huge growth in the use of platforms like Zoom and Microsoft's Teams.[8] For corporate users, encryption and privacy on these platforms are critical to safeguarding valuable company information and meeting practical and statutory privacy obligations to customers.[9] Trial and error forced some companies who initially relied upon Zoom to quickly ban its use for corporate content because the platform did not meet basic security requirements at the time.[10]

(Continued on page 48)

Mitigating Cyber Risk During COVID-19

(Continued from page 47)

Security officials are better able to manage and secure information technology networks in an office or other captive workspace environment. Employees' home Wi-Fi networks likely have weaker protocols that hackers can access more easily.[11] The Cybersecurity and Infrastructure Security Agency (CISA) found that even where organizations use virtual private network (VPN) solutions to connect employees to their networks, new vulnerabilities are being found and targeted by malicious cyber actors.[12]

The COVID-19 pandemic also seems to have ushered in a resurgence of state-backed hacking.[13] The hacking was targeted at COVID-19-related data.[14] However, those hackers are now trained and likely won't be going anywhere anytime soon. In April 2020, security experts at Google sent 1,755 warnings to users whose accounts were targets of government-backed attackers.[15] These hackers targeted business leaders in financial services, consulting, and healthcare around the world, including in the United States.[16]

In general, hacking and phishing attempts have increased during the pandemic.[17] Malicious actors are successfully preying on workers' anxieties and fears surrounding the pandemic[18], and exploiting the uncertain circumstances to increase their rate and scope of cyberattacks.

Finally, the U.S. workforce is largely unsophisticated when it comes to teleworking, which could be exacerbated if and when organizations move towards a hybrid work schedule. When workers constantly switch from office to remote work, an organization risks complacency. And complacency risks exposure. Entities with private personal, health, or financial data, like law firms, brokers and financial advisers, and medical offices, must protect their clients' sensitive personal information. While working from home, telephone and other communications must remain confidential. These businesses must find ways to guard against the predictable tendency for employees to be less careful while teleworking. Going back and forth from the office to remote working will require a heightened level of vigilance.

Best cybersecurity practices for remote or hybrid work start with educating and training the workforce.[19] Employees must know what to look for and how to prevent phishing or malware attempts.[20] Issuing employer-owned devices for all workers with defined security is ideal.[21] Employers must keep software and systems updated, ensure that their workforce is using strong passwords, and regularly monitor accounts for suspicious activity.[22]

The future of cybersecurity likely involves leveraging powerful technologies such as artificial intelligence (AI) and automation.[23] AI can be used for fraud detection, malware detection, intrusion detection, scoring risk in a network, and user/machine behavioral analysis.[24]

In the present, there are several steps organizations can and should be taking to mitigate their cyber risks:

1. **Continue to develop awareness among the organization's personnel:** With many employees placed into an unfamiliar remote work environment, it is more important than ever to develop their ability to detect (and report) cyberattacks and to train them to recognize that threat actors may deploy new forms of attacks to take advantage of the disruptions of COVID-19. For example, deploying phishing simulation tests themed with pandemic-related content may lead to substantially a higher click-through rate among users.[25] Now is a good time to reflect on the organization's security awareness plan as it relates to training users and testing the efficacy of said training.

2. **Regaining control over the network:** For many years, cybersecurity professionals concentrated their efforts on securing the "perimeter" of the network,

with the idea that the worst threats would originate from outside the network. As threat actors became more skilled at infiltration and internal threats became more prominent, the industry began to question the reliability of this model. The sudden mass migration to a remote work argument has now put an end to the notion that the best way to defend the network is to simply secure it against exterior access while extending unlimited trust to users inside the network.[26] The challenge now facing companies is how to configure remote work solutions in a fashion that avoids creating new infiltration routes into the core network, and that provides a measure of comfort that IT and security are aware of what is going on inside the walls.

As noted above, for many users, VPNs have been at the forefront of their remote work experience. The concept behind the VPN approach is traffic is encrypted and sent through the VPN's internet connection. However, what traffic is redirected through the VPN connection is a question of configuration, and a VPN network may not be configured to direct all of a user's traffic through the VPN network (called "split tunneling") and this configuration, while beneficial from the standpoint of lessening the load on the network, may create its own opportunities for a threat actor to attack.[27] Therefore, it is important to reassess how employees connect to the organization's network and whether additional education is required regarding the limitations and vulnerabilities of the organization's remote work solution(s). Are patches being distributed in a timely manner? Can remote access be configured in a manner to increase security without compromising the essential user experience?

3. **Understanding your organization's remote tools:** As alluded to earlier, the sudden transition of the workforce to reliance on online conference and collaboration tools created vast incentives for mischief (so-called "zoom bombing" and similar misbehavior) along with more destructive attacks. Users then needed to be educated on the security controls built into these tools and on how to configure their use to avoid exposing the organization to these kinds of attacks.[28]

4. **Maintain a firm grip over your IT devices and resources:** "Shadow IT," reflecting the deployment of technological solutions outside of the purview of the IT department, is a greater threat than usual in a remote work environment as the temptation for users to find a solution to an immediate need will place them in tension with IT best practices.[29]

(Continued on page 50)

Mitigating Cyber Risk During COVID-19

(Continued from page 49)

In a remote work environment, IT needs clear channels of communication for recognizing, confronting, and resolving these kinds of business needs in a manner that does not compromise the safety and security of the organization's data and networks.

5. **Planning for resignations, furloughs, and layoffs:** Many organizations have not had to plan for how to handle employee departures outside of the normal office environment. Terminating employee access to the network, retrieving employer-provided devices, and ensuring the return and disposal of the employer's data now present a host of new challenges, especially for companies whose employees may have become geographically dispersed after the transition to the work from home environment. If the Human Resources department hasn't been confronted with these issues to date, then now is the time to put together a plan.

If you are interested in more information on this topic, check out our related article: *Nonprofits Evaluate Risks of Pandemic-Driven Technology,* which discusses how nonprofit organizations can limit the risks associated with pandemic-driven technology.

[1] Chip Cutter, *Companies Start to Think Remote Work Isn't So Great After All*, Wall St. J. (July 24, 2020), https://www.wsj.com/articles/companies-start-to-think-remote-work-isnt-so-great-after-all-11595603397.

[2] *Id.*; [3] *Id.*

[4] Carrie Rubinstein, *Beware: Remote Work Involves These 3 Cyber Security Risks*, Forbes (Apr. 10, 2020), https://www.forbes.com/sites/carrierubinstein/2020/04/10/beware-remote-work-involves-these-3-cyber-security-risks/#1671a13661c4.

[5] *Id.*; Cutter, *supra* note 1. ; [6] *Id.*

[7] Peter Henderson et al., *Hacking Against Corporations Surges as Workers Take Computers Home*, U.S. News (April 17, 2020), https://www.usnews.com/news/technology/articles/2020-04-17/hacking-against-corporations-surges-as-workers-take-computers-home.

[8] Kanishka Singh et al., *Zoom Participant Numbers Top 300 million Despite Growing Ban List, Shares Hit Record (April 23)*, REUTERS (April 23, 2020), https://www.reuters.com/article/us-zoom-video-commn-encryption/zoom-users-top-300-mln-despite-growing-ban-list-shares-hit-record-idUSKCN22420R.

[9] *Id.*; [10] *Id.*; [11] See Rubinstein, *supra* note 4.

[12] Cybersecurity & Infrastructure Security Agency, *Cybersecurity Resources for COVID-19*, U.S. Dept. of Homeland Security, https://www.cisa.gov/cybersecurity-resources-covid-19 (last visited July 17, 2020).

[13] Anurag Maan, *Google Sees Resurgence in State-Backed Hacking, Phishing Related to COVID-19*, REUTERS (May 28, 2020), https://www.reuters.com/article/us-health-coronavirus-cyber/google-sees-resurgence-in-state-backed-hacking-phishing-related-to-covid-19-idUSKBN2340CH.

[14] *Id.*; [15] *Id.*; [16] *Id.*; [17] See Henderson et al., *supra* note 7.; [18] *Id.*

[19] Christina Quaine, *Taking a Closer Look at Remote Workplace Fraud Vulnerabilities: How to Mitigate Escalating Threats*, *Security Magazine (June 11, 2020)*, https://www.securitymagazine.com/articles/92588-taking-a-closer-look-at-remote-workplace-fraud-vulnerabilities-how-to-mitigate-escalating-threats.

[20] *Id.*; [21] *Id.*; [22] *Id.*; [23] *Id.*; [24] *Id.*

[25] Michelle F. Davis, Max Abelson, and Donal Griffin, *Greed and Fear Collide: Wall Street Calls Traders Back to Office*, BLOOMBERG (April 7, 2020), https://www.bloomberg.com/news/articles/2020-04-07/greed-and-fear-collide-wall-street-calls-traders-back-to-office (last visited Sept. 13, 2020) ("The firm later ditched the plan and sent people home, where employees received an important email from a top executive: 'Highly Confidential: COVID-19 - Staff Infection List.' Workers who clicked the attachment realized it was an anti-phishing test on behalf of the compliance team and that they had failed it."); World Health Organization, *Beware of criminals pretending to be WHO*, https://www.who.int/about/communications/cyber-security (last visited Sept. 13, 2020); Centers for Disease Control and Prevention, *COVID-19-Related Phone Scams and Phishing Attacks*, https://www.cdc.gov/media/phishing.html (last visited Sept. 13, 2020).

[26] Sam Greengard, *The Perimeter is Dead* (April 30, 2018); https://www.securityroundtable.org/security-without-boundaries-perimeter-dead/ (last visited Sept. 13, 2020); Tim Brown, *Patrolling the New Cybersecurity Perimeter* (Jun. 21, 2019); https://www.darkreading.com/perimeter/patrolling-the-new-cybersecurity-perimeter-/a/d-id/1334985 (last visited Sept. 13, 2020); Jayne Lytel, *Why traditional network perimeter security no longer protects* (June 9, 2020); https://www.helpnetsecurity.com/2020/06/09/zta-perimeter-security/ (last visited Sept. 13, 2020).

[27] Susan Bradley, *How to minimize the risks of split tunnel VPNs* (April 29, 2020), https://www.csoonline.com/article/3539509/how-to-minimize-the-risks-of-split-tunnel-vpns.html (last visited Sept. 13, 2020).

[28] For an idea of where to begin, see: Kristen Setera, *FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic* (March 30, 2020), https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic (last visited Sept. 13, 2020).

[29] For example, users may seek to find software solutions to the problem of how to scan documents in a remote work environment and some of these software solutions may host data on the cloud or in some other fashion that is incompatible with the organization's policies and procedures.

About the Authors:

Craig R. Blackman is a partner and co-chair of the Insurance Practice Group at Stradley Ronon Stevens & Young, LLP, in Philadelphia, PA. He focuses his practice on a variety of insurance industry issues, including cyber, commercial and personal lines, directors & officers, and environmental. He can be reached at cblackman@stradley.com or 215.564.8041.

Peter Bogdasarian is a counsel in the Cyber & Privacy Group and serves as Chief Privacy Officer to Stradley Ronon Stevens & Young, LLP. He focuses his practice on general litigation matters and also counsels clients in connection with data privacy and cyber security-related issues. He can be reached at pbogdasarian@stradley.com or 202.419.8405.

Stradley Ronon hosted Rachel Ortiz as a 2020 summer associate at the firm's Philadelphia, PA office.

About Stradley Ronon: Counseling clients since 1926, Stradley Ronon has helped private and public companies – from small businesses to Fortune 500 corporations – achieve their goals by providing pragmatic, value-driven legal counsel. With offices in seven strategic locations, including the Route 422 Corridor, our responsive team of more than 200 attorneys seamlessly addresses the full spectrum of our clients' needs, ranging from sophisticated corporate transactions, complex commercial litigation, and employment/labor matters to real estate transactions and trusts and estates work. The firm has offices in Malvern, PA; Philadelphia, PA; Washington, DC; New York, NY; Chicago, IL; Cherry Hill, NJ; Wilmington, DE.

NONPROFITS EVALUATE RISKS OF PANDEMIC-DRIVEN TECHNOLOGY

By Jennifer Gniady & Peter Bogdasarian, Stradley Ronon

As nonprofits enter the last quarter of a year like no other, many have adapted to the pandemic's challenges through technology. Employees have pivoted to working from home via laptops and wi-fi, staff and client meetings take place on video platforms, and even fundraisers can be held online without either cocktails or chicken dinners. But these technology stopgaps carry their own risks that should not be underestimated by nonprofits.

Consider the news in September 2020 that the Jewish Federation of Greater Washington suffered the diversion of $7.5 million of its endowment fund in unauthorized transfers to international accounts. An investigation is ongoing but indicates access was facilitated through the e-mail accounts of employees working from home, possibly on personal computers. E-mail, remote access, video-conferencing software and file transfer programs used by employees all create potential openings into an organization's information and operations. Many nonprofits also rely on third-party vendors for critical services and software, which come with risks highlighted this summer when the cloud computing provider BlackBaud disclosed a ransomware attack that left its customers' donor information exposed.

Tight budget constraints and a culture that often minimizes operating and overhead costs may contribute to nonprofits giving short-shrift to mitigating these risks. Nonprofits may have minimal staff to assess and respond to technology risks or rely on third parties whose contracts and locations limit the speed and scope of their response. And while many nonprofits don't consider themselves in the same category of risk as a bank or financial services firm, even organizations without hefty endowments can have significant losses. Information about donors and clients, including their payment information, eligibility for services, health and insurance, or contribution history, can be valuable currency in the wrong hands. The organization also risks losing donors, grants, and the trust of those it serves through its charitable mission.

High-profile losses may be rare, but the organization can lose data in more routine ways that won't make the news in this new virtual environment. Consider the following scenarios:

• An employee needs to be terminated for cause but is working from home with full access to company systems through an organization laptop and accounts. Does your organization have a plan for securing the accounts, as well as the return of the organization's technology?

• Your communications director maintains organization accounts on multiple social media accounts, as well as corporate access to accounts for mailing lists services, website content management software, and news distribution services. Does your organization keep an inventory of accounts and understand how they are used and who else has access to them?

(Continued on page 52)

Nonprofits Evaluate Risks of Pandemic-Driven Technology

(Continued from page 51)

• An employee working off-site loses a corporate laptop and security key fob that provides authentication, or worse, decides to quit without notice and not return these items. Does your organization keep a regular inventory of physical technology assets and have clear procedures for employees to report the loss of phones, computers, or security devices? Do you have a plan for forensic data recovery, including an understanding of the costs to rebuild or restore lost data?

Legal counsel can be as critical as the right technology strategy in these situations. For our nonprofit clients who are thinking about ways to limit risk, the Stradley Insurance practice has put together an overview of mitigation strategies to serve as a starting point for your own review. And we can help with finding the resources you need to address these issues, whether it means evaluating your collection, retention, and disposal of data containing personal, financial or health information, reviewing your contracts with technology vendors, evaluating a cyber-insurance policy or claim, preparing appropriate data security policies and procedures, putting in place an employee management plan, or conducting an investigation into a possible loss.

▶ Evaluating your collection, retention and disposal of data containing personal, financial or health information:

- New York's SHIELD Act went into effect in March 2020 and requires any person or business owning or licensing computerized data that contains the private information of a resident of New York to implement and maintain reasonable safeguards to protect the security, confidentiality, and integrity of the private information
- Massachusetts' Standards for the Protection of Personal Information of Residents of the Commonwealth require that every person or business owning or licensing personal information regarding a resident of Massachusetts is required to develop, implement, and maintain a comprehensive written information security program and set a minimum floor for the security covering an organization's computer systems and network
- Although nonprofit organizations are exempt from the California Consumer Privacy Act (CCPA), vendors, providers, and other third-parties are not exempt

▶ Reviewing your contracts with technology vendors:

- Do your vendors maintain reasonable security programs, including adequate cyber-insurance coverage?
- Do you have consistent contract provisions related to security and the handling of a cyber incident?
- What obligations do your contracts impose with respect to the disposal of data?

▶ Evaluating a cyber-insurance policy or claim

- Weighing your organization's need and risk
- Explaining different forms of coverage
- Assessing the details of compliance with your cyber-insurance policy

▶ Preparing appropriate data security policies and procedures

- Does your organization have policies for data classification, password strength, access controls, the use of encryption, data disposal and/or patch management?
- Do you have an Incident Response Plan?
- Do you understand the potential benefits and/or drawbacks attached to contacting law enforcement if your organization is the target of a cyberattack?

▶ Employee Management Plans

- Evaluating employee risks and planning to train employees to prevent losses, protect data, and report problems.
- Ensuring your employee handbook and policies reflect organization expectations about technology, data, and devices.
- Developing a plan for handling remote work, including securing data and devices in the event of a termination.

▶ Investigations into a possible loss

- Providing specialized expertise in retaining and directing computer forensic and other services in connection with a cyberattack or a potential cyberattack
- Analyzing and assessing the legal and contractual duties that could arise from a successful cyberattack on the organization

About the Authors:

Jennifer A. Gniady is Counsel in the Nonprofit and Religious Organizations practice group of Stradley, Ronon, Stevens, & Young, LLP. She advises nonprofits on tax-exempt regulations, governance structures, and fundraising practices. She also specializes in issues unique to religious organizations, such as corporate structures, trusts, and religious protections. She can be reached at jgniady@stradley.com or 202.419.8436.

Peter Bogdasarian is a counsel in the Cyber & Privacy Group and serves as Chief Privacy Officer to Stradley Ronon Stevens & Young, LLP. He focuses his practice on general litigation matters and also counsels clients in connection with data privacy and cyber security-related issues. He can be reached at pbogdasarian@stradley.com or 202.419.8405.

About Stradley Ronon: Counseling clients since 1926, Stradley Ronon has helped private and public companies achieve their goals by providing pragmatic, value-driven legal counsel. With offices in seven strategic locations, including the Route 422 Corridor, our responsive team of attorneys seamlessly addresses the full spectrum of our clients' needs, ranging from sophisticated corporate transactions, complex commercial litigation, and employment/labor matters to real estate transactions and trusts and estates work.