Brought to you by the publishers of COMPLIANCE WEEK

INSIDE THIS PUBLICATION:

Data privacy enters age of Coronavirus

An e-Book publication sponsored by exterro

About us

COMPLIANCE WEEK

Compliance Week, published by Wilmington plc, is a business intelligence and information service on corporate governance, risk, and compliance that features a daily e-mail newsletter, a bi-monthly print magazine, industry-leading events, and a variety of interactive features and forums.

Founded in 2002, Compliance Week has become the go-to resource for chief compliance officers and audit executives; Compliance Week now reaches more than 60,000 financial, legal, audit, risk, and compliance practitioners. www.complianceweek.com

exterro

Exterro was founded with the simple vision that applying the concepts of process optimization and data science to how companies manage digital information and respond to litigation would drive more successful outcomes at a lower cost. We remain committed to this vision today as we deliver a fully integrated Legal GRC platform that enables our clients to address their regulatory, compliance and litigation risks more effectively and at lower costs. With software solutions that span privacy, legal operations, compliance, cybersecurity and information governance, Exterro helps some of the world's largest organizations work smarter and more efficiently. For more information, visit exterro.com.

Inside this e-Book

Do we sacrifice privacy to be safe from coronavirus?

The collective answer might determine how successful we are in the next phase of this fight. **Aaron Nicodemus** has more.

How much of our privacy rights and civil liberties will we be willing to give up in the fight against the coronavirus pandemic? After the terrorist attacks of Sept. 11, 2001, Americans showed they were willing to allow these basic rights to erode—a little here, a little there—in exchange for safety.

The coronavirus is an even more insidious threat than terrorism. It has no agenda, respects no borders, and preys on the old and the sick. Successfully beating back this virus may require further erosion of these basic rights in a democracy. But this time, working hand-in-hand with government to monitor our behaviors and restrict our movements, could be some of America's biggest companies.

How will it happen? Let's examine the pandemic response playbook. The playbook's first two responses to an infectious disease outbreak are identification (testing), then isolation. North America and Europe are still mostly still tackling these two responses.

Contact tracing, the third response, has been mostly forced to the sideline as hospitals overflow with desperately sick patients and healthcare workers struggle to obtain sufficient personal protective equipment. But contact tracing may come to dominate the response to the pandemic this summer.

What's contact tracing? Once a person has tested positive for coronavirus and been isolated, health officials attempt to establish every person the infected patient has come into contact with in the past two weeks. Officials then contact those people and advise them to watch for symptoms as they self-isolate.

Contact tracing has been used successfully in China and South Korea to limit the spread of coronavirus. Several U.S. states, including Massachusetts, are examining how to ramp up contact tracing this summer while hiring lots of people to conduct it, according to STAT, a healthcare industry reporting website.

We probably have to accept contact tracing as a necessary evil. It will help to slow coronavirus hotspots

and to beat back a potential second wave of infections. For contact tracing to work, we in democratic, western societies will have to give up a little bit of our rights. Remember what it was like to travel before 9/11, then after? Remember our tolerance for government eavesdropping before, and after? For torturing terrorism suspects before, and after? Like that.

This time, though, we may be ceding our rights to Big Tech. Google and Apple recently announced a partnership to call a truce between these fierce corporate rivals in the name of fighting coronavirus. The companies will allow their current Android and iOS devices to interface with each other "using apps from public health authorities" for the purpose of using their devices to trace who they've been in contact with.

While the tech giants expect to release their portion of the technology in May, it will likely be into the summer before public health authorities release a contact tracing app to the public.

Here's how it would work. People would voluntarily download the app, and it would begin collecting information on their movements, stored only on their mobile devices. If the person tests positive for coronavirus, s/he would enter that information into the app.

The app would then notify all people whose smart phones (with the voluntary app) have been within six feet of the infected person in the past two weeks. They would be advised to self-isolate for two weeks.

Some privacy experts worry the technology is ripe for misuse, either by government, Big Tech, or other bad actors. "Contact tracing apps collect and combine two highly sensitive categories of information: location and health status," wrote University of Washington Law Professor Ryan Calo, in April 9 testimony before the U.S. Senate Committee on Commerce, Science, and Transportation. "It seems fair to wonder whether these apps, developed by small teams, will be able to keep such sensitive information private and secure."

He listed other concerns, like that the app would be inaccessible to the poor, it could show an area as "safe" only because few users had downloaded the app, or how people could game the system by uploading fake positive tests to make an area look like a hotspot.

This entire argument also depends on the government ramping up coronavirus testing so that everyone—not just those showing symptoms, because health officials acknowledge that 25-50 percent of people infected may show only mild symptoms—can be tested. At least in the United States, we are far, far away from universally available coronavirus tests.

Back to the privacy and civil liberty concerns. Google and Apple have pledged to be as open and transparent as possible, while also protecting the privacy of people using the app.

"Privacy, transparency, and consent are of utmost importance in this effort, and we look forward to building this functionality in consultation with interested stakeholders," the companies said in their statements. "We will openly publish information about our work for others to analyze."

The Trump regime has not yet unveiled how much information it intends to reveal about the creation and use of this app, and that has some Democrats worried. "I would hope that the Department of Health and Human Services—and the Trump Administration as a whole—follow similar steps to be more transparent and, for example, publish the full agreements they have signed with tech companies such as Apple," U.S. Sen. Robert Menendez (D-N.J.) told The Verge.

The Trump administration hasn't said if it will release those agreements, or much information at all at this point. It will be up to us—the people who will be subject to contact tracing and who voluntarily agree to use this technology to track our movements—to demand that the Trump administration make this information available.

We should demand to know the terms of the deal the government is making with these companies in order to create this app; we should demand to know how it is protecting our rights under the Constitution; and we should know how the government will ensure the data collected will not be used for purposes other than contact tracing.

Americans may very well be willing to give up a little bit of privacy, a little bit of control, in order to be made safer. We just want to know if it's worth it. ■

CCPA, Shield Act take back seat during coronavirus?

While privacy regulation dips during coronavirus, consumers—and the plaintiffs' bar—are still watching, writes **Lori Tripoli**.

News that a number of trade associations asked the California attorney general to postpone enforcement of the California Consumer Privacy Act (CCPA) until Jan. 2, 2021, can't help but make one wonder just how much data privacy laws as a whole are being adhered to right now. Companies in the age of the coronavirus pandemic, after all, are slightly more focused on how to generate revenue as all of their employees work remotely.

Those firms deemed "essential" likely are scrambling to keep up as members of their workforce fall sick. Employer interest—and that of the general public—in the health of workers as well as their movements prior to any COVID-19 diagnosis would seem to place data privacy law compliance on a back burner.

But even if privacy is not top-of-mind in this new world order, state data privacy laws as well as federal ones "remain in place," noted Brian Kint, a member at law firm Cozen O'Connor.

Employers walk a tenuous path as they seek to protect their employees in part by finding out which ones happen to be afflicted with COVID-19. "There is legal risk associated with disclosing the identity of an afflicted employee," said Jeffrey Poston, co-chair of the Privacy & Cybersecurity Group at law firm Crowell & Moring. While "employers are generally protecting the identity of the employee," they are also "gathering the names of the employees with whom the patient may have had contact and notifying those individuals and urging them to get tested," Poston said.

Companies have to balance the privacy and confidentiality of a coronavirus-diagnosed employee "with employee safety," Kint said. "If a company has to notify employees that they may have been exposed, it should do so without releasing the identity of the infected employee," he suggested. Keeping that confidentiality will "encourage employees to report a positive test result that they may otherwise be reluctant to share with their employer," Kint said.

Significantly, HIPAA privacy protections remain in place. In February, the Office for Civil Rights at the U.S. Department of Health and Human Services (HHS) issued "a warning to employers that the HIPAA Privacy rule continues to apply during the outbreak of infectious disease or other emergency situations," cautioned Steve Cosentino, a partner at law firm Stinson.

HIPAA "has been around for quite some time" though, Cosentino noted. "It is not surprising that we have not seen similar proclamations about some of the newer state privacy laws," he said. But the HHS Office for Civil Rights is giving some people a break in this fraught time; the agency also announced it would be "exercising its enforcement discretion" to not impose penalties on healthcare providers using telehealth communications in good faith during the COVID-19 nationwide public health emergency.

Not long after California Governor Gavin Newsom declared a state of emergency to help address the spread of COVID-19, more than a dozen trade associations along with some companies wrote to ask California Attorney General Xavier Becerra to hold off on CCPA enforcement until next year. The March 17 letter from entities including the Association of National Advertisers, the Cemetery and Mortuary Association of California, and the United Parcel Service (UPS) expresses concern that "given current events and the presently unfinished status" of CCPA regulations, "businesses will not have the operational capacity or time to bring their systems into compliance" with the CCPA by its current July 1, 2020, enforcement date.

That effort did not sit well with some. "This is a cynical attempt by industry to avoid honoring California consumers' constitutional right to privacy, and industry shouldn't exploit the health crisis to

ignore consumer requests to companies to stop selling their data," said Justin Brookman, director of privacy and technology policy at Consumer Reports, via press release.

"Now that more consumers are working from home and relying on tech companies for crucial communications, the attorney general needs to ensure that appropriate safeguards are in place," Maureen Mahoney, a policy analyst at Consumer Reports, added.

Whether the California AG can unilaterally opt to defer CCPA enforcement for a year "is not immediately clear," said Laura Jehl, global head of the Privacy and Cybersecurity Practice at McDermott Will & Emery. "The original delay in enforcement of the privacy provisions—from a January 1, 2020, effective date to July 1, 2020—came about as a result of an amendment to the law" passed by the California state legislature, she said.

Even so, absent egregious behavior by a business, "it's unlikely that we will see a significant CCPA enforcement action this year," Jehl predicted. Still, "the major provisions of the law have been reasonably clear for some time," she said. Moreover, "the AG earlier warned that he expected companies to come into compliance by January 1," Jehl recalled. As such, it "is not inconceivable" that Becerra would pursue enforcement for a "blatant" violation, "particularly by a company with the sophistication and resources to have engaged in a compliance program before now," she said. Alternatively, the California AG's office could just issue a strong warning or direct a violator to cease and desist inappropriate practices, Jehl noted.

Given the state of business during the current pandemic, the risk of a CCPA enforcement action within the next six months should probably not be "high on a company's list of things to be worried about right now," said Kirk Nahra, co-chair of the Cybersecurity and Privacy Practice at law firm WilmerHale.

Meanwhile, data security elements of New York's Stop Hacks and Improve Electronic Data Security Act (SHIELD Act) went into effect on March 21, 2020.

Although New York has been hard hit by the coronavirus pandemic, so far "there has been no indication" that Attorney General Letitia James "will not enforce security and privacy-related laws during the global pandemic," said Kate Hanniford, a senior associate at the law firm Alston & Bird.

Most of the SHIELD Act's provisions "have already taken effect" anyway, noted Brian Mahanna, a partner at WilmerHale. "The reasonable data security provisions are all that's newly in place," he said.

As a practical matter, states attorneys general have a lot on their plates right now. "It seems unlikely at this particular point in time that the CCPA will be the [California] AG's top priority on account of the pandemic," observed Aaron Simpson, a partner at law firm Hunton Andrews Kurth.

The judiciary was also impacted by the recent turn of events. "State courts are shutting down and limiting court activities to emergency matters," Kint noted. Although the California AG "has the power to bring a civil enforcement action," any such efforts likely "will be delayed" for as long as courts are closed, Kint said.

The same holds true elsewhere. "Given the significant current COVID-19 outbreak in New York, any immediate enforcement of the SHIELD Act seems highly unlikely," Jehl said.

But private rights of action have not been eliminated. Indeed, a class-action complaint filed earlier this year in federal court in the Northern District of California against Hanna Andersson, which sells children's apparel, and Salesforce, a provider of cloud-based e-commerce services, alleges, among other things, violation of the CCPA. The case is ongoing.

Despite the stress, "COVID-19 has increased the importance of a company's privacy and security compliance," Hanniford said. "The shift to remote work arrangements may raise more specific issues depending on a company's information security environment."

Even at this challenging moment, "all organizations should make cyber-security—whether defined as 'reasonable security' under CCPA or 'reasonable administrative, technical, and physical safeguards' under the SHIELD Act—their top priority," Jehl suggested. "Many experts are predicting a significant upturn in cyber-crime while employees, including IT and information security staffs, are working from home." ■

THE 3 BIGGEST MISTAKES COMPANIES ARE MAKING WITH CCPA

With the California Consumer Privacy Act (CCPA) officially launching January 1, 2020, many organizations are still playing catch-up in determining exactly how they'll comply with major provisions before full enforcement begins July 1, 2020.

So far, the biggest risks stemming from the CCPA have touched on a few major areas: the ability to respond to consumer requests for data, breaches of personal data and the resulting fines, and maintaining proper preservation of data needed for civil or criminal litigation. Below, we'll take a look at each of these commonly made mistakes that companies are making, and offer a roadmap to CCPA compliance.

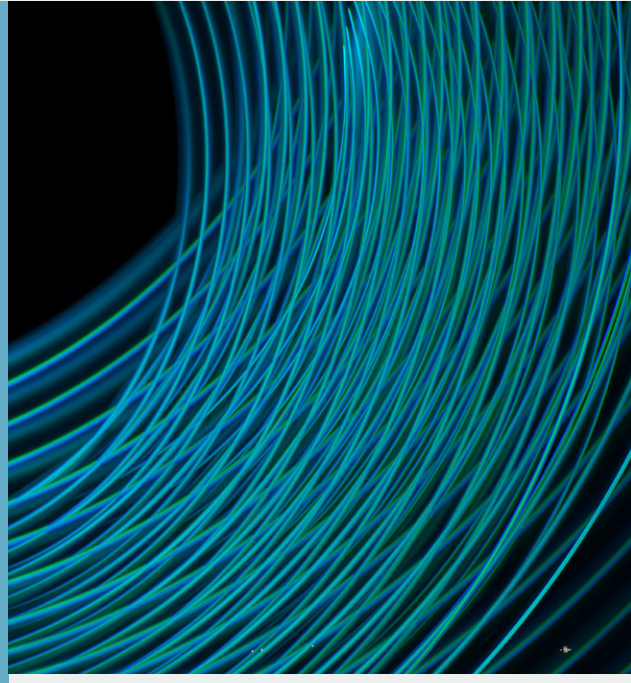
Most of the mistakes that businesses and individuals are currently making regarding their compliance efforts fall into one of the following three categories:

- **Failure to harmonize the DSAR process with litigation requirements**
- **Forgetting to include paper records in the DSAR process**
- **Over-retaining data, which heightens the potential impact of data breaches**

In this guide, we'll look into each of those obstacles and offer defensible practices to avoid adverse legal and financial consequences.

MISTAKE #1:

FAILURE TO HARMONIZE YOUR DSAR PROCESS WITH LITIGATION REQUIREMENTS



Data Subject Access Requests (DSARs) are a key feature of both the CCPA and the EU's General Data Protection Regulation (GDPR). They allow an individual to request to know what data a business holds on them, and ask that it be deleted. Under the CCPA, a business has 45 days to fulfill a DSAR.

DSARs are fraught with risk: The timeline is tight for any organization that doesn't have automated processes and workflows to answer these requests, they're expensive to respond to (Gartner reports that it costs about $1,400 per request) unless technology is used, without a *data inventory* it can be difficult to verify that all of the information has been turned over or deleted.

But what if that data requested is already legally-bound by another law or regulation, and therefore required to be saved under a legal hold?

Deleting data that is this potentially relevant to anticipated or pending litigation (civil or criminal) can have devastating consequences, making it imperative that any DSAR process must harmonize with information under a legal hold. How do you go about squaring a customer exercising their right to have data deleted with the legal requirements that that same information be saved?

Considering the speed at which many companies are trying to, in many cases, delete data (45 days, as required by the CCPA, or 30 days, as required by the GDPR), it's not hard to see how mistakes can happen if processes aren't connected and people aren't communicating.

The Recommendation:

There are four primary considerations with DSARs:

- **TIME.** How long does it take to fulfill a single request?
- **COST.** How expensive is it to fulfill a single request?
- **SCALE.** Is your process able to maintain efficiency even with a 10-fold or 100-fold increase in the number of requests?
- **RISK.** How do you know you're handing over all of the correct information to the correct individual in a secure manner—and not deleting legally-protected material?

The request answering process that your organization builds should consider where it makes sense to cross-reference the DSAR request with the person or team in charge of legal holds, and verify that the information can be deleted.

MISTAKE #2:

NOT INCLUDING PAPER IN YOUR DSAR PROCESS

Paper records have become close to an afterthought in our digital world, but many companies that have been around for decades are still likely to have filing cabinets or boxes filled with documents that they really don't need. But those records still count as data, and still must be produced during a consumer request. So even if it seems that paper records are harmless, they're largely the subject of GDPR requests involving employees of former businesses: They want paper documents.

The CCPA doesn't delineate between electronic and paper data. Plaintiff's attorneys seeking large settlements due, for example, to a termination in which an employee is seeking all of the information held on them want to make it difficult on that business to produce everything. Therefore, paper is a bigger threat to compliance than it may seem.

In fact, the first fine issued under the GDPR had to do with over retention of paper data. Doorstep Dispensaree, a London-based pharmacy, housed boxes of paper documents of patient records in an unsecured shed on the business's property. The documents were back-dated further than the retention laws of the GDPR allows, therefore leading to the violation.

The Recommendation:

Organizations should try and work towards making all data digital, and removing the need for storage of paper records entirely, if allowed by the regulations that govern your industry. This means reviewing paper records and transferring that data to a digital means which, ideally, would be easier to keep track of and inventory.

If paper records must stay a part of the business, then it's even more important to follow data retention laws, for which most major data privacy laws have a provision. In fact, the Irish Data Privacy Order addresses this in a handy *checklist on their site*, offering a couple of questions to clarity data retention and minimization requirements:

- **Is the personal data collected limited to what is necessary for the purposes for which it is processed?**
- **Are retention policies and procedures in place to ensure data is held for no longer than is necessary for the purposes for which it was collected?**

Whether it's paper or digital, the question remains the same: Why are you retaining the data in the first place? Does it have a business purpose? There's a good chance many of those paper records serve no business process, so review and disposal in the name of better compliance should be a priority.

MISTAKE #3:

OVER-RETAINING DATA AND THE CORRESPONDING RISK OF DATA BREACHES

In recent years, high-profile data breach cases ranging from Equifax to the recent Hannah Andersson data breach—the first class-action lawsuit citing the CCPA—have forced larger companies to put cybersecurity on their radar of business needs. With Marriott and British Airways both facing record fines due to data breach violations under the GDPR, major companies are officially on notice that cybersecurity is no longer optional.

While full enforcement of the CCPA won't start until July 1, the data breach provisions—along with resulting fines and class-action suits that an organization might face for a breach—actually began on January 1. Only a month later, a *high-profile class-action suit* was filed.

Over-retention of data also has negative impacts on litigation. The more data that is just sitting in organizational repositories, the more there is to sift through if a discovery request is made. This means that there are larger volumes of data to collect and review: An expensive and time-consuming conquest. Unfortunately, it also means that there is likely to be more relevant information to uncover and produce—which could end up being a negative during the course of the litigation.

If there is one, crux issue that affects most other downstream processes and is most likely to lead to fines, it would be over-retention of data.

The Recommendation:

Businesses need a plan to reduce their volumes of data for reasons pertaining to litigation and data breach risk.

There are two good reasons to create and enforce retention policies at any business:

- **Data you don't have can't be breached. You don't have to protect data that you don't have. And, with respect to DSARs, you don't have to spend time and money searching for data you don't have.**
- **To minimize the impact of e-discovery on litigation, either current or in the future.**

We're still early in this new era of data privacy regulations, and already the astronomical fines are grabbing headlines. Building and enforcing retention policies that are in line with major compliance rules can help prevent enterprises everywhere from becoming the next big headline and reducing potential monetary liability that may occur if your data is ever breached.

Confusion around GDPR prompts EDPB response

Neil Hodge looks at the European Data Protection Board's attempt to clarify how personal data can be processed during coronavirus

As the coronavirus pandemic has spread throughout Europe, data protection authorities (DPAs) have faced questions about how far employers and companies—including schools, apartment blocks, and shopping centers—can go in terms of asking people personal and medical-related information to protect the rest of the public at large.

And despite the fact the European Union has one overarching piece of stringent data privacy legislation—the General Data Protection Regulation (GDPR)—several of the 28 EU member states have taken views that are not wholly consistent with the rest of the pack.

While all DPAs agree that only "essential" information should be collected and shared, there appear to have been varying levels of tolerance as to what "essential" might cover. DPAs in France and Italy, for example, made clear signals early on that employers should not actively collect information about their employees' state of health or ask questions about where they had traveled to, or the health and wellbeing of their family and friends.

Other DPAs, such as those in Denmark and Ireland, said that while sensitive personal data could legally be collected and disclosed under the GDPR, they also stressed the importance of assessing whether such processing is legitimate and limited to what is necessary. The U.K.'s Information Commissioner's Office, meanwhile, said data protection didn't prohibit employers from asking questions, or from notifying colleagues, but warned that organizations shouldn't ask for more information than necessary and reminded them to apply typically "appropriate safeguards."

Lawyers have said the lack of consistency might have led to greater confusion among companies about how they could legitimately ask pertinent health-related questions to employers and third parties without breaching the GDPR and other privacy legislation.

As a result, the European Data Protection Board (EDPB), the body ensuring privacy legislation is applied evenly across the European Union, clarified how personal data could be processed during the pandemic.

First of all, says the EDPB, the GDPR allows "competent public health authorities and employers" to process personal data in the context of an epidemic, so "there is no need to rely on consent of individuals." Where employers may have a legal duty to report health concerns to a public health authority, companies would not be bound by the GDPR when they need to pass on relevant or requested information.

The EDPB makes it clear, however, the type of information being sought needs to be "explicit" and specific rather than general, and that employers cannot make undue demands. For example, companies that want to ask employees and visitors questions about whether they pose a risk to others can do so, but they should only require health information "to the extent that national law allows it." The same goes for performing medical check-ups on workers—if national law permits it, employers are free to try it out.

Also, notes the EDPB, employers should inform staff colleagues they may be infected, but they should only reveal their names if national law allows it; if they can justify such a step is necessary; and only after the affected workers have been notified beforehand.

Some may feel the EDPB has been slow to react, and its guidance may still leave some organizations and compliance officers scratching their heads about what the limits of questioning workers over their health might be—as well as what the legal repercussions could be if they overstep the mark.

Others may feel the EDPB's statement may be moot anyway. In many EU countries, companies are already laying workers off in droves or asking them to take unpaid leave for up to three months, so there is no need for them to worry about asking health-related questions anymore. ■

App offers $1M bounty for hacking smear campaign

Social networking app Houseparty is offering a $1 million bounty for an alleged data breach smear campaign. **Kyle Brasseur** explores.

Popular face-to-face social networking app Houseparty is on the defensive amid claims of a data breach, offering a $1 million bounty for proof of what it believes may be a "paid commercial smear campaign."

The Twitter account for the app shared notice of the bounty on March 30, noting the company is "investigating indications" that the recent reports of its privacy flaws might be the result of someone wishing to harm the platform, which has surged in users during the coronavirus pandemic. One of the original sources of the hacking reports, Twitter user @megycassidy, has appeared to have since deleted their account. Other tweets to allege hacking that have gone viral have also been deleted.

Twitter users have alleged Houseparty was trying to access other apps on their phone, including Spotify and Netflix. Some users even claimed their online banking accounts were compromised. None of the claims have been definitively proven.

"All Houseparty accounts are safe - the service is secure, has never been compromised, and doesn't collect passwords for other sites," Houseparty responded.

Houseparty, launched in 2016 and purchased in 2019 by Epic Games, the organization behind the mega-popular video game Fortnite, has boomed in activity in recent weeks as people across the globe have been ordered to stay home in an effort to slow the spread of the coronavirus pandemic. The app saw its weekly average downloads jump to 2 million in early March, according to data tracked by Apptopia.

But with increased users comes added attention. Video conferencing company Zoom is in the same boat, now facing scrutiny from the New York Attorney General's office for its data privacy and security practices, according to the *New York Times*. AG Letitia James sent a letter to Zoom questioning whether the platform's current security controls can keep up with its surge in users.

Maarten Stassen, partner in the privacy and cyber-security group at law firm Crowell & Moring, says he isn't aware of another company going to the extent to defend itself like Houseparty has with its bounty offering. "Sabotage is part of the new risks posed by the digital world we all depend on and already happens on a smaller scale, for example, intentionally posting false reviews of restaurants or stores for competitive gain," he adds.

Apps new to the mainstream, like Houseparty, are also at risk of being blamed for breaches that may just be coincidental, notes Sundeep Kapur, an associate in the privacy and cyber-security practice at law firm Paul Hastings. That's why privacy experts recommend using different passwords for different services in order to avoid widespread hacking.

"With more user awareness about privacy when using video chat apps, criticism around potentially undue data collection may be the fallout that Houseparty has to deal with, even if they assuage fears that user credentials are stored securely," says Kapur. ■

Zoom lessons: Coronavirus exposes teleconference risk

Explosions of use for popular videoconferencing platforms during the pandemic raise new privacy concerns. **Aaron Nicodemus** reports.

Millions of employees ordered to stay at home to limit the spread of coronavirus are using videoconference platforms to stay connected.

But as companies have scrambled to convert their office workforces to stay-at-home, many have had to deal with employees unfamiliar with videoconferencing, as well as those working on personal laptops and unsecure connections. Companies have been left to balance the need to communicate regularly with employees with risks involving data privacy and cyber-security.

Not surprisingly, stay-at-home orders have led to explosions of use for popular videoconferencing platforms like Zoom and Cisco Webex. Zoom went from 10 million unique daily users in December 2019 to 200 million in March; Cisco Webex reported that its traffic in China increased as much as 22 times since the coronavirus outbreak began. Other popular videoconferencing platforms like Microsoft Teams and Google Hangout have not released customer usage numbers.

With all the new users have come new problems, particularly for Zoom. Some Zoom users have report-

ed incidents of "Zoombombing," where an unauthorized user crashes a video chat and posts hateful, racist, or pornographic content. Zoom Technologies recently posted an apology and explanation from founder and CEO, Eric Yuan.

Zoom was originally founded to serve large institutions with robust IT support, he wrote.

"However, we did not design the product with the foresight that, in a matter of weeks, every person in the world would suddenly be working, studying, and socializing from home. We now have a much broader set of users who are utilizing our product in a myriad of unexpected ways, presenting us with challenges we did not anticipate when the platform was conceived," he wrote.

As a result of those challenges, Zoom is now facing scrutiny from the New York Attorney General's office for its data privacy and security practices. The company has had a class-action lawsuit filed against it in California alleging potential violations of the California Consumer Privacy Act (CCPA), which went into effect in January. Even the Federal Bureau of Investigation has warned of the trend of "Zoombombing."

In response, Zoom says it has worked to train new users on its protective features, removed a software code on its Facebook login that sent Zoom user data to Facebook, and has made other upgrades and improvements to its service. But it might be too little, too late.

Other companies popping up in the videoconferencing space are seizing on these shortcomings and highlighting the vulnerabilities of more established competitors. Lifesize, for example, offers encrypted videoconferencing, saying in a recent blog pitch that "associating your brand with security breaches and vulnerabilities can create hesitancies in your partners' and clients' willingness to do business with you."

Managing the risks

For some companies, the explosion in videoconferencing use has led to monitoring and compliance headaches. How can you tell if an employee is sharing privileged or proprietary business information with an unauthorized user? How can you help new employees from mistakenly providing hackers with access to your company data?

Devin Redmond is CEO and co-founder of Theta Lake, a Santa Barbara, Calif., compliance software company. A recent Theta Lake survey of 100 global compliance officers found that 90 percent of their companies are using video as part of their collaboration platforms, but that 89 percent aren't using modern compliance tools.

Redmond said businesses can take relatively simple steps to help prevent cyber-security problems with new remote workers and to keep tabs on them for possible violations, intentional or otherwise.

Although he does not recommend that businesses use these functions, most videoconferencing platforms can limit all sharing. Doing this allows only the presenters to speak and present information. This should be considered a stopgap measure, he said, "because it really defeats the purpose of this technology," which is to provide an online forum for two-way conversations.

Employers can also segment different user groups, which creates a smaller subset to monitor. New users and those operating with personal laptops are most likely to have issues with videoconferencing technology and are susceptible to mistakes that could endanger privileged company data.

Second, some videoconferencing platforms have real-time compliance components as part of their packages, he said, which allow employers to log and record such behavior for later review and correction.

"A lot of organizations aren't paying attention to what's happening on their videoconferences," he said. "Users can share anything on the screen that their device has access to." A joke or comment made during a videocall could become the foundation of a lawsuit later, he said, and having a way to retrieve evidence will be crucial in forming a company's defense. ■

5 tips to immunize yourself against COVID-19 hackers

In this time of fear and uncertainty, it's more critical than ever to practice good cyber-security hygiene, writes **Jaclyn Jaeger**.

As companies around the world continue to require, or highly recommend, that their employees work remotely to prevent the further spread of the novel coronavirus, hackers who thrive off fear see this as an opportune time to carry out a cyber-attack. In this time of fear and uncertainty, it's more critical than ever to practice good security hygiene (just think of it as the technical version of proper handwashing).

"This is a moment that a lot of hackers across the world have been preparing for," says Brian Finch, a partner at law firm Pillsbury who co-leads the coronavirus response team. "This is an opportunity to conduct pretty robust cyber-espionage, if not cyber-hostage taking. We are already seeing a spike in cyber-attacks, including on remote connection services."

Coronavirus-related schemes have been occurring with such frequency, in fact, that in the United States the Department of Justice has made them an enforcement priority. "The pandemic is dangerous enough without wrongdoers seeking to profit from public panic, and this sort of conduct cannot be tolerated," Attorney General William Barr wrote in a March 16 internal memo to all U.S. attorneys' general. "Every U.S. Attorney's office is, thus, hereby directed to prioritize the detection, investigation, and prosecution of all criminal conduct related to the current pandemic."

Hackers prey on fear, so a common hacking scheme works like this: "Using simple phishing techniques, bad actors are targeting individuals with e-mails that appear to come from an official source. The emails purport to share helpful information about the virus and encourage readers to open an attachment, which then downloads malware to infect their computer and gather personal information," explains Jake Olcott, vice president of government affairs at BitSight.

In his memo, Barr cited reports of "individuals and businesses selling fake cures for COVID-19 online" as one example of a fraudulent scheme going around (the Federal Trade Commission is similarly cracking down in this area). He also cited reports of phishing emails from attackers impersonating government healthcare authorities, like the World Health Organization (WHO) and the Centers for Disease Control and Prevention (CDC). In February, WHO itself warned of criminals disguising themselves as WHO officials to steal money or sensitive information.

On March 16, the U.K. National Cyber Security Center (NCSC) announced that it's urging companies to follow its online guidance, including how to spot phishing emails and how to mitigate malware attacks. "We know that cyber criminals are opportunistic and will look to exploit people's fears, and this has undoubtedly been the case with the coronavirus outbreak," said NCSC Director of Operations Paul Chichester. "In the event that someone does fall victim to a phishing attempt, they should look to report this to Action Fraud as soon as possible."

Cyber-security tips

Across all industries, it is critical that companies and employees review security practices, controls, and protocols to reduce the risk of opportunistic cyber-threats amid the coronavirus. What follows are some tips for doing just that:

1. Verify the authenticity of communication by healthcare authorities. Phishing attacks can come from a myriad of communication platforms—emails,

"This is a moment that a lot of hackers across the world have been preparing for. This is an opportunity to conduct pretty robust cyber-espionage, if not cyber-hostage taking. We are already seeing a spike in cyber-attacks, including on remote connection services."

Brian Finch, Partner, Pillsbury

text messages, phone calls. "Be wary of any form of communication that requires you to click on a link, download an attachment, or ask for any kind of personal information," says Heinan Landa, CEO and founder of Optimal Networks, an IT services firm. Upon receiving communication from a person or organization purporting to be from a government health authority, verify its authenticity before responding.

2. Watch for red flags. "Look for spelling errors and bad grammar and beware of anything asking you to download content or provide sensitive information to receive information/tips on how to protect yourself from coronavirus," Landa says. "Even if you are led to what looks like an official webpage after clicking on a hyperlink in an e-mail, if a pop-up message comes up asking you for any kind of information, do not provide it."

3. Educate employees and keep them informed about cyber-threats. "Organizations must implement effective security awareness training, such as teaching employees how to recognize and report phishing attempts," Olcott says. "While people are sometimes painted as a company's weakest security link, they can also be an organization's best defense against cyber-attacks."

4. Be aware of security vulnerabilities posed by third parties. Third parties pose significant risk to all industries, but amid coronavirus hysteria healthcare organizations are especially vulnerable to cyber-attacks for the protected health information and other sensitive data they handle. Often, third parties are targeted by threat actors "with the intent of penetrating the upstream networks of hospitals and health systems," Olcott says. "To combat this threat, healthcare organizations need a way to gain visibility into the security postures of these third parties and continuously monitor them over time for potential security gaps or malware infections."

5. Adhere to industry regulations when working remotely. "Some industry sectors are subject to regulatory cyber-security requirements for remote access," states a client alert from law firm Crowell & Moring. "Government contractors, for example, may be subject to specific technical controls established by NIST SP 800-171, including for access control, awareness and training, configuration management, incident response, media protection, physical protection, and system and communications protection. This is a good time for government contractors to review their system security plans for compliance with these controls for teleworking."

Recent research reveals how coronavirus-related schemes are evolving. According to the research that was conducted by Proofpoint, new coronavirus-themed e-mail attacks, for example, are attempting to disrupt global shipping by targeting susceptible industries, "including manufacturing, industrial, finance, transportation, pharmaceutical, and cosmetic companies (in that order)," Proofpoint said.

Practicing robust and regular cyber-security hygiene should always be top-of-mind, but the coronavirus pandemic really puts security practices to the test. Companies, financial institutions, healthcare organizations, and others that have truly healthy security practices should find themselves immune to the coronavirus. ■

Your CEO has coronavirus: Who needs to know?

Experts discuss when and how companies should reveal if a senior officer has the coronavirus. **Aaron Nicodemus** reports.

As infections stemming from the coronavirus pandemic continue to mount around the world, publicly traded companies face questions about when and where to disclose that their CEO or other key executives have contracted the virus.

There are also good reasons to make a public disclosure if a key company executive is quarantined but not infected, especially if the quarantine somehow inhibits that executive's ability to perform his or her leadership functions.

In this environment, boards of directors should "err on the side of over-disclosure" when it comes to CEOs and C-suite executives contracting coronavirus, said Jackie Liu, co-chair of Morrison & Foerster's Global Corporate Department.

When should companies report their CEO or other key executives are infected?

"There's no bright line," Liu said. In her position with Morrison & Foerster, Liu has counseled publicly traded companies for two decades about what information should be conveyed to regulators like the U.S. Securities and Exchange Commission (SEC) and when. The general guideline is to report a material change to business operations as soon as it is known.

With the coronavirus pandemic and its effect on nearly every aspect of business, Liu says she is coun-

seling her public company clients to disclose if a CEO or C-suite level executive is infected with coronavirus.

"It's difficult to argue that is not material," she said.

Two publicly traded companies, a mining company and telecommunications firm, informed the SEC that they will delay filing certain financial reports because their CEOs have contracted the coronavirus or entered quarantine, according to a March 20 blog by Audit Analytics.

Other companies have also announced their CEOs are infected. Altria Group CEO Howard Willard disclosed he had contacted coronavirus, and he retired during his recovery, as did the president of Harvard University, Lawrence Bacow. In addition, the CEO of Holy Name Medical Center in Teaneck, N.J., Michael Maron, tested positive for coronavirus.

Even so, disclosure of positive test results for a CEO or executive should not be automatic, argued Kevin Abikoff, partner and firm co-chair at Hughes Hubbard & Reed.

Companies often have to make the difficult balancing act in considering whether immediate disclosure through a press release or Form 8-K (as opposed to period filings) is required. One company employee—be it the CEO or other "critical inspirational people"—going out of pocket temporarily requires detailed analysis but does not automatically trigger a need for immediate disclosure, Abikoff said.

In March, Liu said a disclosure trigger could be in upcoming earnings calls (which have since come and gone), as companies might find it difficult to explain away the unexplained absence of a key executive like a company CEO.

Another trigger might be the press, according to a recent blog post by the firm Vinson & Elkins.

"As a practical matter, absent any public- or shareholder-facing notice that your CEO has tested positive for COVID-19, the press may end up doing it for you," the blog post read. "A public communication can provide opportunities to assure shareholders and dissipate panic. It can also do the opposite, and companies must be cautious not to provide misinformation."

Should companies decide to disclose that their CEO or key executives are infected with coronavirus, Liu cautions against playing it too cute. The company should name the executive officer and explicitly say the medical condition sidelining them is a coronavirus infection, she said. Otherwise, a disclosure might just create more uncertainty.

"In this environment, you can't just say a named executive has a medical condition. No one is going to buy that," she said.

Peter Cohan, author and professor of strategy and entrepreneurship at Babson College in Wellesley, Mass., argued companies have an obligation not only to disclose coronavirus infections of key executives, but provide regular health updates.

"Without such disclosure, companies are holding on to market-moving information that they should disclose to investors so they can make informed decisions," he said. "Absent such disclosure, the board ought to be liable for any insider trading that occurs as a result of a failure to disclose the information."

What about informing other employees?

If a company decides not to make a public disclosure about a positive coronavirus test for an executive, the company is still obligated to inform employees who came in contact with that person.

"Privacy regulators in the U.S. and around the world have cautioned employers about the need to protect the confidentiality of employee health information, including in response to the current pandemic," said Chris Lyon, a partner in Morrison & Foerster's Privacy and Data Security practice. "However, companies may face competing pressures to reveal the identity of the affected individual, when the individual is a key senior executive whose absence may attract attention notice or require explanation. This may require a more tailored risk-based approach, working with the individual where possible to align on the nature and content of the disclosure." ■

FUTURE-PROOF YOUR COMPLIANCE APPROACH

Get ahead of the coming regulatory onslaught by preparing your organization now with automated processes and technology that facilitates easy compliance with the CCPA, GDPR, and other data privacy regulations. Request a demo of Exterro's Legal Software Suite, the industry's only Legal Governance, Risk, and Compliance (GRC) platform, and see how future-proofing your compliance approach can pay dividends in cost avoidance.

GET A DEMO

exterro
Legal GRC Software