August 2021

CYBERSECURITY:

STAYING A STEP AHEAD

Special Report

Produced by:

THE LEGAL DESCRIPTION

OCTOBER RESEARCH LLC

ABOUT US

The Legal Description is a production of October Research, LLC specializing in business news and analysis for the settlement services industry and is published 24 times a year.

Contact information:
October Research, LLC
ATTN: The Legal Description
3046 Brecksville Road, Suite D
Richfield, OH 44286
Tel: (330) 659-6101
Fax: (330) 659-6102
Email: contactus@octoberresearch.com

EDITOR'S NOTE

Essentials in today's business environment

Dear Readers,

Thriving in the business world today no longer is only about providing superior products and services at reasonable prices. You can do all these things and still be derailed by cybercriminals.

So, what should you know?

The first step is educating yourself and your employees about the threats which abound. That includes being aware of the increasing amount and sophisticated nature of ransomware attacks; training your team to be cybersafe; and taking stock of your data inventory, as criminals not only are targeting your ability to operate but the sensitive information your company collects.

Of course, companies also need to know what to do after they've been attacked. It's sad that these things are vital. But they are.

Our hope is our Staying a Step Ahead special report will serve as an important resource for your company.

Mark Lowery
Editorial Director
mlowery@octoberresearch.com

THE LEGAL DESCRIPTION

OCTOBER RESEARCH LLC

CONTENTS

Ransomware continues changing the game

Ransomware incidents have increased in frequency, scope, and sophistication in the last few years. The reported rate of ransomware attacks increased 300 percent in 2020, The New York State Department of Financial Services (NYSDFS) noted in a release announcing guidance on ransomware.

Additionally, larger extortion payments have financed the development of more effective hacking and ransomware tools and added more hackers to their ranks.

Elizabeth McGinn, partner, Buckley LLP, noted reports say $350 million was paid last year and there have already been some very notable cases in 2021.

Hackers also have started shifting their focus from individual companies to various infrastructure.

"We are seeing not only in the industry but across the world that hackers used to focus on individual sites for their destruction and malware and they've become more sophisticated lately," said **Tom Weyant**, vice president, risk management and data security, and privacy officer Alliant National Title Insurance Co. "We see that they attack infrastructure."

He pointed to the Colonial Pipeline attack earlier this year.

"You [used to] see individual sites, like a gas station would be down, but when they hit the infrastructure it was the entire east coast service stations, as well as airports were all impacted because with Colonial Pipeline, they attacked the infrastructure."

McGinn noted ransomware has been around for a while, but what we are seeing is how it is being structured and the actors. It is almost like a corporate-like structure.

"The one-man band operation is almost completely gone due to how lucrative this is," she said.

"This criminal enterprise and the money has caused other advanced threat groups that weren't known to deploy ransomware to shift their tactics and techniques and procedures toward ransomware. The service has become very professional, very organized. Groups like DarkSide tend to have very sophisticated operations. Some groups have a marketing team that advertises their products and services, customer service support offerings, negotiators that communicate with the victims.

This set up makes criminal activity easier while creating a new revenue stream for the malware owners."

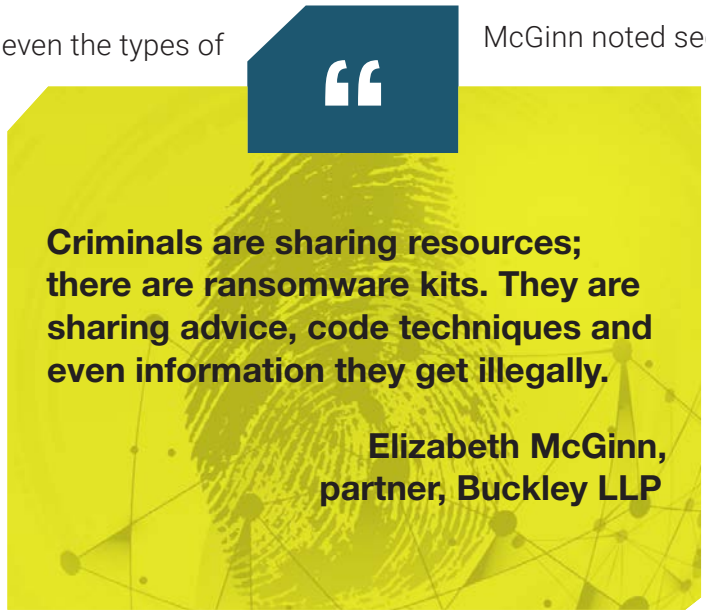
She said one of the most shocking factors with this shift in ransomware is the customer service mentality that seems to be in place.

"Negotiating ransom and obtaining decrypters follows the same model as a customer service help desk," McGinn said. "Upon emailing the address given in a ransom notice, basically a customer service rep walks you through the process. When negotiating a ransom, its common for the point of contact to say he or she needs to check with a manager for approval for a lesser amount."

She said once the ransom is paid and the victim gets the decryption key, she's heard of the hackers offering cybersecurity services to help the victims avoid similar attacks in the future.

"The actors are changing, even the types of attacks [are changing]," she said.

"We are seeing big game hunting schemes targeting larger enterprises, we've seen in the last weeks and months ransomware demands going up. Criminals are sharing resources; there are ransomware kits. They are sharing advice, code techniques and even information they get illegally."



NYDFS issues guidance

NYSDFS examined the ransomware incidents reported by its regulated entities over the past year and a half and has observed they follow a similar pattern: hackers enter a victim's network, obtain administrator privileges once inside, and then use those elevated privileges to deploy ransomware, avoid security controls, steal data, and disable backups.

NYDFS urged all regulated entities to prepare for a ransomware attack by implementing measures such as:

- Train employees in cybersecurity awareness and anti-phishing.
- Implement a vulnerability and patch management program.
- Use multi-factor authentication and strong passwords.
- Employ privileged access management to safeguard credentials for privileged accounts.
- Use monitoring and response to detect and contain intruders.
- Segregate and test backups to ensure critical systems can be restored in the face of an attack.
- Have a ransomware-specific incident response plan that is tested by senior leadership.

McGinn noted segregating and testing backups are very important.

Also, you should have a ransomware incident response plan besides your general one. If you haven't done something like that, it's a good thing to do. Also, when you do your tabletop exercises, plan one around ransomware.

The guidance reflects NYSDFS's commitment to improving cybersecurity and sharing information to protect consumers and the industry.

The agency also has issued multiple alerts regarding ongoing cyber threats, including the SolarWinds Attack, weaknesses in Microsoft Exchange Server, and an ongoing cyberfraud campaign identified by the department.

Training your team to be cybersafe

As recent events have demonstrated, it is vital that your staff is trained on cybersecurity best practices. As cybersecurity threats continually evolve and become more sophisticated, staff members need to act proactively, companies need to have security measures in place, and they also need to know how to respond to an incident.

Recently, **Linda Grahovec**, national agency director of education and marketing strategy, FNF Family of Companies; and **James Chou**, associate, Buckley LLP, discussed these topics during an October Research webinar titled "Training Your Team to be Cybersafe."

Among other things, the duo discussed best practices, how to test your staff to ensure they're following through, how to host an incident response exercise, how real-life attacks play out, and available resources for continuing education.

A prime target

Chou said companies within the financial and professional services industry remain the top target for cybercriminals.

"There are a lot of attractive reasons why financial services remains a top-tier target. There's a lot of financial gain, not only with the kind of money that passes through financial and professional services, but also the data that is maintained by financial institutions as well as professional services or just law firms, [which] is very valuable to a lot of attackers," Chou said.

"Either they resell the information or they hold it hostage. What has changed is the density of the attacks. I mean, we still see a lot of phishing attacks. It's still widely used to gain a foothold in somebody's network. But what has really changed is once the foothold has been established, there have been more and more sort of sophisticated attacks, not just in terms of stealing data and the traditional data breach sense.

"But we now have sort of ransomware, which has been around for about 10 years or more, but now becoming very, very sophisticated. And really what has made ransomware sophisticated over the years is that the actors themselves are becoming more sophisticated."

First things first

Unfortunately, even with safeguards in places, breaches can happen. When they do, it's vital companies provide information to the FBI's Internet Crime Complaint Center (IC3) immediately.

"We recommend if something happens, no matter what it is in the cybersecurity realm, that you participate and provide a complaint and application of that complaint to IC3.gov," Grahovec said. "Now, I have heard some feedback back regarding, well, why should you do all this work and provide all this information, because they don't call me back. It's not like they can help me solve the problem. But there's a big reason why we need to take the time and really put those breaches, or anything that has happened in the cybersecurity realm into the IC3 system."

"They utilize the information they get in order to do all sorts of public service announcements, whether it is creating a flyer or a one pager that you can use in your

title agency or a Realtor can use in their real estate companies or lenders or attorneys," Grahovec said. "So, in order to bring about this public awareness, we need your help. When things happen, we need you to put the information into IC3.gov. Does it take a few minutes? Absolutely. But it is worth it."

Grahovec said the FBI [through IC3] receives more than 2000 complaints daily. She said there have been over $4.2 billion in losses that have been reported over 440,000 complaints received per year. Grahovec said much can be learned from studying the information gathered by the FBI.

Simple steps can ward off big problems

One of the first things a company should do is work with cybersecurity professionals to ensure email accounts, online systems, and business practices are secure and current.

"I cannot tell you how many times we advise our agent partners about patching their software, making sure that programs are updated and up-to-date, making sure that you and your customers alike use two-factor authentication for email accounts. I even recommend this for real estate agents," Grahovec said.

"When you start a relationship with a buyer client, sit down and talk with that client who has a Gmail account, Yahoo account, AOL account, and say, 'Hey, you and I are going to be looking at houses for the next couple of months. I would feel safer if you would use multifactor authentication on your email since you're going to be sending me personal information, and we're going to be sending financial information back and forth,' meaning the financial information that's on a real estate contract."

She also suggested changing passwords frequently, changing passwords to pass phrases, avoiding free Wi-Fi, and using virtual private networks.

"We have a lot of employees that are working from home," she said. "You want to make sure that they are all on secured networks. Educate your customers, clients, and the consumers. I cannot say that enough, communicate, communicate, communicate. Provide expectations on how and when the closing costs are supposed to be provided."

Targeted solutions

Chou said companies should reduce their "attack surface" or open doors through which cybercriminals can infiltrate.

"It really behooves you to kind of really understand where your data is residing, where all your critical data is, and ask yourself, do you really need this data in five different clouds and four different systems off six different laptops?" Chou suggested.

"Do you need administrative passwords being stored on the network? Because one of the things we find in sort of attack scenarios is attackers will gain a foothold on the network, and then they'll easily just find an administrator password right on the network, because it's just stored there as a matter of convenience."

Chou advises examining your system accounts and determining whether you have accounts that aren't needed. He also suggests having three copies of your data — two backups of your data, with one copy offsite.

"Your backups should really have the same security as you would protect your regular data. There's a lot of common pitfalls with backup solutions and that [some companies] just back up the data, it's stored

unencrypted, and it really just ends up becoming another liability to you," he said. "So, you want to make sure that you're providing adequate security around your backups so that they stay secure…And also part of a good backup solution is routinely testing that backup. So, you know, can I actually recover from my backups?"

Chou said companies also need to have incident response plans in place, including communicating with law enforcement, regulators and consumers and remediation efforts.

Supplement policies, procedures with constant communication

It's important, of course, to have written polices and procedures in place regarding cybersecurity. These, however, won't prevent human error.

"We can try to think about putting different policies and procedures in place let's say today, but what are you going to do about it in three months?" Grahovec asked.

"Are you going to retrain your employees? Are you going to make them go through some sort of a webinar?"

Grahovec said communication with team members and business partners regarding cybersecurity must be constant and consistent.

"One mistake can bring our companies down. I don't mean to scare anybody, but we need to be scared," she said. "We are holding bags of money, real money that is not ours in our hands all the time. We are also carrying with us tons of data that is personal. Some of it is non-public private information."

Other tips Grahovec offered include:

- Identifying all equipment and their vulnerabilities. Do you have an inventory of every device that has internet attached to it, whether it be laptops, phones, tablets? Does your copier have a Bluetooth on it? Do your printers have Bluetooth capability? Do you control who logs into your network? Do you have security software? Is it encrypted?
- Dismantle USB portals. These present vulnerabilities. Also, check your network for unauthorized users or connections.
- Regularly test your plan. "Again, we can have the best written policies and procedures, but if you're not testing those every quarter, or at least twice a year, it's not going to help," she said. "Same thing with those backups. If you don't try that policy and procedure, and you don't know that it works 100 percent, then when it actually happens to you, it could possibly be an epic fail, which we do not want your businesses not to be able to be up and running within minutes and then recovery."

Taking stock of your data inventory

As many companies have shifted back to working in the office, it is a good time to take a new inventory on what sensitive data you have and to review and evaluate your data security standards. In a recent blogpost, the Federal Trade Commission (FTC) provided steps to do just that.

The first thing the FTC suggested companies do is update their data inventory.

"Important business records need to be on your system and not on the personal laptops, tablets, or phones of staff members," the post stated. "Work with your employees to make sure need-to-keep documents are where they need to be and that confidential information that shouldn't be in employees' personal possession is securely removed."

It's also important to know what paperwork employees printed out while they were working from home and how they handled any printed confidential documents. The FTC suggested companies make sure their security discussions

include sensitive documents that were created at home.

In addition, it's important to conduct a security double-check on any new platforms and software.

"To keep the business up and running during the COVID crisis, many companies had to move quickly to adopt new platforms and software, many of which have become indispensable productivity tools. If you continue to use them, now is a good time to make sure you've configured them to comply with your security standards," the FTC stated.

It said companies should consider having an in-house security refresher.

"Some people on your staff have spent more than a year without locking desk drawers or securing their computers at the end of the workday. Plan supplemental training to reinforce security basics," the post stated.

Finally, the FTC said companies should evaluate and adjust their practices considering their COVID experience.

"The past 15 months have given you a new perspective into your company's information practices. While those lessons are fresh in your mind, reassess your security procedures and revise your policies," the FTC stated. "While you're at it, take advantage of your company's most valuable resource by asking employees at every level and in every department for their advice about what the past year has taught them about best security practices. Resilient companies understand the need to expect the unexpected and build contingencies for the next weather emergency, power outage, or other operational threat."

We've been attacked, what's next?

In today's world, companies rely on each other for many things and hire third parties to help them with different aspects of their business. Everyone is vulnerable to attacks from hackers and other malicious actors and what happens to one part of the chain could impact the rest of it. What should you do if another connected entity is the victim of a cybersecurity incident?

It starts ahead of time

"If your provider is the victim of a ransomware attack, the first steps to protect your data and that of your clients should have taken place well before the actual breach," said **Bruce Phillips**, senior vice president and chief information security officer, WEST, a Williston Financial Group company. "The best preventative measures is to have an actionable plan in place that addresses all of the fail points."

This includes having an incident response plan, educating staff about the risk of phishing and other malicious attack types and putting fail-safes in place to ensure that you can access your data and systems on at least a limited basis during times of crisis.

"When a breach takes place, you can use your incident response plan as a road map for responding to the crisis," Phillips said. "Start by determining the nature of the breach, identifying what information and functionality have been lost, and implementing a plan for recreating the data and restoring the lost capabilities until functionality and data access can be restored.

"If you don't have an incident response plan in place, then determine what information and capabilities you've lost and identify how you can recreate them in order to keep business going."

Prepare your backups

Another important thing to do to ensure your data is protected and you can keep going is to replicate critical and sensitive data to an offline backup system.

"Make sure you protect yourself from a ransomware

attack by replicating your sensitive data to an offline backup system and keep it updated," Phillips said. "This offline backup system should be operated outside of the other service providers you utilize and should remain directly accessible to you, and not accessible through your service provider. By taking this step prior to a ransomware breach, you can prevent cybercriminals from accessing your backup files as well. It will also enable you to access your backup data source as a temporary solution to keep your business up and running after a breach so you can continue operations.

"Before loading your backup data into your operating system, it's important to ensure that the system has not been corrupted by the attackers," he continued. "As a fallback, you should also have a standalone copy of your operating system that you can load onto a desktop computer along with your backup data, so nothing is completely lost. This will enable you to continue working, albeit at a slower pace."

He also noted companies can protect their data from an attack by encrypting the data within their operating systems. This way attackers cannot access the data.

Your data was compromised, now what?

Phillips said once you find out that your data or that of your clients has been compromised, you should immediately implement your incident response plan.

"This plan should include having known security experts at your disposal so they can immediately evaluate your circumstances and direct you on how to respond," he said. "You should also contact your company's legal counsel and insurance carriers as soon as you are aware of the breach to get them up to speed and on notice right away. In many instances, these providers have experts on hand who can help you in a time of crisis, providing forensic assistance, crisis communications advice, and more."

He emphasized that the first people you should contact if a data breach or ransomware attack occurs should be your company's corporate legal counsel and insurance providers.

"Involving corporate counsel and insurance carriers early on will help ensure that you're contacting the appropriate regulatory authorities and doing so within the appropriate timeframes, as well as complying with consumer notification requirements," Phillips said. "These professionals frequently have expert resources on hand that can assist with complex areas, such as forensics and crisis communications. You should also notify law enforcement, any applicable regulatory bodies and your underwriter, as well as filing an official complaint on the Internet Crime Complaint Center site, IC3.gov.

If it is a service provider who has been compromised, **Tom Weyant**, VP, risk management and data privacy officer Alliant National Title Insurance Co., said it is also important to stay in contact with that provider. They will be able to give you updates on what is going on and estimates as to when systems and operations may resume.

"The other reason to stay in touch with them is because you are going to need a root cause analysis that they are obligated to provide you," he added. "You may need that for several things. Number one, to provide to your state. You may need to provide it to your insurance carrier or to your legal department. It's important to stay in close

touch with them and get that root case analysis and postmortem once things settle down."

Opportunity to reassess

Weyant and Phillips both noted that a breach at a service provider gives you additional incentive to reassess your own security.

"Even if you're not impacted by your vendor's ransomware attack, you should use the close call as a training exercise to ensure preparedness against future potential breaches," Phillips said. "Review your company's Incident Response Plan, get as much information as you can about what's happening and then evaluate how you can respond to the situation as effectively as possible. Do you have data on the vendor's compromised system and what does it include? Do you have access to a standalone copy of your business process system? Knowing all of this upfront will enable you to respond with much greater efficiency."

Weyant said companies should make sure they have things like multifactor authentication and strong passwords or passphrases to access systems and applications, making sure encryption is deployed for emails as well as any data at rest.

Federal and state regulators eye changing cybersecurity landscape

The cybersecurity landscape has changed significantly in the last few years, and new threats have emerged over that time. State and federal regulators have done much to adapt their regulations to the changing environment. During a recent webinar, three partners of Buckley LLP outlined some of those changes.

FTC focus

Elizabeth McGinn, partner, Buckley LLP, noted the Federal Trade Commission (FTC) enforces more than a dozen rules designed to protect the privacy and security of consumers' personal information. The FTC is currently in the process of doing reviews for a few of those regulations.

In addition, she pointed out the FTC Act authorizes the FTC to conduct studies based on information from companies submitted in the form of special reports. In 2020, the FTC issued orders to nine social media and video streaming services. These orders required the companies to provide data on how they collect, use, track and present personal information, as well as information about their advertising and user engagement practices and how their practices affect children and teens.

McGinn also said the FTC has great material on their website regarding consumer and company education. Last year, the FTC hosted three workshops bringing different parties together to discuss key privacy and security issues. The topic of one of those workshops was the Safeguards Rule; another workshop was on data portability.

The FTC has distributed millions of copies of consumer education materials on topics ranging from identity theft, mobile privacy, credit reporting, Do Not Call, and computer security, McGinn said. It also has a wide range of materials to help companies as well. She noted these materials can give you an idea what the FTC is interested in and ways you may be able to improve your privacy and security practices.

Recent publications the FTC has issued include ransomware prevention, a case discussing security safeguards, and the role of corporate boards in data security oversight.

In addressing safeguards, McGinn noted the FTC suggested companies reevaluate their information security program periodically, vet their vendors and make sure they have a strong vendor management

program, and not be afraid of asking questions of vendors to ensure they are protecting the information entrusted to you.

"Another publication that was issued this year was called 'Corporate boards: Don't underestimate your role in data security oversight,'" McGinn said. "The publication stated that it is essential for boards to do what they can to ensure employee data is protected. The good news, according to a recent study, is that the FTC says, 60 percent of the directors surveyed stated they plan to improve their cyber oversight this year.

"It's no longer an IT department that should be leading the charge," she continued. "They believe it starts with the board of directors and for them to build a team, have oversight and hold regular security briefings and really understand the risks and challenges the company faces."

She noted the FTC is emphasizing the importance of not confusing legal compliance with security because compliance doesn't necessarily translate into good security.

"You cannot just check the boxes when you are trying to comply," McGinn said. McGinn believes board conversations should include questions such as: What type of data are we keeping and why? What are our policies and procedures? Are they adequate to meet what we need? Do our practices line up with what we are saying, not only our policies, but our public facing statements? What about our investments? Are we investing in the appropriate amount given our risks and threats these days?

Lessons from enforcement

During the webinar, **Sasha Leonhardt,** partner, Buckley LLP, discussed four recent enforcement actions and some key takeaways attendees can glean from them.

He first talked about an enforcement action where the vendor of a financial services provider allegedly stored unsecured information in a misconfigured cloud environment where anyone on the internet could find it. According to the FTC's complaint, the

information was available on the cloud for almost a year. In bringing the action, the FTC alleged the financial services provider violated the Safeguards Rule.

In another enforcement action, Leonhardt noted a company that created smart home devices claimed its devices were unhackabledue to a level of encryption. However, the FTC asserted this was not true. Security researchers allegedly were able to hack into these devices because they used unencrypted Bluetooth communications and, in some instances, the researchers could simply unscrew a panel on the backs of devices that were designed to be left out in public.

"So there, the FTC alleged a disjunction between a company's claim of security and how the devices were actually created and implemented from a hardware and software perspective," he said.

He then discussed an action against a video conferencing platform that claimed to consumers it had end-to-end encryption at 256 bits, but the FTC asserted neither of these was true. The platform also claimed meetings were stored in an encrypted fashion immediately upon completion, when in fact meetings could be unencrypted for some time before later being encrypted.

Lastly, Leonhardt discussed the FTC's case against a healthcare insurance company that, according to the FTC, maintained an unsecure cloud data base containing 130,000 consumer records. Although the company undertook an investigation of the database to determine whether there had been unauthorized access that would require breach

notification, Leonhardt said the FTC determined that the investigation was not comprehensive enough to be a complete investigation. The FTC also noted that the company's website had several different logos from recognized third parties such as the Better Business Bureau attesting to its various standards and certifications, as well as a generic logo that said, "HIPAA Compliance." However, because no recognized third party had reviewed the company for HIPAA compliance, the FTC found the HIPAA Compliance logo's use and placement to be misleading.

Leonhardt shared several takeaways that companies should be aware of. The first takeaway was data inventories need to be performed and they need to be used so companies understand what data they have, what risks it may create, and how they can handle consumer information in compliance with relevant laws.

The second takeaway was the importance of data security.

"Everyone remembers to encrypt data in transit, but data encryption at rest is often missed," he said. "Three of these four enforcement actions involved data that was not encrypted in storage. More and more we are seeing data security incidents involving data that was stored either on the cloud or on an individual device or corporate network, but it was not stored securely. That is where the data is being found and accessed, and where breaches are occurring."

The third takeaway involved data access. It is important to control access to data both in a company, but also for vendors.

"The vendor of my vendor is my vendor," Leonhardt said. "You are not only responsible for your own security, not only responsible for that of your vendors, but you may be held responsible for a vendor that a vendor of yours engages."

Leonhardt noted several of the actions discussed were based on disclosures and practices that did not match what consumers were told. He said companies should keep an eye on what promises they are making regarding cybersecurity and review their policies and procedures — and potentially consider third party verification — to ensure they are living up to their commitments to consumers.

Looking ahead

Amanda Lawrence, partner, Buckley LLP provided some insight into some things we can expect from the FTC in the future. The first was potential changes to the FTC Safeguard Rule. She said pre-pandemic, the FTC issued a proposed rulemaking to update the rule. Currently, she said the rule is more high-level establishing certain standards that could apply to any type of financial institution, regardless of its size. It has certain standards that financial institutions subject to the Safeguards Rule are supposed to meet, and leaves the details as to what is appropriate for a particular financial institution to be determined by that financial institution based on its size, complexity, and nature and scope of its activities.

Lawrence said the proposal is fashioned in part on New York's Part 500 Cybersecurity Regulation and adds more detail in terms of specific standards. It includes things like mandating the encryption of consumer information in transit and at rest, risk assessments and how they must occur and what they need to cover, what sort of access controls for information and physical controls need to be in place. She said that the timing of any proposed new rule is uncertain but may be as early as the fourth quarter 2021 or the first quarter of 2022.

She said much of what is in the proposed rule are things that many companies in the financial industry already are doing and suggested companies look at them to see if their institution is in line with what the proposed rule could look like.

Leonhardt noted that the FTC is starting to partner more with other federal and state regulators.

"FTC Commissioner **Rohit Chopra** spoke broadly about that and since he is slated to take the helm of the CFPB, we would expect there to be more coordination between the CFPB and the FTC. That may allow the FTC to move matters over or incorporate the CFPB's authority to get consumer remediation."

NYDFS expectations

Lawrence noted that the New York Department of Financial Services has been active in cybersecurity and data privacy for several years now. Its cybersecurity regulations were effective starting in March 2017 with certain provisions having later effective dates. She also noted that DFS has been very active in enforcing its regulations and in issuance guidance to the industry.

For example, it recently released ransomware guidance that Lawrence said details NYDFS's expectations with respect to ransomware, but also contains information about what it expects regulated entities to do in any situation. She recommended taking a close look at this guidance. Among other things, the guidance makes clear that DFS is evaluating whether it needs to revise its cybersecurity regulations, noting that cybersecurity and the threats companies currently face now is very different from when DFS was drafting the regulations in 2016 and 2017.

"DFS really take its work here very seriously," Lawrence said. "They will say time and time again that they want to be at the forefront of cyberregulation and they look at your organization as a whole. They are not just focused on what is going on with New York consumers or even necessarily, if you are an entity that has a number of branches, what is going on in your New York branches.

"The other thing I would say is even though we've been and are in a pandemic, the pandemic is not an excuse to them, nor should it be," she continued. "They are very focused on regulated entities making sure that they are on top of what their cybersecurity should look like given all of the changes that companies have had over the last 18 months, especially with remote work environments."

Lawrence recommended that if a company has not conducted a risk assessment in more than a year, and their systems have changed significantly due to the pandemic or otherwise, they should consider conducting a risk assessment. She said that if DFS conducts an examination and the risk assessment is out of date and/or relates to systems that are different than the one your institution currently uses, DFS likely will find deficiencies with the risk assessment.

> **"More and more we are seeing data security incidents involving data that was stored either on the cloud or on an individual device or corporate network, but it was not stored securely.**
>
> **Sasha Leonhardt, Partner, Buckley LLP**

State regulators

McGinn noted one development regarding state regulators is there have been quite a few multistate investigations in 2020. These can take many years to resolve. Typically, a state will take the lead on these, or a committee of states will.

Leonhardt noted regarding state laws, three states now have statutes with provisions that state if you put in place certain defenses in your cybersecurity, they will allow you to escape liability or escape punitive damages claims. These states are Utah, Connecticut, and Ohio.

He also noted that there are three states that have passed privacy laws—California, Virginia, and Colorado.

"Each of these is primarily a privacy law, but privacy and cybersecurity are intertwined," Leonhardt said.

"Each of these has some provisions for cybersecurity, although the requirements that are affirmatively placed on companies vary based on state."