The CYBERSECURITY LAW REPORT

www.cslawreport.com Volume 2, Number 21 October 19, 2016

FTC

Demystifying the FTC's Reasonableness Requirement in the Context of the NIST Cybersecurity Framework (Part One of Two)

By Jill Abitbol

The NIST Cybersecurity Framework, while useful, is not a panacea, the FTC recently said, leaving many companies still wondering how to develop and implement a data security program that meets the regulator's reasonableness requirement. With input from in-house and outside counsel, we examine the FTC's data security expectations in the context of the NIST Cybersecurity Framework. Part one of this two-part series explores the implications of the FTC's recent communication, how and when practitioners use the Framework and details three initial steps companies should take to meet the FTC's reasonableness standard. Part two will cover the Framework's core functions, how they align with the FTC's requirements and steps companies can take to incorporate these functions into their own security practices. See also "*A Behind-the-Curtains View of FTC Security and Privacy Expectations*" (Mar. 16, 2016).

Implications of the FTC's Recent Blog Post on the NIST Framework

Recently, the FTC published a blog post, The NIST Cybersecurity Framework and the FTC, in which it said that compliance with the Framework does not equal compliance with FTC requirements. While the FTC acknowledged that the framework is aligned with the agency's long-standing approach to data security and that it may serve as a useful tool for companies developing and evaluating a security program, it "is not, and isn't intended to be, a standard or checklist." And "there's really no such thing as 'complying with the Framework.'"

The FTC's intentions in this blog post were two-fold, Mark Paulding, InfoLawGroup's senior counsel, told The Cybersecurity Law Report. "First, because the NIST Cybersecurity Framework is not really designed to be a compliance checklist, the FTC is reluctant to give industries the impression there is anything that could be unequivocally defined as compliance with it." He agrees that it is "more of a guideline on security best practices and security strategies than a testable or measurable compliance structure like, for example, the PCI Data Security Standard, which was designed in large part to be an auditable standard."

Also, Paulding continued, "the FTC's mission is both challenging and a bit more straightforward than the Framework in its purview in that it deals more with threats to consumer information, whereas the Framework is designed to cover a wide variety of security issues up to and including protecting critical infrastructure, which was its impetus." The FTC's guidance "tends to reflect an intent to be as accessible as possible to as wide a range of companies as possible." The NIST Framework, however, was "written largely with a technologist audience in mind. While it provides very good guidance for anyone, I don't necessarily think it was intended to be a guide for a medium-sized regional business."

This is "not new news," Jodi Golinsky, general counsel and chief compliance officer for FS Card, Inc., told The Cybersecurity Law Report. Rather, the FTC "confirmed what it had been saying all along, seemingly to clear the record and emphasize that there is not some sort of rote framework or program a company can put together to avoid a Section 5 claim."

While the high-level principles of the Framework are "absolutely good practice," Paulding believes the FTC wants companies to understand that they do not "necessarily have to go out of their way to dive deep into the NIST Cybersecurity Framework as long as

they are practicing in a manner consistent with the guidance that the FTC has prepared." See, e.g., "*The FTC Asserts Its Jurisdiction and Provides Ten Steps to Enhance Cybersecurity*" (Jul. 15, 2015).

Not a One-Size-Fits-All

"The implications of the blog post can be quite positive," said Mary Hildebrand, a Lowenstein Sandler partner. She believes the Framework's guidance incentivizes companies to take a close look at their own data security needs in the context of the types of data they collect, the purpose for which they use it, where and how it is stored and what kind of disclosures they want or will be making. Companies will need to prioritize their approach to security and "that is a positive thing. It is not a one-size-fits-all."

At Golinsky's small startup company that works with an issuing bank to offer credit cards, the NIST Framework is not immediately applicable. But she stressed that "any company needs to have security practices and policies, regardless of whether a company's size and complexity makes it a fit to comply with a framework like the NIST Framework."

She also agreed that the post serves as a reminder to companies that every case is going to be decided based on that company's particular risks and whatever the particular facts are. Thus, while "there is not any kind of safe harbor that companies can rely on to feel confident that its cybersecurity measures are going to pass muster, they can take some comfort that if they are focused on the issue and doing something to try to manage their risk according to the Framework, they should hopefully be on the right track."

Citi's Institutional Clients Group director and associate general counsel Anjli Garg agreed that a company's approach to security will depend on various factors. The NIST framework is "a voluntary framework and not a stringent set of rules," she said, adding that companies should consider using it "in building their own framework on the security side." She said that it will be up to the individual organization to make a determination about what measures get put in place "based on what its industry is, what data it is collecting, what it needs to keep safe and how its systems operate. Every company is different. If you have servers all over the world and you are using third parties globally to store data, your situation is going to be different than if you are a very small company localized in one place."

Garg acknowledged the framework's value, noting that it was "developed after a rigorous process." But organizations should understand that "it is just one framework and not the gold standard."

Does NIST Risk Management Approach Demonstrate Reasonableness?

The FTC has said the NIST Framework is not intended to serve as a checklist. Because it "very effectively parallels what the FTC is looking for," however, unless there is a very specific failure in the company's practices, if an organization applies the risk management approach that is presented in the NIST Framework, the FTC "would most likely conclude that it is maintaining reasonable security standards," Paulding said. The NIST framework "is a good baseline," if it fits the company's environment and structure.

Hildebrand agreed. While the Framework "is not a prescription for doing it right, it does prescribe significant guidance. So, if a company is looking for guidance on how to structure a data security program, knowing that the FTC could inquire about it, the security team could point to implementation of the NIST standards to demonstrate that its program was appropriately tailored to its business."

Companies should still be cautious, however, Golinsky said. NIST is a framework and not a prescriptive regulation or legal standard and "it will come down to the specific facts and circumstances as to whether the FTC would find a security program is put together and followed with the right level of vigor. The vigor is the key." In other words, a company should

be able to demonstrate reasonableness only if a proper security program is implemented with reasonable "rigors and controls," she stressed. See also "*Regulators Speak Candidly About Cybersecurity Trends, Priorities and Coordination*" (Apr. 27, 2016).

How Practitioners Use the NIST Cybersecurity Framework

Typically, Paulding uses the NIST Framework much like the FTC blog post suggests, "as a baseline for some of my clients, largely depending on the level of complexity of their data flows, their organization and the threats that they face. It is not necessarily a tool that I would use with medium-sized clients." For his medium-sized clients subject to HIPAA or those whose primary source of sensitive, personal information is payment card information, "the clear guidance of the HIPAA security and privacy rules, or the PCI data security standards tend to be more immediately relevant control frameworks." Otherwise, he uses the FTC's Start With Security or Protecting Personal Information guide to business as a framework for medium to relatively large companies.

Guidance for Sophisticated Companies

The NIST framework is often a good basis for guiding companies that face a larger threat structure. The NIST Framework is more likely to serve as guidance "when I am dealing with much larger, sophisticated Fortune 100 and Fortune 500 companies, in large part because they also have more security resources available," Paulding said. Thus, it is easier to implement the NIST Framework's more detailed approach.

These bigger companies also tend to be targets for a wider variety of cyber threats, Paulding noted. He finds the "NIST guidance to be an easier way to structure a multi-layered security program designed to mitigate a very wide variety of risks." These sophisticated companies are facing "not just the individual hacker looking to steal some data that they'll sell on the black market to the first buyer, but also hacktivists, state-sponsored threats and disgruntled employees, who tend to be a little bit of a bigger threat in Fortune 500 types of environments."

Building Blocks of Security

Hildebrand reads the framework for her own education as part of understanding her clients' business and for participating in some initial brainstorming with them. She also will send it to clients with the recommendation that the IT and security people read it as part of helping them understand the process for building and implementing a data security program. The NIST framework's core values are "like the building blocks of security" and they come together to create a whole process. What some clients think of as a policy might not qualify as one because "they effectively put it in a drawer and don't look at it again," Hildebrand noted. The NIST framework, however, provides tools to help "make that policy a living concept."

Strong Similarities Between Standards

"There are very strong similarities between all of the applicable data security standards of PCI, HIPAA, FTC enforcement actions, NIST and ISO. The general principles of good cybersecurity are actually pretty universal," Paulding pointed out. See also "*Privacy and Data Security Considerations for Life Sciences and Health Technology Companies (Part One of Two)*" (Oct. 14, 2015); *Part Two* (Oct. 28, 2015).

While the various data security standards are structured differently, "the general principles of identifying risks on a continuous basis, designing your security controls to address the reasonably foreseeable risk, monitoring the security on your systems and maintaining things like minimum necessary access are pretty universal across all of those standards," Paulding added.

That being said, if a company is within the scope of a specific set of regulations, then those should be its "first touchpoint," Paulding advised. Companies handling protected health information would start

with HIPAA. With payment card data, the FTC has not gone so far as to say compliance with PCI meets the reasonableness standard, "but I have yet to see an enforcement action involving payment card data that did not also involve allegations of practices that were inconsistent with PCI," he added.

Three Initial Steps to Meet the Reasonableness Standard

Given the changing technology landscape and the variety of business models, the FTC will not define what actions specifically meet the reasonableness standard, Hildebrand noted. "With the FTC reluctant to define exactly what meets the reasonableness standard, companies find themselves needing to navigate the regulator's consent decrees, and various frameworks and guidelines that outline the contours of what the FTC might expect." While this can be an overwhelming undertaking, the experts with whom we spoke offered some advice on where to start.

1) Start At the Top

To develop and implement an effective data security program, companies need to start at the top, Golinsky advised. There has to be a company-wide commitment and "if it doesn't come from the top, you are never going to have an effective framework. So, you have to start at the top to make sure the compliance program has support at the highest level because, as with any kind of compliance program, if you do not have the correct cultural tone at the top about it being a priority, it is never going to really be successful." See "*Establishing Strong Cybersecurity and Data Privacy Leadership: The Roles of the Chief Information Security Officer and Chief Privacy Officer (Part One of Two)*," (May 6, 2015); *Part Two* (May 20, 2015).

While the commitment starts at the top, there also needs to be "resources devoted to the program in all the right places. Something like cybersecurity may not involve just an attorney or a technology person," Golinsky said. There needs to be cross-functional support so that "you can ensure you have the requisite direction and expertise to build something that complies with whatever your legal obligations are. So, you start at the top, you get the right tone and commitment to the program and you make sure you have the right players at the table who provide you all the pieces of expertise that you need to actually build something that is both compliant and effective." See "*How Can a Company Mitigate Cyber Risk With Cross-Departmental Decisionmaking?*" (Apr. 8, 2015).

2) Take Stock of the Risks

When Paulding is advising clients, he always starts with a key question: "Do you have a process in place for conducting formal assessments of the risk to your confidential information? That's always the first step, because actual security measures should be based on an assessment of the foreseeable risk facing the organization."

Golinsky agreed that the risk assessment is important. The first practical step, once there is commitment at the top and the necessary players are at the table, "is doing an inventory of what your cybersecurity current state is, what your risks are, where you have strengths and where you have weaknesses." With that information, the company can determine whether what it is doing is adequate or if there are practices or policies that need work. See also "Ten Actions for Effective Data Risk Management" (Apr. 8, 2015).

Part of the assessment will include a "very thorough inventory of your entire company and all the places where you have data or information that would cause a problem if something happened," Golinsky continued. Once a systematic inventory (whether it is done by business unit or type of data) and the "technological outlook" is complete and any security holes or gaps are identified, the organization should "make sure it has plans and back-up plans in place. First you want to make sure data is secure but then you also want to have a back-up plan. If your security is broken, then what are your protocols for making sure that you are stemming the damage?"

3) Create a Formalized Security Program

Once the assessment is complete, the next step is to ensure that the security program is formalized.

"It's important to remember that the formalization process forces the organization to sort of challenge its assumptions about its existing safeguards and its existing risks and forces it to maintain a certain level of continuity in its security program," Paulding stressed. Because "staff changes as business expands, having a formal written policy that is also subject to the same continuous review process as all other risk is critical for ensuring a company is rigorous about its security program and that it remains rigorous over the long term – not just when it becomes a priority or in the immediate aftermath of a breach," Paulding added.

Formalizing the program involves documenting it and conducting regular reviews and updates "to maintain effectiveness in light of how your business evolves," Paulding continued. However, "that's not always enough," he pointed out. He suggested that it is important for the program documentation to accurately reflect the company's risks and safeguards. "Security documentation and programs should never be aspirational. They should be factual. They should reflect actual practice and actual business needs and that is very important because often the data security documentation is written in a vacuum and then sort of bolted onto existing business practices. That will frequently fail if there's no business buy-in and the business does not appreciate that the program was designed to function within what they do," he cautioned.

"Ultimately, there are very few companies that are in the business of cybersecurity," Paulding noted. Most of his clients are companies where cybersecurity is an operating cost. "So, in order to get buy-in from the revenue centers, they need to feel like that security program fits with what they do to make money." That is one of the reasons why it is "very important to make sure that the documented policies are consistent not just with the company's risks, security needs and legal obligations, but also with what the business does, essentially for a living."

See also our three-part guide to developing and implementing a successful cyber incident response plan: "*From Data Mapping to Evaluation*" (Apr. 27, 2016); "*Seven Key Components*" (May 11, 2016); and "*Does Your Plan Work?*" (May 25, 2016).

The CYBERSECURITY LAW REPORT

www.cslawreport.com Volume 2, Number 22 November 2, 2016

FTC

Demystifying the FTC's Reasonableness Requirement in the Context of the NIST Cybersecurity Framework (Part Two of Two)

By Jill Abitbol

Many companies are still wondering how to develop and implement a data security program that meets the FTC's reasonableness requirement. "There is a hunger for a checklist," Kelley Drye partner Alysa Hutnik told The Cybersecurity Law Report. Although not necessarily applicable across the board, the NIST Cybersecurity Framework, along with the FTC's comments on it and its release of a new breach response guide, serve as useful resources. In this second part of our two-part series on the FTC's data security expectations in the context of the NIST Cybersecurity Framework, in-house and outside counsel discuss how the Framework's core functions align with the FTC's requirements. They also provide steps companies of all types and sizes can take to incorporate these functions into their own security practices. Part one explored the implications of the FTC's recent communication and detailed three initial steps companies should take to meet the FTC's reasonableness standard. See also "*A Behind-the-Curtains View of FTC Security and Privacy Expectations*" (Mar. 16, 2016).

Key Elements of Cybersecurity

The Framework recognizes that there is no one-size-fits-all approach to managing cybersecurity risk because organizations face different threats and have different vulnerabilities and risk tolerances. Given these variances, the "FTC's focus is about process," Hutnik said. The Framework "provides an outline of the process to apply but it is up to the company to decide the nuts and bolts of what happens during that process."

While the Framework cannot serve as a checklist, it provides organizations with a risk-based compilation of guidelines that can help them identify, implement and improve cybersecurity practices. This compilation of practices is referred to as the "Core." This Core is composed of five concurrent and continuous functions – Identify, Protect, Detect, Respond and Recover – that provide a strategic view of the lifecycle of an organization's management of cybersecurity risk. The FTC believes the "five functions signify the key elements of effective cybersecurity." These functions "line up very closely with the FTC's expectations," Hutnik said.

Applying NIST Core Functions

There are specific practices that can achieve the outcomes associated with each of the NIST Core functions, experts told The Cybersecurity Law Report.

Although the FTC has communicated that these concepts apply to all companies, the extent to which companies implement them will vary, Hutnik said. "If you have any kind of personal information, then these basic concepts are something the FTC does expect that you have in place."

Identify

The Identify function helps organizations gain an understanding of how to manage cybersecurity risks to systems, assets, data and capabilities. "Starting at the beginning and making sure you understand your exposure is the most important first step," Jodi Golinsky, general counsel and chief compliance officer for FS Card, Inc., told The Cybersecurity Law Report. Gaining an understanding of your business' protectable data assets and the attendant risks requires a "team approach," Lowenstein Sandler partner Mary Hildebrand advised.

Particularly with large or fast-growing companies, many aspects of the business may be decentralized or geographically dispersed. Companies may also have a significant number of employees who work

remotely, or a structure where employees do not have assigned offices but, rather, work from laptops within a larger work space. These structures may make it more challenging to be able to identify data assets. "Decentralization may sometimes lead to a more casual environment and a boost in productivity, but asset identification is one area where you don't want to be too casual," Hildebrand cautioned.

So, "it is not realistic or recommended for any one person in an organization to be charged with sole responsibility for identifying data assets across the enterprise or making risk assessments," Hildebrand explained.

The team approach requires IT and legal to work together in order for there to be appropriate implementation of the Identify function with an appropriate program in place. When there is a lack of partnership between IT and legal, "there may not be an effective risk assessment and written program," Hutnik said. See "*Coordinating Legal and Security Teams in the Current Cybersecurity Landscape": Part One* (Jul. 1, 2015); *Part Two* (Jul. 15, 2015).

"The low-hanging fruit for the FTC has often involved cases where the company lacked a comprehensive written information security plan." So, having written policies and procedures in place is a "key aspect of the identify function," Hutnik said.

"One person or a small team could be responsible for gathering data and then executing the plan, but it needs to be an enterprise-wide undertaking. It's not a localized function," Hildebrand advised. The key is to start with an inventory and "have all of the right people who have knowledge and information at the table," Golinsky added. See also "How Can a Company Mitigate Cyber Risk With Cross-Departmental Decisionmaking?" (Apr. 8, 2015).

Protect

The Framework's Protect function provides guidance to help organizations develop and implement appropriate safeguards to ensure the delivery of critical services and to limit or contain the impact of a cybersecurity event.

To meet the Protect function set forth in the NIST Framework, Hildebrand emphasized the importance of access control, which includes matching job functions to the data that is required in order for the individual to meet his or her responsibilities. For example, a business that uses highly sensitive information that is kept in a database should determine who will have access to that information, for what purpose and how the access will be monitored. While this is "fairly straightforward, when a company is moving a billion miles an hour, focusing on the issue can be a challenge."

These technical and administrative safeguards should come from the written program, Hutnik said. The program should address what the sensitive information is, where it is stored, who has access to it and then, how it can be reasonably protected. "Knowing is the first step. Once you have the information the doing something about it is the Protect step."

Hildebrand noted, for example, a recent breach that occurred when a company's IT department accidentally granted a temporary worker access to HR information, including reviews and bonuses. "That kind of error has the potential to be quite damaging. If an appropriate system is in place to detect the error early, then the consequences should be manageable; however, achieving this level of preparedness requires a thoughtful evaluation and assigning accountability within the company to ensure the protocols are followed. All of these considerations point to the importance of training for employees and agents. That's so, so critical," she said.

Hutnik agreed. "The human element of the Protect function should be addressed as reasonably as possible through training, reminders and auditing."

Another part of access control requires restrictions around adding new technologies to the network, Hildebrand said. "While companies are, on the whole, savvier about this, we still see situations where employees introduced new programs to the system without consent and there's no infrastructure to block that access." She believes this is "readily addressed from an IT standpoint."

Detect

The Framework's Detect function delineates various steps that organizations could take to develop and implement appropriate methods to identify the occurrence of a cybersecurity event in a timely manner. "The FTC and other regulators really focus on breaches that get disclosed a long period after they occur because the reason may be that there is a failure to detect that the breach happened in the first place," Hutnik noted.

Hildebrand suggested there are "a number of approaches to detect security incidents," including many "technology products and services." One of the most important approaches is 24/7 monitoring. Companies should also have "appropriate protocols in place so that people understand their obligation to report an anomaly and may do so without fear of losing their jobs. Employees' first reaction should not be to cover it up, or delay reporting."

"You have to stay current with the technology and market conditions. I don't think there's any substitute for staying current," Hildebrand said. Hutnik added, "The best of plans and life sometimes collide." A company may have a security plan that served it well for the past several years but "the fact is that things keep evolving." Companies need to be mindful of that and ask themselves whether their current data security plan still works, their training program is effective, their firewalls are sufficient, and remote access is secure enough. "Unless you are actually looking and have controls in place to see if your program is working, it is going to be really tricky to figure out if you have a gap that needs to be addressed," she noted.

Respond

The Framework's Respond function provides guidance on how to develop and implement appropriate actions in response to a detected cybersecurity event to effectively contain its impact.

"Assume and plan for the worst," Hildebrand advised. Companies must be prepared to do "a very quick analysis of what transpired in order to resume conducting business as soon as possible, or move operations to disaster recovery mode. There's no question that disaster recovery planning is an integral part of a response plan." She stressed that all of these components require constant and effective communication to key stakeholders.

The Response function is "a consumer protection fundamental," which requires an "incident response plan that people are trained on and familiar with." Hutnik pointed out that, "the FTC aside, there are a lot of studies showing how much money is saved by just having that type of control in place."

Once an effective response plan is in place, "the timing of the response is going to be crucial," stressed Hutnik, adding that "a number of factors go into a company's ability to respond in a timely fashion." These factors may include "doing the tabletops, knowing who your team is and working through the hypotheticals or scenarios that perhaps the company has gone through in the past and examining what would they do differently."

All of the stakeholders should be aware of their roles in advance of a breach so that they are not stuck "learning under a time clock," Hutnik advised. "I don't care how many [breaches you handle] – you are always learning something new. But, the more that [response] becomes muscle memory, the more efficiently you are going to work."

The Response function also applies in the context of a product security flaw. Given the foreseeability of software security flaws, Hutnik recommended having a process in place to deal with it "so that you can respond in an appropriate way."

Recover

The Framework's Recover function outlines steps organizations could take to develop, implement and maintain plans for resilience and to restore capabilities or services that were impaired due to a cybersecurity event.

Of all of the Framework's different functions, Recover is "probably the one that is most fact-sensitive because efforts to recover from a security incident or data breach depend on the nature and severity of the breach and the data involved," Hildebrand said. If, despite best efforts, a security incident or data breach occurs, a company may need to upgrade its technological defenses, address internal policies regarding access to critical data, security protocols, vendor management programs or other areas. Recovery "is very fact-specific in terms of what's undertaken and the concept of what an improvement would actually mean in practice."

The Recover function is a critically important opportunity to learn from the incident/breach, and improve the process in anticipation of the next event. "By the time you get through a data security incident, you're pretty much exhausted. When things finally seem to be back to normal, the instinct may be, 'Well, thank God that's over. I'm not going to do this again.' But you're really doing yourself and your team a disservice if you let it drop without doing a retrospective to learn everything the incident can teach you about what to do, and what NOT to do," Hildebrand said, adding that when she works with clients after a data breach, she always waits a few days and then encourages them to undertake these efforts. "It's the right time to do it. Everyone's memories are fresh, so that's a good time to tweak a plan or take another look at your defenses and the other programs you have in place from a security standpoint and decide what could be improved."

Part of the remediation plan also includes having a budget and insurance, and understanding what that insurance does and does not cover. Planning a budget requires considering what might need to be purchased to remediate, negotiating pricing in advance and knowing what internal resources will be used, Hutnik said.

Synthesizing FTC Enforcement Actions

The FTC's reference to its 60-plus enforcement actions as guidance with respect to reasonable cybersecurity practices "is excellent because it provides insight regarding minimum standards, as well as examples of circumstances that might justify a higher standard of care," Hildebrand opined.

See "*FTC Director Analyzes Its Most Significant 2015 Cyber Cases and Provides a Sneak Peek Into 2016*" (Jan. 6, 2016).

With each enforcement action comes a new fact pattern. "In the early days of the FTC's enforcement, you could come up with your very clear list of top 10 things it was focused on – for example, sequel injection attacks, the unencrypted laptop with sensitive information or the vendor where you had no security controls with teeth on them." While practitioners in this area will read each of those 60-plus actions and settlements, the FTC synthesizes lessons learned from these actions in its guidance, Hutnik pointed out.

For attorneys and other professionals whose jobs entail data security responsibilities, Hutnik recommended setting "Google alerts for the FTC's data security enforcements or signing up to have press releases come to your inbox so that you see when there is a new privacy or data security enforcement example or closing letter."

Enforcement Trends

Opinions differ on whether the FTC's enforcement trends follow particular industries. However, Hildebrand said she believes the FTC "identifies situations where a

company has not evidenced clarity of thought regarding data privacy and security," and responds with a series of organizational programs.

For a number of years, the FTC focused on breaches, but more recently there has been a focus on product, and having secure process and controls around products released to the public, Hutnik noted, citing AsusTek, Henry Schein, and Nest Labs.

Hutnik also suggested that recent guidance and workshops indicate the FTC's emphasis on the internet of things and mobile apps. There are also "some enforcement examples that tie with that. So, when you see guidance go out, and you see some enforcement, those are indicators of concern by the FTC." In many of these cases, "the focus has really been on sensitive information," such as health data. Thus, "if you are in that space, that is a good indication that you are going to be under the spotlight for a while."

Ultimately, it comes down to whether there is consumer harm. "That's what you often see the agency focusing on and their view of harm is a broad one but they can make ripples in the industry," Hutnik said.

See also "*Regulators Speak Candidly About Cybersecurity Trends, Priorities and Coordination*" (Apr. 27, 2016).

Other Resources That Provide Guidance

With the various standards out there, if there is an aspect of the NIST Framework guidance that is not necessarily a fit for a particular company, there are other resources. "And, in many cases, that is going to be okay with the FTC if you have thoughtfully applied appropriate controls to your business and the data and risk that your business has," Hutnik shared.

In its "blog post, the FTC makes it clear that the Framework is not going to be a silver bullet. If you are looking to satisfy the FTC, you should of course follow its guidance. The best strategy is one that takes all guidance into consideration and staying abreast of anything the FTC puts out on this," FS Card's Golinsky cautioned.

She explained, "the Framework was published in 2014 and things change a lot in this area. I don't know that there is anything out there as comprehensive, which is why it's such a useful resource." However, she believes that "anything the FTC publishes that would help provide guidance is critical for any company to use and take into consideration."

Start With Security

The FTC's "Start With Security" guidance "echoes a lot of the process elements of NIST," Hutnik noted. She suggested that, "when figuring out where to start, both resources are helpful," but cautioned companies to ensure that any security program they implement is relevant to their business and that they "haven't left out big areas of risk related to privacy or security on that route."

See "*The FTC Asserts Its Jurisdiction and Provides Ten Steps to Enhance Cybersecurity*" (Jul. 15, 2015).

Hildebrand finds Start With Security "more straightforward than NIST." She likes it because it makes an implicit point that "you cannot have privacy without adequate security."

FTC's Recent Breach Response Guidance

On October 25, 2016, the FTC released a guide for businesses on how to respond to data breaches. This guidance essentially "restates similar guidance and best practices on data breach response in a user-friendly, clear format, and includes a model template consumer notice, which is likewise in a user-friendly format," Hutnik observed. She cautioned, "If an organization chooses to use the FTC's template, it will need to make a few adjustments to account for some state law variations."

"If using the NIST Framework, much of the incident response is within the Respond (by having effective incident response processes that are able to quickly identify and contain the breach) and Recover (steps to take after the security event, including

communicating with affected parties – such as consumers, law enforcement) functions. And if the breach event uncovers gaps in the program, then the Protect function may need to be updated, as appropriate."

California AG Guidance

Recently, the California AG referenced in their guidance the CIS Controls page. For no charge, "it provides, under license, excel spreadsheets that go through their various controls and how to do that in practice," Hutnik explained. This, and other inexpensive or free process-focused resources out there "can help along the way so you do not need to reinvent the wheel and do it from scratch. But at the end of the day, they are just giving you those tools for you to then apply. I have not seen a successful scenario where you take these tools off the shelf and you just publish them. You really have to do the process part of the work and apply it to your business."

NIST HIPAA Standard

The NIST HIPAA Security Rule guidance is "not just for clients subject to HIPAA, Hildebrand said, noting that she refers to this guidance "a lot. In some sense it's a gold standard because of its extremely high standard of data encryption."

See also *"Privacy and Data Security Considerations for Life Sciences and Health Technology Companies" Part One* (Oct. 14, 2015); Part Two (Oct. 28, 2015).

Experienced Counsel

While there is certainly no shortage of guidance out there to help companies of all sizes and in all industries get started, "you need sophisticated and experienced counsel and compliance individuals to assess what the standard is and then how to measure the standard. Legal counsel explains what the legal standard is and then, on the client side, there needs to be a person to monitor and manage that standard," Golinsky said.