The Risk: Cybersecurity Dangers During and After COVID-19

ALA® Association of Legal Administrators

ALA Association of Legal Administrators

Table of Contents

The Risk: Cybersecurity Dangers During and After COVID-19

Drew Sorrell

Shareholder and Chair, Cybersecurity and Privacy Group, Lowndes and Meritas Member

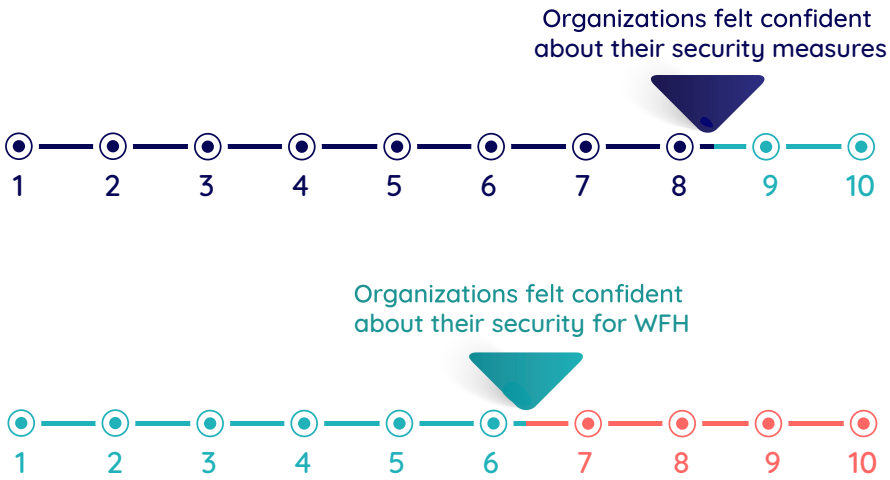
INTRODUCTION

"Nobody expects the Spanish Inquisition!"[1] Likewise, no one expected a global pandemic that would send society into retreat and isolation where *work from home* would become a cliché catchphrase *in these times.* Organizational security was not ready for this event, and whether global cybercriminals were ready can be debated. Regardless, crime will find a way. Given the current circumstance, which is likely to persist well into 2021, this paper examines cybersecurity in the work-from-home (WFH) context.

BACKGROUND

Post-COVID-19 Work-from-Home Technical Vulnerabilities

At the outset of the pandemic, approximately one-third of American employers moved 81% to 100% of their employees to a WFH model, while 70% moved 61% of their workforce to WFH status.[2] According to the same survey, organizations — especially larger ones — felt confident about their organization's security measures, rating it slightly above an 8 on a 10-point scale.[3] However, confidence in their organizational security for WFH was rated materially lower — just above a 6 on the same scale.[4]



In contrast to readiness, the same survey suggested that organizations that had transitioned to WFH felt equally secure working from home as at the office.[5] The surveyors observed that this confidence is probably the product of hubris rather than objective reality[6, 7] because organizations likely do not have day-to-day insight into employee home security settings and access controls, as compared to at the office. Likewise, given the rapidity with which WFH was rolled out, mistakes must exist that are currently latent and subject to exploit.[8] Against this backdrop, this same surveyor noted the material uptick in cyberattacks since the onset of COVID-19 in the United States.[9]

Similarly, another leading technical cybersecurity company reported that COVID-19 was accompanied with a 53% uptick in cyberattacks.[10] The primary WFH issues were identified as endpoint vulnerabilities, virtual private network (VPN, which is the usual encrypted "pipe" for information to flow between home and the office's servers) vulnerabilities and lack of trained security staff.[11] With respect to VPN and endpoint vulnerabilities, the research explained that 27% of attacks preceding the survey included Internet of Things (IoT) attacks with an island-hopping component. In other words, an internet-connected device (such as a cellphone, a tablet or even a *coffee maker*)[12] was used as the initial break-in point for the attacker to then "hop" to another device or system (i.e., hop from one "island" to another).[13] Even more troubling is that 40% of these attacks spread destructive malware as part of the attack.[14]

Timing, Cost and Case Example of Island Hopping and Destructive Malware

By definition, litigation arising from cybersecurity events lags the event giving rise to the suit. An IBM study determined that on average it takes 197 days to detect a breach and another 69 days to contain a breach.[15] As such, courts are not yet seeing a surge in COVID-19-specific breach cases. Based on IBM's numbers, we predict an uptick in cases to begin in December 2020. The IBM study also revealed that the clear majority of companies expected both the time to detect breaches and the cost to contain them would increase due to the added complexities of WFH.[16] Consistently, WFH was expected to add an additional $137,000 in cost to a data breach on top of the current American average cost of $8.64 million.[17]

A U.S. District Court in North Carolina recently issued an opinion illustrative of island hopping and the related difficulty of containing a breach on a personal device. In *Williams v. AT&T Mobility, LLC,*[18] the plaintiff alleged that his cellphone was used as the initial attack vector from which the perpetrator attacked other business systems (i.e., island hopped from an IoT device to attack other systems).

The plaintiff is alleged to be an investor in blockchain technology and digital assets with $1.5 million invested in digital currency mining hardware. For his complaint, Williams alleges the SIM card[19] associated with his cellphone account was illegally transferred from his phone to that of a hacker. In doing so, the criminal gained access to his email and text messages, enabling the hacker to change the passwords of Williams's other accounts.

Williams claims he communicated with AT&T after the first illegal transfer and AT&T assured him that it had added additional security to his account. Six illegal SIM transfers later[20] — which allegedly included, among other things, theft of some of Williams's cyber currency, hijacking certain of his bitcoin accounts, personal threats by the thief against Williams and his family, theft of his Social Security number, and theft of a copy of his passports and passports of certain family members — Williams claims he had

to discontinue currency mining due to the inability to secure his accounts. Likewise, Williams closed his AT&T account and purchased a new phone, with AT&T allegedly refusing to refund the cost of the AT&T phone.

Demonstrating the perniciousness of such attacks during both his and AT&T's attempts to stop the repeated illegal SIM transfers, AT&T supposedly added restrictions to the account that were intended to require that his SIM transfers could only be made in-person at a specific Raleigh, North Carolina, store and that Williams would be required to present *two* passports as proof of identity. Because of the extent of the thieving, Williams also complained that he outright lost access to certain financial accounts due to the thief resetting usernames, emails and "backup/reset" emails. With control of his phone number, the thief was able to send and receive multifactor authentication responses as if they were Williams, thereby "permanently" stealing the accounts.

While the foregoing allegations are still to be proved, AT&T moved to dismiss Williams's initial complaint by making various arguments, including Williams's own supposed negligence in securing his accounts. The court denied the motion to dismiss, permitting it to proceed to discovery and possibly ultimately to trial.[21]

Also of note is that the court permitted Williams's claim for electronic trespass to proceed, with the court citing the seven fraudulent transfers and explaining that to hold otherwise would *de facto* provide immunity to companies for such claims. This is remarkable because it essentially permits a customer to make a claim against a company for the company's improper access of the company's own accounts related to that customer.

Stepping away from *Williams v. AT&T,* class actions are increasingly attempting to target corporate officers and directors for breach of fiduciary duty regarding security oversight. A superior court in California approved a $29 million settlement of consolidated derivative suits against the Yahoo! officers and directors, which included an $8.6 million attorney fee award. The Yahoo! suit targeting officers and directors alleged liability stemming from the data breach of over 1 billion users.[22]

Similarly, in 2019, the Northern District of Georgia dismissed a class action against most of the officers and directors of Equifax arising from the Equifax breach; however, the court did not dismiss the claim against the chief executive officer (CEO), who was alleged to have personal knowledge of the security deficiencies that gave rise to the breach.[23]

Traditionally, large corporations have incorporated in Delaware because it is a corporate-friendly state. Delaware law generally permits corporations to isolate officers and directors from personal liability by including an exculpatory provision in their incorporating papers. This immunity is not unassailable, however, because officers and directors may still theoretically face liability if their failure to prevent a data breach rises to the level of a violation of loyalty, bad faith acts/omissions or knowing violations of law, with the last being particularly relevant to highly regulated industries such as banking and finance. Moreover, Delaware courts have created another opening for director liability for data breach via a so-called Caremark claim.[24]

Caremark permits a showing of lack of good faith when a director(s) (a) utterly fails to implement any reporting or information system/controls, or (b) despite such controls, fails to monitor or oversee such operations and thereby preventing them from receiving information about dangers requiring their attention. While early attempts to link Caremark with data-breach liability have been rocky, the continuing evolution of the law suggests Caremark claims may be successful as the courts continue to define the standard of care and related duties for corporations *vis-a-vis* data security. As of now, no legislative national standard exists leaving the courts to create them from scratch.[25]

SOLUTION

Remedial Measures

Current reports suggest that a COVID-19 vaccine will not be widely available until the second quarter of 2021. Even once a vaccine is available, it is likely that working from home (telecommuting) will continue to be a popular option if for no other reason than the reduction in required commercial footprint and its associated costs. Thus, organizational security should include planning for persistent remote working. But what does that mean?

At the outset, it is clear that organizational security is no longer the domain of the IT department. Rather, organizational security begins with an organization's officers and directors who should be creating and maintaining systems and processes to assure organizational security and ongoing oversight. Organizational security has become a strategic priority:

- Identification, location and format of organizational information requiring protection
- Plans for how that information is to be protected (including any contractual, regulatory or statutory requirements)
- Data retention schedules for such information
- Plans for testing security (remediation or vulnerabilities)
- Employee training plans and schedules regarding the foregoing
- Breach incident response
- Disaster-recovery planning should data be lost, destroyed or stolen

The written plan should be a "living" document that is reviewed and revised on a set schedule or more frequently as needed.

The written plan should incorporate adjustments for more aggressive guidance on acceptable remote working situations, home network security requirements and testing those implementations. Consideration should be given to multifactor authentication, whitelisting remote-working equipment, geofencing access from locations where workers are not present and aggressively monitoring access, systems and software. Of course, IT professionals will all have opinions on what else needs to be done given that each computer system, its software and the operating environment are unique, thus calling for a plan tailored to each situation.

As foreshadowed above, at least one state requires a written information security plan for systems that house information related to citizens of its state.[26] Your company's situation may implicate other federal, state and local statutes and regulations, as well as contractual requirements for vendors and clients — e.g., the Payment Card Information Data Security Standard (PCI DSS), New York SHIELD Act, California Consumer Privacy Act (CCPA) and General Data Protection Regulation (GDPR). That said, a written information security plan will be one of the first documents asked for in a suit arising from a data breach, and while not *per se* required to show your company acted reasonably in securing sensitive data, it will go a long way in that regard. A written plan can be proof positive that the organization took the issue seriously enough to write it down (in a thoughtful way), and the writing itself should help guide the corporation's staff into the creation of a thorough and comprehensive security plan.[27]

From there the plan should identify or inventory the company's data, including its location within the system, its format (e.g., paper or electronic) and the applicable access/security controls. Additionally, companies often keep data "forever" because it "may be useful someday" or no one has the authority to delete it. This legacy data, however, has very little upside but great downside if lost or stolen. Corporations should therefore resist the urge to keep it because it might come in handy one day, as this type of retention policy can do more harm than good.

Once identified, the plan should include security details for the data's protection indexed to the sensitivity of the data. Not all data need be kept in

a metaphorical Fort Knox. Similarly, plans for testing the security of that data should be implemented and routinely tested through paper review, penetration testing and the like.[28]

As suggested above, in the new WFH world, security planning and testing must include consideration to adjustments in security planning for remote and personal systems. For instance, does the employee have an encrypted access point? Do they know how to use a VPN or does the system do that automatically? Who has access to their house and computers, and is that OK? Do they lock the system when not in use? Is their work computer on the same network as their lightly defended internet-enabled refrigerator or baby cam? What if their home is burglarized and the computer (or paper?) records stolen? These scenarios all require a different style of testing than when the assets and information were all accessed and resident "at corporate."

However, the preceding is useless if employees are not trained on the basics of security. This training should include basic understanding of the common attacks and how to respond to them, as well as how to be resistant to them. It should also incorporate training and/or refreshers on corporate security policies and procedures. The results of such training should be recorded to provide for remediation as necessary. As with security leadership starting at the top, so too should training start at the top —executives should be included in such organization-wide training.

Finally, consideration, planning and the written plan should include data breach response (and disaster response). Usually, a data breach response plan is separate from an overall security plan but adjunct to it. Such a plan should identify at a minimum (a) the members of the corporate team, (b) the lawyers, (c) the forensics expert company and (d) the crisis communication company.[29] The response plan should include basic responses and operational procedures. Once the plan is written, the team should actually meet and engage in training that could include a tabletop exercise to learn to work as a team and prepare hypothetical responses to scenarios.

Disaster response is different than security planning, but the two complement each other. Such planning — now — should include planning for disasters befalling an employee's house, if that is where the data is.

CONCLUSION

The paradigm has changed and likely will have changed forever. Companies need to adjust their thinking to account for this new reality. Budget and corporate attention must be commensurate with the risk associated with that paradigm shift. Failing to plan could lead to increased liability for the company and may also lead to personal liability for the executives and directors.

* * *

ENDNOTES

1. "Nobody Expects The Spanish Inquisition." *Know Your Meme,* 9 Sept. 2020, knowyourmeme.com/memes/nobody-expects-the-spanish-inquisition.
2. Malware Bytes p. 7
3. Malware Bytes p. 8
4. Malware Bytes p. 8
5. Malware Bytes p. 23
6. Malware Bytes p. 23
7. An alternative explanation is that employers, having now moved to a work-from-home model for somemonths, have adjusted to and compensated for the security risks of work from home.
8. Malware Bytes p. 23
9. Malware Bytes p. 4
10. VM Carbon Black p. 4
11. VM Carbon Black p. 4
12. Goodin, Dan. *Ars Technica, "*When coffee makers are demanding ransom, you know IoT is screwed". ars-technica.com/information-technology/2020/09/how-a-hacker-turned-a-250-coffee-maker-into-ransom-machine/. Last visited September 28, 2020.
13. VM Carbon Black p. 6
14. VM Carbon Black p. 6
15. ibm.com/security/digital-assets/cost-data-breach-report/#/
16. ibm.com/security/digital-assets/cost-data-breach-report/#/
17. ibm.com/security/digital-assets/cost-data-breach-report/#/
18. 2020 WL 1492803 (W.D. N.C.).
19. SIM stands for "subscriber identification module".
20. Seven transfers in total.
21. *Williams,* at *6.
22. *See In re Yahoo! Inc. Shareholder Litig.*, Case No. 17-CV-307054, (Cal. Supp. Ct Jan. 4, 2019).
23. *See In re Equifax, Inc. Secur. Litig.*, Case No. 17-CV-3463-TWT (N.D. Ga. Jan. 28, 2019).
24. Taking its name from *In re Caremark Int'l Derivative Litigation.,* 698 A.2d 959 (Del. Ch. Ct 1996).
25. The foregoing specter of liability should prompt directors and officers to examine their officers and directors-related insurance coverage in this context. Further, such officers and directors should consider whether the company's state of incorporation permits company indemnification for such claims as well as how their own employment contract treats such issues.
26. Massachusetts law requires such written information security plan but does not as of this writing provide guidance on what that plan should entail. Bear in mind that even if your company does not *per se* operate in Massachusetts, it may still be affected by this law if it maintains records of Massachusetts citizens.
27. Note that the opposite can be true too. If the so-called written security plan is so riddled with half-thoughts, typos and errors, then it may not make sense to even create the document. The document should not be a "check the box we have something in writing" exercise.
28. Note that the creation of the written security plan could and should spur conversations about data recovery in the event of disaster or attack.
29. Along with their after-hours phone numbers and other pertinent contact details.

ABOUT THE AUTHOR:

Drew Sorrell is Shareholder and Chair of the Cybersecurity and Privacy Group at the Lowndes Law Firm. He focuses on complex commercial issues, relating to both litigation and contract/policy drafting. He has years of experience litigating business matters, intellectual property/patent infringement disputes, data breach/privacy issues, wire fraud (spoofing/spear phishing), business torts/disputes, insurance coverage, personal injury and employment litigation. He has drafted and negotiated software licenses (SaaS), internet service provider agreements, data privacy/breach policies and procedures, and employment/services agreements, as well as the indemnity and insurance coverage related to those agreements in website and mobile app accessibility litigation. He frequently publishes and lectures in this area. Lowndes is a member of the Meritas international network of independent law firms.