CYBERSECURITY IN THE AGE OF COVID-19 (AND BEYOND)

May 8, 2020

Brian Vail, QC
Counsel
780-423-7691
bvail@fieldlaw.com

I. INTRODUCTION

The COVID-19 pandemic is causing massive amounts of disruption the world over. Governments have been issuing Orders and passing Legislation to restrict in–person contact and enforce social distancing. Some operations that have been allowed to continue have chosen to close or work remotely from the workplace as much as possible. This means that people are now attempting to "carry on business" remotely from their homes.

Many businesses have radically altered their methods of operating to become more digital. People working from home have been linking to the workplace servers and videoconferencing for meetings and hearings. People have been communicating more by electronic messaging (such as emails or text messages) than was previously the case. Many businesses are increasing or facilitating the sale of their products or provision of their services online. There is an increased reliance on online ordering of products followed by delivery or curbside pickup. As the Conference Board of Canada puts it:[1]

> With governments and organizations enforcing social distancing to curb the spread of COVID-19, businesses and consumers are relying more on digital solutions for economic and social activities. Online conferencing, e-commerce, social media, entertainment streaming and other online service companies are facing unprecedented demand.

It is crucial for organizations to understand the various digital tools that are available, and to weigh their respective risks and benefits simply to survive. Pretty much any business or organization has had to focus on personnel working remotely from home. Thus the pandemic has highlighted the key role that digital technologies can play in assisting organizations to survive and to build resiliency for the future.

Adaptations being implemented to deal with the pandemic are not likely to be temporary or of short duration for at least two reasons: First, it is uncertain how long the pandemic (including government restrictions and orders) will be necessary. "Health experts suggest the

[1] Conference Board, p. 8

virus could stick around and become endemic in the human population, like influenza".[2] A vaccine could take 12 to 18 months to develop. Second, the changes to digital operations may prove to enhance the efficiency and security of the organization. It makes sense that at least some of the adaptive measures undertaken to weather the storm will prove useful even after the current disruptions have ended. The pandemic is causing organizations to rethink their operations such that many cyber and other measures they have adopted may be continued after the pandemic ends.[3] The Conference Board of Canada notes as follows[4]:

> We expect consumers and businesses to rely more on digital solutions after the crisis than they did before. Businesses that can take advantage of online platforms and other digital technologies will be in a better position to handle supply chain disruptions, both now and in the future.

Accordingly, “the ongoing disruptions may be a wake-up call for organizations to invest in digitalising their operations and introduce online consumer platforms".[5] The pandemic “could also accelerate the adoption of other digital tools" which can “reduce costs for businesses" as well as enable small and medium-sized organizations to access global markets more easily.[6]

The bottom line is that organizations that survive the current crisis will not want to simply go back to doing things the way they did before. As Frederick Nietzsche said “that which does not kill us, makes us stronger".

Unfortunately, the society-wide shift towards working remotely gives rise to increased new cyber risks, including exposure to liability claims. Hackers and other cyber criminals have not gone on vacation but are taking advantage of opportunities created as the legitimate world struggles to find cyber solutions on an urgent basis. Many authors have commented on this:

> Cybercriminals love a crisis and COVID-19 is no different. In the last several weeks, cyber-crime has increased exponentially as hackers seek to take advantage of the migration to a remote workplace.[7]
>
> The COVID-19 pandemic has proven to be an extremely disruptive event, affecting all components of society. The IT world is not immune. The pandemic has forced both public and private sectors to rethink how, when, and where work is performed. Traditional models of office versus home-based work environments have been completely inverted; in many cases, most employees are now working remotely. This inversion has caused IT management, implementers, and clients to scramble to adapt to a new way of working. Unfortunately, this rapid transformation presents both new and unique opportunities for threat actors to take advantage of. The entire IT hierarchy, from management to client, must be made explicitly aware of this fact and take every precaution possible.[8]

[2] Conference Board, p.5
[3] Conference Board, p.3
[4] Conference Board, p.3, and see also p.8
[5] Conference Board, p.8 and see also p.6
[6] Conference Board, p.8
[7] Kantrowitz
[8] Canadian Centre for Cyber Security (Advice and Guidance)

> As businesses have rushed to mobilize at-home workforces in response to shelter-in-place measures - for many this an entirely unfamiliar experience - the new procedures, makeshift security measures, and decentralized oversight have left their business more vulnerable to cyber-criminals.[9]
>
> Cyber criminals have moved quickly to take advantage of the fear and concern around COVID-19, along with increased reliance on social media to stay connected, to launch very sophisticated cyber-attacks. These range from generic "phishing" campaigns, perpetrated by sending an email—or, increasingly, a text message—that appears to originate from a trustworthy source, or "spear phishing," where the hackers monitor social media and specifically tailor the attack to the victim.[10]

Class action lawsuits are already proliferating with respect to how organizations have responded to the pandemic, including claims for inadequate cyber security by service providers.[11]

While businesses are forced to rely on third party applications and platforms, they do have room to make some choices and take some steps to mitigate the risks. In this paper I aim to provide an overview of the risks and how they might be addressed, first with respect to digital operations overall and second more specifically with respect to videoconferencing.

II. TECHNICAL CHALLENGES

Organizations, digital network operators and software developers are rushing to implement changes, without the luxury of time to fully consider and test these changes. The viability of existing applications, service providers and network structures is being severely challenged with the increased use of same:[12]

> … The huge surge in Internet traffic and the increased reliance on remote access and online conferencing platforms have created concerns over the resilience of the IT infrastructures that keep things running. Working from home also exposes companies to increased security risks and Internet fraud.
>
> IT service providers worldwide, such as Internet broadband providers, virtual private network (VPN) operators and cloud computing firms, are facing unprecedented challenges to meet demands so as to enable businesses to continue to operate while employees work in their home environment. Apart from the potential strains on different IT systems, interruptions in societies may also prevent engineers from attending onsite checks and maintaining hardware and cables, posing a real-time stress test on the world's IT infrastructures.

Again, this creates opportunities for cyber criminals who are moving to take advantage of unexpected gaps and glitches that arise.

[9] Tomlinson
[10] Charfoos
[11] Cameron Deagle, Kimrey
[12] Chan

III. CYBERSECURITY ISSUES

A. Introduction

The Cyber Awareness System Cybersecurity and Infrastructure Security Agency (CISA) in the U.S. and the National Cyber Security Centre, (NCSC) in the U.K. have found it necessary to issue a joint alert regarding the threats that they are witnessing from the worldwide changes in digital operations.[13] The Canadian Centre for Cybersecurity has also issued a number of alerts and guidance sheets.[14]

Both the CSA and the NCSC have noted an increasing use of COVID–19 related themes by cyber criminals to lure victims[15] which, combined with the increase in online work, has increased the abuse of vulnerable online services.[16] The result has been an increase in the number of data breaches, Business Email Communication (BEC) frauds such as phishing and social engineering, and ransomware/malware attacks and (2) Business Email Compromise (BEC), which includes wire fraud. These cyber-attacks have been aimed at organizations of all sizes.

B. Overall Remote Operations

1. Identified Threats and Issues

The threats that have been observed by the CISA and NCSC with the increase use of digital operations include: [17]

1. “Phishing, using the subject of coronavirus or COVID-19 as a lure”. Cyber criminals have expanding these attacks beyond emails to other forms of e-communication such as texting.
2. The distribution of malware with COVID-19 themes[18] in an environment where many are assiduously seeking updated information on a regular basis.[19] People should be looking for the following types of cyber messaging being employed by hackers to access confidential information or load malware/ransomware:[20]

    (a) General updates re COVID-19;

[13] CISA AND NCSC (Alert). See also CISA and NCSC (Defending Scams).

[14] Canadian Centre for Cybersecurity (Advice and Guidance); Canadian Centre for Cybersecurity (Cyber Hygiene); Canadian Centre for Cybersecurity (Remote Work)

[15] CISA AND NCSC (Alert); Imran

[16] Charfoos; Imran

[17] CISA and NCSC (Alert). See also Canadian Centre for Cyber Security (Cyber Hygiene); Kantrowitz; McAnally.

[18] CISA and NCSD (Alert)

[19] Charfoos

[20] Charfoos

(b) Offers of medical supplies or insurance;

(c) Government aid and other government communications;

(d) Updates from customers, venders and business associates;

(e) Internal corporate communications; and

(f) Exposure to COVID-19, (*e.g.* email purportedly from a medical caregiver or agency that the subject may have been in contact with the virus).

3. Registration of new domain names purporting to relate to COVID-19.

4. “Attacks against newly — and often rapidly — deployed remote access and teleworking infrastructure”, such as videoconferencing.[21] Hackers are relying on the shift to working remotely to exploit vulnerabilities of remote access/communication platforms and apps.

2. <u>Recommended Precautions</u>

I now turn to what people may do to protect themselves from these threats. There is a lot of common ground respecting recommendations as to what precautions can be implemented, such as the following:

1. Test the increased remote connectivity and train personnel regarding remote access, including bandwidth limits and redundancies.[22] Organizations should also prepare backup plans.

2. Conduct a security assessment in the context of the new environment regarding all remote work platforms to “confirm that all new access points are secure and that technical defences are fully implemented”.[23]

   (a) The organization must understand and manage its digital footprint, including by way of testing, table exercises and planning for a cyber incident.[24]

3. Closely monitor cyber incidents and disruptions.[25]

4. Review vendor contracts, especially with respect to new vendor services necessary to allow personnel to work remotely.[26]

[21] CISA AND NCSC (Alert)
[22] Calhoun; O’Connor; Stiffler
[23] Owen. See also Chan.
[24] Imran; O’Connor
[25] Chan

5. Create a secure alternative method for senior management of the organization to communicate in case of email disruption.[27]

6. Rely only on trusted sources such as legitimate government websites for COVID-19 updates.[28]

7. Encourage personnel to practice good cyber hygiene in general, including with respect to:[29]

   (a) Installing software updates in a timely fashion;

   (b) Maintaining good password protection;

   (c) Maintaining updated anti-virus protection;

   (d) Enabling multi-factor authentication; and

   (e) Installing applications only from trustworthy sources.[30]

8. Train personnel regarding remote access and publish internal policies to be on the alert for abnormal activity such as phishing and requests to transfer funds, including:[31]

   (a) Be wary and circumspect regarding disclosure of personal or confidential information via e-communications and to refrain from responding to inquiries for such information.[32]

   (b) Avoid clicking on links in unsolicited emails or texts from sources that you do not recognize and be wary of attachments.[33]

   (c) Exercise high vigilance regarding the authenticity or legitimacy of sources requesting transfer of funds or donations, including by way of the following:[34]

      (i) Check for spelling and grammatical errors (which is the most telltale sign of a fraudulent communication).[35] Note typos and "weird spacing".[36]

[26] Chan; Jacobs; Kohne; Owen; Stiffler
[27] Kantrowitz
[28] CISA and NCSC (Defending Scams); Kantrowitz; McAnally
[29] Imran; Kantrowitz
[30] See also Charfoos; Kohne
[31]Chan; McAnally;, O'Connor
[32] CISA and NCSC (Defending Scams)
[33] CISA and NCSC (Defending Scams); Charfoos
[34] CISA and NCSC (Defending Scams; Chan; Kohne

(ii) Be alert where the sender is not someone with whom you normally interact or a platform which is not one on which you have communicated in the past.[37]

(iii) Ensure that the sender's email address and information conforms with legitimate communications with the vendor, customer or contact in the past.[38]

(iv) Even then, be aware of the ability of hackers to fraudulently display a proper sender's email address, *i.e.* the ability to "spoof" a legitimate email address, even with respect to legitimate COVID-19 sources such as the Center for Disease Control or the World Health Organization.[39] Sometimes hovering the cursor over the displayed address of the sender may reveal the actual sender and one should hover over the URL of an attachment to compare it with the URL displayed in the email.[40]

(v) Be on the lookout for emails purporting to be from government agencies which ask you to click on links or open attachments. Such entities "tend to explain in the body of the email the news they wish to convey" and "it is unlikely they would try to funnel your attention to a website with a clickbait title or get you to open an attachment".[41]

(vi) Question why you are being asked to open a link or attachment – consider whether the information to be provided or the action requested is appropriate.[42]

(vii) Be suspicious of a zip file attached to an email.[43]

(viii) Encourage personnel to communicate directly with the alleged sender of the communication, colleagues and other relevant contacts to confirm any instructions to change procedures or secure activities, especially with respect to transfers or payment of funds.[44] Do this by contacting the other person at the phone

[35] Margallo; McAnally
[36] Margallo
[37] Kantrowitz
[38] Kohne; Margallo; McAnally
[39] McAnally
[40] Charfoos
[41] McAnally
[42] Charfoos; Jacobs; McAnally
[43] McAnally
[44] Chan; Kantrowitz; Kohne; Owen; Tomlinson

number or email address that you have in your contact information for that person. "The most effective method is to verify wiring instructions through a telephone call to a known contact at the recipient and an oral request for a confirming email from that contact".[45]

(ix) Remember that "[a] good rule of thumb is, when you receive a 'suspicious' email with attachments, one that does not look or feel right, it probably is not right."[46]

(d) Encourage personnel to promptly report any suspicious communications or irregularities that they notice, so that any potential attack may be nipped in the bud.[47]

9. All the while, remember to maintain the organization's culture.[48]

C. Videoconferencing

1. Introduction

Organizations must rely on audio and videoconferencing for personnel to be able to continue to work while maintaining social distancing, self–isolation and quarantines. Videoconferencing has become popular, especially since the onset of the pandemic. Various platforms are available including Zoom, Skype, Microsoft Teams, Google Meet and WebEx. Employment of videoconferencing "has now proven largely useful to respect social distancing measures while preserving a sense of, albeit new, normalcy".[49]

There has been a dramatic increase in the use of videoconferencing platforms since the onset of the pandemic. Between December 2019 and of March 2020, the number of daily meeting participants using zoom has grown from 10 million to 200 million.[50] Indeed, over the month of March 2020 Zoom's daily traffic in the United States has grown by 500% and it has become the most downloaded app in that country.[51] Broda-Bahm suggests that videoconferencing is not a panacea for group communication because it requires more energy and attention than in–person meetings.[52] It can make it more difficult to recognize and read

[45] Tomlinson
[46] McAnally
[47] Kohne, Imran; Kohne
[48] Owen
[49] Rhodes
[50] Deagle
[51] Deagle
[52] Broda-Bahm

non–verbal cues. Silence and pauses can sometimes be difficult to interpret – is the speaker pausing for effect or has there been a glitch in the transmission? Also, "participating in a web–conference can lead to individuals focusing on the performative aspects of their own presentation".

2. Identified Threats and Issues

A number of threats and issues have been raised with respect to videoconferencing:

1. "Zoom-bombing". There has been a plethora of incidents where "uninvited participants have disrupted meetings by interjecting inappropriate language or displaying hateful or pornographic images into business meetings"[53], facilitated by a hacker's interception of videoconference links and passwords.[54] It has become so prevalent that it has prompted the FBI to issue warnings about it.[55] This gives rise serious threats in addition to the disruption of a videoconference, including:

   (a) The potential for the unauthorized disclosure of confidential or personal information.[56] An allegation has been made about "[t]he Windows version of Zoom being vulnerable to attackers who could send malicious links to users' chat interfaces and gain access to their network credentials".[57]

   (b) The potential for law enforcement and regulatory agencies to request and, if necessary, subpoena the contents of videoconferences for their investigations.[58]

2. Insufficient or non-existent encryption and other technical vulnerabilities.

   (a) Some videoconference platforms are alleged to have exaggerated their encryption capabilities: [59]

   > Despite frequently asserting it used 'end-to-end encryption for video meetings' which would ensure neither external attackers nor Zoom itself could access the contents of a video meeting, Zoom using only transport encryption for video meetings, meaning Zoom has access to unencrypted audio and video from meetings.

[53] Boerner. See also Rahman.
[54] Bruder
[55] Rahman
[56] Boerner
[57] Deagle
[58] Rahman
[59] Deagle. See also Boerner.

(b) Facetime offers end-to-end encryption but only where all participants are on an Apple device.[60]

3. Inadequate privacy.

(a) There have been suggestions of videoconference platforms improperly using subscriber data.[61] At one time it was alleged that Zoom forwarded data from users of its IOS app to Facebook for advertising purposes.[62] Indeed, litigation has been brought against Zoom for this.[63].

(i) However, it appears that Zoom implemented a new privacy policy in March 2020.[64] It claims to have disabled the data sharing.

(b) Some videoconference platforms, including Zoom, allow conferences to be recorded without the consent of participants.[65]

(c) Until 2 April 2020, Zoom had an "attendee attention tracker" feature which enabled the conference host to track participant attention by revealing whether a participant's Zoom window was in the background of the participant's screen.[66]

(d) Keep in mind the potential for videoconference attendees to create privacy issues:[67]

> End-users may also create privacy issues. Among other things, confidential information may be mistakenly divulged if an employee shares their screen while such information is visible. If an end-user participates in a video conference in a public space, everything that is said and displayed during the conference is disclosed to those around them. Moreover, if an end-user records or takes screenshots of images displayed during the meeting, those items may be improperly disseminated.

3. <u>Recommended Precautions</u>

Videoconference users can and should take a number of precautions:

[60] Kimrey
[61] Boernerk; Bruder; Deagle
[62] Bruder; Deagle
[63] For example, see ***Cullen v. Zoom Video Communications, Inc***., Class Action Complaint, Case 5:20-cv-02155-SVK (U.S. Dist.Ct., N. Cal.) https://www.classaction.org/media/cullen-v-zoom-video-communications-inc.pdf
[64] Bruder; Deagle; Kimrey
[65] Deagle
[66] Bruder
[67] Boerner

1. Analyze and compare available videoconferencing platforms, with the assistance of IT professionals, before choosing one, including with respect to:[68]

    (a) Confidentiality and privacy policies;

    (b) Security measures;

    (c) Retention and deletion policies;

    (d) Liability exclusion clauses; and

    (e) Policies for purposes other than conducting the videoconference itself such as using or sharing attendee information to third parties.

2. Develop a "robust videoconferencing policy" and communicate that to personnel.[69]

3. Keep the videoconferencing software updated, applying patches promptly.[70]

4. Refrain from opening unanticipated videoconference invitations or clinking on links to same.[71] Note that cyber criminals send out false invitations in hopes of installing malware or ransomware.

    (a) Conference hosts should advise desired participants in advance to expect an invitation for a specific time.[72]

5. Restrict videoconference access to invited or approved attendees, by way of the following:[73]

    (a) Implementing password protection to access a conference, including the use of differing passwords for one's account and individual meetings and requiring hosts to have random meeting IDs generated as opposed to relying on provider-generated links or personal meeting IDs.

    (b) Prohibiting attendees from changing their user names so as to conceal their identities.

    (c) Requiring the conference host to adjust settings so that only that host may share the screen or to employ the "waiting room" feature whereby prospective attendees are initially placed there before being approved by the host to enter the videoconference.

[68] Boerner; Chan; Deagle; Fabricant; James; Rahman; Rhodes
[69] James
[70] Boerner; Fabricant; James
[71] Fabricant; Kohne
[72] Fabricant
[73] Boerner; Bruder; Deagle; Fabricant; James; Kohne

(d) Requiring the host to lock the meeting once all attendees have joined.

6. Hosts can require users to keep their cameras and mikes off when they are not speaking or set that as the default.[74] Attendees should confirm that this is the case.

7. With respect to recording of videoconferences:

(a) Be mindful of laws and regulations governing recording video and other conversations.[75]

(b) Control the ability of participants to record the conference.[76]

(i) Some platforms disclose whether or not a conference is being recorded, such as by a light on the screen, but this does not always occur.[77]

(ii) One option is to prohibit attendees to record[78] and to instruct them to refrain from creating screenshots[79]. Attendees should confirm that the host has done this.

(iii) The bottom line is that it is best to assume that the conference may be recorded and to be circumspect about disclosing confidential information.[80] Keep in mind that if a participant is unsure about conference security confidential information can be shared by other means such as encrypted email.[81]

8. Maintain a confidential work area. Do not have confidential documents lying around to be seen by other conference participants.[82] Zoom allows participants to upload and set a photo as a background.[83]

9. Considering alternatives for sharing confidential information instead of videoconferencing[84] such as:

(a) Conference calls.

[74] Boerner; Deagle; Fabricant
[75] Rahman
[76] Boerner; Deagle; James; Rhodes
[77] Fabricant
[78] Deagle
[79] Boerner
[80] Fabricant; James
[81] Bruder; Rhodes
[82] Boerner; Fabricant
[83] Deagle
[84] Bruder; Deagle; Fabricant; Kimrey

(b) Encrypted email.

(c) Webinars. Webinars often do not involve uncontrolled group communication. Often, attendees only have the ability to listen as opposed to speaking. They may be given the opportunity to post questions or comments to the webinar host who can screen them before sharing or responding to them.

(d) Enterprise services.

IV. CONCLUSION

The COVID–19 pandemic is brought about social distancing, self-isolation and quarantines. Organizations and individuals have had to alter their ways of doing things, by focusing more on digital communications, to communicate, work and socialize. There has been a significant shift to working from home and meeting by way of video conferencing.

The dramatic increase in reliance on digital communication methods has intensified the risk of employing such methods, and given rise to new ones. More than ever before, organizations and individuals need to be aware of security issues and take precautions.

At least some of the new approaches and methods for communicating digitally will be continued even after the pandemic is passed, as organizations discover efficiencies and develop security measures. They will be with us for a long time to come.

Be careful out there!

V. AUTHORITIES

Boerner: R. Boerner & L. McDaniels, 27 April 2020, ***Fisher Phillips***, https://www.fisherphillips.com/resources-alerts-10-point-plan-to-protect-your-business

Broda-Bahm: K. Broda-Bahm, Web-Conferencing? Don't Let Your Energy Zoom Away, 27 April 2020, ***Persuasive Litigator***, https://www.persuasivelitigator.com/2020/04/web-conferencing-dont-let-your-energy-zoom-away.html#page=1

Bruder: A. Bruder, *et al.*, Zoom Video Conferencing: Data Privacy and Cybersecurity Implications, 4 May 2020, ***Mayer Brown COIVID-19 Response Blog***, https://www.covid19.law/2020/05/zoom-video-conferencing-data-privacy-and-cybersecurity-implications/#page=1

Calhoun: P. Calhoun & P. Carreiro, Six Steps to Protect Against Increased Telehealth Cybersecurity Dangers, 21 April 2020, ***Carlton Fields***, https://www.carltonfields.com/insights/publications/2020/six-steps-to-protect-against-increased-telehealth

Canadian Centre for Cyber Security (Advice and Guidance): Focused Cyber Security Advice and Guidance During COVID-19, April 2000, ***Canadian Centre for Cyber Security***, https://www.cyber.gc.ca/sites/default/files/publications/Focused%20Cyber%20Security%20Guidance%20COVID-19%20e-f.pdf

Canadian Center for Cyber Security (Cyber Hygiene): Cyber Hygiene for COVID-19, ***Canadian Centre for Cyber Security***, https://www.cyber.gc.ca/sites/default/files/publications/Publication-COVID-19-e.pdf

Canadian Centre for Cyber Security (Remote Work): Cyber Security Tips for Remote Work (ITSAP.10.116), ***Canadian Centre for Cyber Security***, https://www.cyber.gc.ca/sites/default/files/publications/ITSAP10116_1.pdf

Chan: M. Chan, Working from home – A checklist of the IT risks and exposures, 22 April 2020, ***White & Case LLP***, https://www.whitecase.com/publications/alert/working-home-checklist-it-risks-and-exposures

Charfoos: A. Charfoos & C.M. Blakey, Don't Feed the Fish: COVID-19 Phishing Scams and Malware Attacks, 24 April 2020, ***Paul Hastings Insights***, https://www.paulhastings.com/publications-items/details/?id=fb3d336f-2334-6428-811c-ff00004cbded

Conference Board: COVID-19 Global Supply Chain Disruptions: A Catalyst for Long-Term Changes?, 27 April 2020, ***Conference Board of Canada***, http://go.conferenceboard.ca/hr6KMnG01E000yoHC000FJ4

CISA and NCSC (Alert): Alert (AA20-099A): COVID-19 Exploited by Malicious Cyber Actors, 8 April 2020, ***U.S. Department of Homeland Security***, ***Cyber Awareness System Cybersecurity and Infrastructure Security Agency (CISA)***, , https://www.us-cert.gov/ncas/alerts/aa20-099a

CISA and NCSC (Defending Scams): Defending Against COVID-19 Cyber Scams, 6 March 2020, ***U.S. Department of Homeland Security, National, Cyber Awareness System***, https://www.us-cert.gov/ncas/current-activity/2020/03/06/defending-against-covid-19-cyber-scams

Deagle: W.L. Deagle, *et al*., To Zoom or Not to Zoom—Privacy and Cybersecurity Challenges, 10 April 2020, ***Bloomberg Law***, https://news.bloomberglaw.com/us-law-week/insight-to-zoom-or-not-to-zoom-privacy-and-cybersecurity-challenges

Fabricant: J. Fabricant, Video conferencing: 10 privacy tips for your business, 16 April 2020, ***U.S. federal Trade Commission***, https://www.ftc.gov/news-events/blogs/business-blog/2020/04/video-conferencing-10-privacy-tips-your-business

Imran: I. Imran, *et al.*, Episode 2: Cybersecurity Tactics for Turbulent Times, 27 April 2020, ***Blake Cassels & Graydon LLP***, https://www.lexology.com/library/detail.aspx?g=37bf7281-3f39-4b1b-b133-dd203c298f2f&utm_source=Lexology+Daily+Newsfeed&utm_medium=HTML+email+-+Body+-+General+section&utm_campaign=Lexology+subscriber+daily+feed&utm_content=Lexology+Daily+Newsfeed+2020-04-28&utm_term=

Jacobs: G. Jacobs, et al., IT Best Practices for Building COVID-19 Resilience, 28 April 2020, ***FTI Consulting***, https://www.fticonsulting.com/insights/articles/it-best-practices-building-covid-19-resilience

James: J. James & A. Maciejewski, Work From Home Cybersecurity Basics: Videoconferencing Security (United States), 21 April 2020, ***Bryan Cave Leighton Paisner***, https://www.bclplaw.com/en-US/insights/work-from-home-cybersecurity-basics-videoconferencing-security-united-states.html

Kantrowitz: D. Kantrowitz & B. Sharton, Practical Steps to Reduce Cybersecurity Risks During COVID-19, 20 April 2020 ***Goodwin Law***, https://www.goodwinlaw.com/publications/2020/04/04_20-practical-steps-to-reduce-cybersecurity

Kimrey: B.C. Kimrey & B.K. Clark, Zooming into New Privacy Issues, 28 April 2020, ***Vedder Price Media & Privacy Risk Report***, https://www.mediaandprivacyriskreport.com/2020/04/zooming-into-new-privacy-issues/#page=1

Kohne: N.G. Kohne & M.A. Reed, Cybersecurity, Privacy and Data Protection > AG Data Dive > Cybersecurity Threat Actors Target Data of Businesses Seeking Economic Relief, 27 April 2020, ***Akin Gump AG Data Dive***, https://www.akingump.com/en/experience/practices/cybersecurity-privacy-and-data-protection/ag-data-dive/cybersecurity-threat-actors-target-data-of-businesses-seeking-economic-relief.html

Margallo: A. Margallo, Looks Phishy? It Probably Is: Tech Safety During The COVID-19 Outbreak, 21 April 2020, ***McManis Faulkner***, https://www.jdsupra.com/legalnews/looks-phishy-it-probably-is-tech-safety-76734/?origin=CEG&utm_source=CEG&utm_medium=email&utm_campaign=CustomEmailDigest&utm_term=jds-article&utm_content=article-link

McAnally: M. McAnally, Working Remotely During COVID-19: FBI Warns of Phishing Schemes, 20 April 2020, ***Butler Snow LLP***, https://www.butlersnow.com/2020/04/working-remotely-during-covid-19-fbi-warns-of-phishing-schemes/

O'Connor: M.C. O'Connor & S.J. Gardner, Work From Home Presents Privacy and Security Considerations for Research and Higher Education Institutions, 14 April 2020, ***Quarles & Brady LLP***, https://www.quarles.com/publications/work-from-home-presents-privacy-and-security-considerations-for-research-and-higher-education-institutions/

Owen: D.R. Owen, COVID-19 and Cybersecurity for Remote Work, 7 April 2020, Cahill Gordon & Reindel LLP, https://www.lexology.com/library/detail.aspx?g=f5a32ee5-940b-427b-8d38-c08ef4a517ff&utm_source=Lexology+Daily+Newsfeed&utm_medium=HTML+email+-+Body+-+General+section&utm_campaign=Lexology+subscriber+daily+feed&utm_content=Lexology+Daily+Newsfeed+2020-04-23&utm_term=

Rahman: M.C. Rahman, *et al.*, COVID-19: The Risks and Rewards of Remote Videoconferencing, 29 April 2020, ***Troutmand Sanders***, https://www.troutman.com/insights/covid-19-the-risks-and-rewards-of-remote-videoconferencing.html?utm_source=vuture&utm_medium=email&utm_campaign=white%20collar%20advisories

Rhodes: G. Rhodes, The legal landscape in the COVID-19 era | Gina Rhodes, 17 April 2020, ***The Lawyer's Daily***, https://www.thelawyersdaily.ca/articles/18571/-the-legal-landscape-in-the-covid-19-era-gina-rhodes-?category=opinion

Stiffler: J.C. Stiffler, *et al*., IT Best Practices for Building COVID-19 Resilience, 28 April 2020, ***FTI Consulting***, https://www.fticonsulting.com/insights/articles/it-best-practices-building-covid-19-resilience

Tomlinson: C. Tomlinson, *et al.*, Beware Compromised Business Email... and the Litigation that Follows, 2 May 2020, ***Moore & Van Allen PLLC***, http://www.mvalaw.com/news-room-1257.html

BAV/ac