Dear members and friends,

The Public Company Accounting Oversight Board announced that William D. Duhnke III was sworn as Chairman. The ceremony took place at the Securities and Exchange Commission.

"I am pleased to lead the PCAOB in its mission to protect Main Street investors and promote public trust in quality audits of public companies whose securities trade in U.S. markets," said Chairman Duhnke.

"As the other new Board members join the PCAOB, I look forward to developing a collaborative and consensus-based approach to PCAOB's programs and operations and advancing sustainable audit quality that benefits the capital markets."

Immediately prior to joining the PCAOB, Chairman Duhnke served as majority staff director and general counsel of the U.S. Senate Committee on Rules and Administration under Chairman Richard C. Shelby.

The committee has jurisdiction over the rules and administration of the Senate and leads the strategic planning and implementation process for the functional and technical infrastructure support of the Senate.

Earlier, Chairman Duhnke twice served as the staff director and general counsel for the Senate Committee on Banking, Housing, and Urban Affairs.

The committee has oversight and legislative jurisdiction over a wide array of matters affecting financial services, including oversight responsibility for financial regulators such as the SEC and the PCAOB.
A Wisconsin native, Chairman Duhnke served in the U.S. Navy, rising to Lieutenant and serving in The White House.

You may read Chairman Duhnke's full biography at: https://pcaobus.org/About/Board/Pages/WilliamDDuhnke.aspx
Thank you so much, David, for that kind introduction. It's great to be here at the Tulane Corporate Law Institute for what, I know, is one of the most highly-anticipated corporate-law conferences of the year. It also doesn't hurt that it happens to be in New Orleans.

Now, before I begin, let me just give the standard disclaimer: the views I express here are my own and do not reflect the views of the Commission, my fellow Commissioners, or the SEC's Staff. And let me add my own standard caveat: I hope someday to persuade my colleagues of the utter, absolute, and obvious correctness of my views.

Although it already seems like a lifetime ago, I was only recently sworn in as an SEC Commissioner in January. It's been a privilege to serve and an amazing experience so far—made all the more so by the incredibly talented and hardworking SEC Staff with whom I have the honor of working each day.

Since I was, in a previous life, a corporate lawyer at Wachtell Lipton, folks have asked me what it's like to be an SEC Commissioner—so let me share a bit about the glamorous existence of a Commissioner.

Each day, my staff and I spend hours combing through thick binders of rules, guidance and enforcement actions that we review, redline and spot check for potential issues. In between meetings, it's not uncommon for us to spend time with other gripping page-turners—you know, like corporate proxy statements.
We're always speculating what the guy down the hall, who spent 20 years being one of the world's finest corporate lawyers, is thinking, and when he might send us more work.

In short: being a Commissioner is a chance to relive the glamorous life I had as a first-year associate working for David Katz! Chairman Clayton tells me that there's little chance of a closing dinner anytime soon. But at least these days I have a nicer office.

Still, I don't think I could possibly find more interesting, challenging, or fulfilling work. Nor a better group of colleagues to do it with. Nor a more important or pressing set of issues to deal with. It's an incredibly important time for our Nation, our economy, and the Commission, and I'm honored to be a part of our efforts to keep pace with our ever-changing markets.

That's why I wanted to focus today on what I think is the most pressing issue in corporate governance today: the rising cyber threat. As anyone who spends time in the boardroom knows, the digitization of our economy is revolutionizing the way business is conducted.

From Wall Street's financial institutions to mom-and-pop retail stores, almost every company—in every sector of the economy—is on some level a technology company.

And advances in computer processing, cloud computing, and smart devices are making it faster, cheaper, and easier for firms to leverage data to improve nearly every aspect of their business every day.

I am, by nature, optimistic about the technological transformation currently underway across corporate America. But I'm also realistic about the challenges we face. Hardly a day goes by that we don't hear about another threat, hack, attack, or major cyber event.

The sources of all these bad acts are evolving—from rogue programmers to organized crime rings to state-sponsored actors. That's why I was so struck to read the Director of the Defense Intelligence Agency's recent statement before the Senate's Armed Services Committee.

Director Ashley told Congress that our "top adversaries are developing and using cyberspace to . . . compromise[e] our national defense."

He's right: our companies, and our country, are under attack.
In 2016 alone, there were over 1,000 data breaches—a record high—costing American companies more than $100 billion, according to data gathered by the Identity Theft Resource Center.

With that much money, you could buy every single team in the National Football League—and still have $20 billion left over to build a stadium.

Last year, 20 million Social Security numbers were exposed in connection with cyber breaches.

That’s the equivalent of having every person here in Louisiana have their Social Security number stolen—four times. And as your clients know well, the financial cost from the fallout once there is a breach—shareholder lawsuits, regulatory penalties, and reputational issues—will only continue to add up.

No issue in recent years has rocketed to the top of the corporate agenda faster. In 1975, 17% of S&P 500 firms' market value was tied to intangible assets; in 2015, that number was 87%.

One recent study showed that nearl two-thirds of executives identified cyber threats as a top-five risk to their company’s future.

That shows how quickly this has become a board-level issue. When I was in practice over a decade ago, these issues weren't even on the radar screen of many corporate directors.

Today there is no doubt for top corporate counsel: if you're not talking about cyber risk with your clients in the boardroom, you're making a mistake.

Indeed, across America companies are desperately seeking direction as they grapple to identify and follow best practices for cyber risk management.

As many of you know, we at the SEC weighed in on this issue just last month, providing Commission-level guidance related to the disclosure of cyber incidents.

Although I reluctantly joined the guidance, I believe that we regulators can and must do more on this issue. More on that in a minute.
Right now, our most sophisticated companies are already taking concrete action to protect their businesses from those who would use technology to cause harm. Many are investing heavily in new defenses, personnel and protocols to improve their cyber risk management posture. They are trying to innovate their way to safety.

But while these companies should be lauded for their efforts, I would suggest that we need a much more comprehensive response.

Yes, new rules and regulations can help push companies toward cyber resiliency. Yes, improved technological defenses will help mitigate the cyber threat. But these are tactical responses to a strategic problem.

We need to think bigger. The cyber threat is not primarily a regulatory issue any more than it is primarily a technological issue.

Cybercrime is an enterprise-level risk that will require an interdisciplinary approach, significant investments of time and talent by senior leadership and board-level attention.

In short: the cyber threat is a corporate governance issue. The companies that handle it best will have relevant expertise in the boardroom and the C-suite, a strategy for engagement with investors and the public, and—most of all—sound advice from corporate counsel who can navigate uncertain times and uncertain law in a critical area for the company’s business.

My project today is to enlist all of you in preparing America’s companies to meet the cyber challenge. I want to describe three areas in which I believe sophisticated corporate counsel can, in partnership with my colleagues at the SEC, help lead the way in developing the practices that will determine whether we win or lose the struggle to protect American companies from cyber crime.

Nothing is more important to the SEC's core mission of protecting the investing public. And nothing is more important to the future of the American economy.

The Law of Cybersecurity and Disclosure

Let’s start with the rules at the core of the SEC’s mission: the law of disclosure. The Commission’s latest guidance, which we issued last month, aims to promote "clearer and more robust disclosure" of cybersecurity breaches.
But that guidance, like the 2011 Staff-level instructions it reaffirms, relies heavily on the judgments of corporate counsel to make sure investors get the information they need.

I worry that these judgments have, too often, erred on the side of nondisclosure, leaving investors in the dark—and putting companies at risk. I think we at the SEC have much more work to do in getting investors the information they need to understand cyber attacks. And we need your help to get there.

Since 2011, empirical study and hard experience suggest that we're not seeing consistent, timely and complete disclosure on cyber attacks. One 2014 paper argued that the boardroom implementation of our Staff's guidance "resulted in a series of disclosures that rarely provide differentiated or actionable information for investors."

Another contended that our guidance in this area "fails to resolve the information asymmetry at which the disclosure laws are aimed."

And our own Investor Advisory Committee recently observed that public-company disclosures regarding cybersecurity incidents have not meaningfully improved since 2011.

What's more, when a company's cyber defenses are breached, that fact can find its way into the market even when the firm chooses not to inform investors by filing an 8-K. You see, SEC rules are hardly the only ones that require public companies to reveal data breaches.

Our rules are based on materiality. Brighter lines are found in the state law arena. There, a patchwork of ever-changing state laws, along with state and local regulators, often require notification to consumers when residents' personally identifiable information has been compromised.

In my home State of New York, for example, when personal data has been wrongfully obtained, that fact must be reported to state regulators as well as to consumers both inside and outside New York.

In fact, all but two States have enacted their own breach-notification laws.

And when state or local laws lead to revelations that are not shared with investors, companies and their counsel face significant risk.
I wanted to learn more about disclosure practices in this area, so I ran the numbers myself. My staff and I compiled evidence on data breaches in 2017 that were reported to state and local regulators, as well as to the press.

After removing minor breaches from our dataset, what we found surprised us: of 81 cybersecurity incidents at public companies in 2017, only two companies chose to file an 8-K disclosing the breach to their investors.

**In other words, in 2017, companies that suffered data breaches chose not to file an 8-K more than 97% of the time.**

That's not to say, of course, that all of these events were material or required disclosure. But there is significant evidence that events like these matter to the market. One recent survey, for example, found that 20 of 25 academic studies found negative and significant stock-price reactions for firms that are victims of cyber attacks.

And in a compelling and important new paper, two Columbia Law School scholars have identified systematic evidence of arbitrage opportunities when traders learn of cyber breaches that have not yet been disclosed.

I don't need to tell all of you about the risks that a board faces when information on a cyber breach leaks before the news has been shared with investors.

**Besides public approbation and litigation**—just days ago, Yahoo! agreed to pay $80 million to settle a suit related to data breaches—the board and management are forced to spend time scrambling rather than pursuing a viable long-term strategy for cyber defense.

In the meantime, a few sophisticated and speedy traders may benefit from informed trading, while average American investors suffer. None of this reflects a productive investment of precious resources—and it's not nearly good enough to meet the rising cyber threat we face.

I've called upon my colleagues at the SEC to give careful consideration to new 8-K requirements governing cyber events.

I understand, of course, that we must strike a careful balance in this rapidly changing area. But I believe America's companies and corporate bar can do better. And I believe that any rules we make are only as good as the work of the lawyers in the boardroom, where the rubber meets the road.
I hope each of you will urge upon the boards you counsel the pressing need for transparency in this area—and will share, with clients and with us at the SEC, the best practices you are developing to ensure that investors get the information they need when our companies are attacked. Those practices will, I hope, soon inform the next steps my colleagues and I will take in this critical area.

**Cybersecurity and Insider Trading**

Now let's turn to an especially troubling implication of some of the most high-profile and recent cybersecurity incidents: insider trading. There's no doubt that investors' confidence is shaken whenever they learn that a company's cyber defenses have been hacked.

But when it's revealed that the insiders entrusted to protect investors used those events as an opportunity to profit personally, investors rightly question the basic trust that forms the core of our markets.

As many of you may know, at the time of the Equifax breach it was reported that certain insiders sold shares even after the firm's Chief Executive Officer discovered the issue but before the breach was revealed to the investing public.

While I cannot comment on any SEC investigations or ongoing litigation, I can say that it is especially alarming when reports of a breach are accompanied by reports of insider trading.

It is deeply troubling that insiders may have been able to profit in this way, regardless whether those specific insiders knew about the breach before engaging in such trading.

There are two important questions raised by these events that I hope you'll help us grapple with. First, are we doing enough in corporate boardrooms to ensure that, when any member of the senior management team learns material nonpublic information, all members of the team avoid trading? As our Chairman, Jay Clayton, has explained, procedures like those are an "important part of good corporate hygiene." They also have the key benefit of encouraging senior management to share critical information early and often with their colleagues.

While I know that some of you are already advising your clients to adopt policies to address these situations, I worry whether those policies have made their way across the wide spectrum of companies and industries that...
make up our markets. Before I joined the Commission, I wrote a study with two much-more-talented colleagues that identified a surprising amount of trading by corporate insiders during the four-day period between the time when material nonpublic information was discovered and when it was revealed to the public.

Although I’m hopeful that Congress, or the Commission, will soon act to address this kind of trading, we can and should learn a great deal from the best practices all of you are developing in this area. I urge you to help us make sure that senior management knows that it makes little sense to trade when material nonpublic information has yet to be revealed to investors.

But there's a second, and even more important, question raised by these developments: Does the law we have today adequately address situations where traders take advantage of nonpublic knowledge that a company has been hacked?

As others have observed, it is far from clear whether or how current law would apply to cases where the trader is not herself a corporate insider.

That raises the very real concern that hackers will not only continue to attack American companies—but that they might be able to profit by trading before the investing public discovers what they have done.

That's a concern that, I know, is shared by your clients. One recent survey of corporate executives found that financially motivated hackers are the actor that concerns them the most in this area.

In the midst of the war we are fighting on the cyber front, we cannot allow our securities markets to be a source of profit for hackers who use technology to harm the companies that are crucial to the growth of our economy. I hope all of you will help us ensure that best practices—and the laws governing insider trading—keep pace with this ever-changing threat.

**Cybersecurity and Internal Controls**

Although I had reservations about our recent guidance in this area, one important part of the Commission's statement has, in my view, been overlooked. The guidance specifically urged companies that "[c]ybersecurity risk management policies and procedures are key elements of enterprise-wide risk management," and noted our expectation that firms will have "sufficient disclosure controls and procedures in place
to ensure that relevant information about cybersecurity risks and incidents is... reported... up the corporate ladder."

Building that kind of system is a significant challenge for most public companies. The reason, of course, is that the experts who best understand the cyber threats a company faces are rarely among the company’s lawyers.

Instead, they are technologists trained to grapple with the latest innovations in the dark art of hacking—and how to protect against them. As one expert in this area recently observed, "lawyers and computer programmers are like foreign cultures."

So we need ambassadors. Counsel like all of you are critical to helping companies build the internal reporting structure that will help boards and management better anticipate, assess, and, where necessary, disclose the next significant cyber attack.

You’ll need to help your clients assess their organization, learn where the critical knowledge is, and make sure there’s a clear and clean path from there to the C-suite—and, eventually, to investors. You might even have to sit in front of a computer and open a program other than Microsoft Word.

Many of you might be thinking that reaching across the divide between lawyers and technologists is a bridge too far, even for the world's finest corporate counsel.

But I'm here to remind you that you have done this before. For if there is anything as Byzantine, complex, intimidating, and critical to the health of a business as technology, it is, of course, accounting.

**Fifteen years after the passage of Sarbanes-Oxley**, the companies you counsel have a comprehensive set of controls that bring that specialized knowledge to the attention of management and, where necessary, the experts in the boardroom.

Many of you helped to build those systems by learning more than you ever wanted to know about the dismal science of accounting—where the key sources of information leading to financial reporting were located in an organization and how to make sure management could rely upon them.

Here, too, we will need your expertise in understanding how to make sure that information from technologists on the front lines of this war reaches senior management—and, where necessary, the board and investors.
This may well be the area that will demand the most attention from all of you over the coming months. **One recent survey** noted that 70% of executives at the S&P 500 named their IT department as a primary owner for cyber risk management—compared to just 37% who identified the C-suite or the board.

The same survey noted that, especially at large and growing companies, responsibility for these issues is often scattered throughout the organization, creating the risk that key information might not make its way to the decisionmakers who need it most.

I am hopeful that this part of our guidance will lead companies and their counsel to ask themselves whether their existing internal controls are up to the daunting task we face. And I know that all of us at the Commission will be on the lookout for the best practices you'll come up with to prepare your clients for this challenge.

* * *

The cybersecurity threat now gripping corporate America poses new challenges for companies, the SEC, and the investors we serve.

But whether those challenges relate to when and how to share information with investors, how to ensure that insiders trade on a level playing field, or how to design organizations so that its senior leaders have the information they need to do the right thing, they are all fundamentally questions of corporate governance.

We regulators can and should do more to protect American investors from the looming cyber threat. We at the SEC should consider **disclosure requirements** that would give all of you clearer marching orders on when and how to share critical information with investors.

And Congress or the Commission should also move quickly to make sure that, when one member of senior management learns material nonpublic information, no member of the team is trading in the company's stock.

We may also need to ask ourselves, more fundamentally, **whether the insider-trading law we have is adequate to meet these new challenges.**

Whatever we do, however, we will need sophisticated corporate counsel to help us make sure that our rules have the intended effect—in the
boardroom, in the marketplace, and in the race to protect our companies and our country from the hackers who would do us harm.

I hope you'll all join me and my colleagues on the Commission in pushing yourselves and your clients to develop the kinds of cutting-edge best practices we'll need to meet this challenge.

And I hope you'll keep this issue at the top of the corporate governance agenda—where it belongs.

Thank you once again for the opportunity to be here with you at Tulane today. I very much look forward to our continued conversations over the coming days.
Thank you very much to the Institute of International Bankers for inviting me to speak here today.

Among my first areas of focus when I was a very young lawyer starting out in my career well over 30 years ago was providing advice to foreign banks and financial firms operating in the United States, and I learned then just how integral, essential, and welcome a part your firms play in our domestic financial sector.

Non-U.S. firms serve as an important source of credit to U.S. households and businesses and contribute materially to the strength and liquidity of U.S. financial markets, so it is critical—not just as a matter of fairness but as a matter of our domestic interest—that we as regulators ensure that they operate in a fair and open financial services sector. I view that as an important part of my job.

So today I want to share my perspective on the appropriate regulatory environment for foreign banks operating in the United States, as well as some thoughts on specific elements of that regime. Before doing that though, we should take stock of the pre-crisis history of foreign firms operating in the United States.

First, the financial crisis revealed that in times of stress, international banking firms with large and complex local operations can contribute to
instability in those local markets and can require extraordinary support from local authorities.

**Second**, a number of foreign financial institutions expanded the size and complexity of their U.S. operations at a rousing pace and scale prior to the crisis, and we did not adjust our local regulatory and supervisory approaches to address the increased risk associated with this expansion.

As a result, the difficulties faced by the U.S. operations of non-U.S. banks during the crisis mirrored that of their similarly sized domestic counterparts, underscoring a need for increased resiliency of both domestic firms and the U.S. operations of foreign banks.

To bolster that resiliency, the environment for foreign banks operating in the United States underwent a number of changes. **While there are important differences**, those changes for foreign firms broadly parallel many of the changes instituted for domestic firms. My Federal Reserve colleagues and I have termed these the core post-crisis regulatory reforms: capital, liquidity, stress testing, and resolution planning.

Of course, the obvious and most prominent difference for foreign firms—as attendees of this conference certainly know—was the introduction of the intermediate holding company (IHC) structure, to which the post-crisis regulatory reforms apply.

In my estimation, these reforms have gone a long way toward meeting our goal of a more resilient financial system.

That said, we are now at a point—with ten years of experience in setting up and living with the body of post-crisis regulation—where it is both relevant and timely to examine the post-crisis reforms and identify what is working well and what can be improved.

If none of the regulatory measures implemented up to now were capable of improvement, this would be the first project of this scale and complexity conducted that had been done exactly right the first pass through.

If there was still work to be done after **Hammurabi**, there is probably still some work to be done now after **Dodd and Frank**. In particular, as I have said elsewhere, we should be looking to see where we can achieve our regulatory objectives in ways that maintain our measures’ effectiveness, but improve their efficiency, transparency, and simplicity. As part of that effort, we will consider additional tailoring and flexibility of our regulations.
in light of their impact on foreign banking organizations (FBOs) based on lessons learned over the past several years.

To illustrate how I am thinking about these issues, I want to focus in my remarks today on two specific regulatory examples. These are, of course, not an exhaustive list of work to be done in the regulation of FBOs, but they tend to be near the top of the feedback list from both the industry and supervisors.

First, I will discuss the application of enhanced prudential standards to FBOs, including our flexibility in implementing certain aspects of these standards. I will also offer some initial thoughts on opportunities for further tailoring that regime for FBOs.

Second is the Volcker rule. I will provide some of my initial thinking on how we might be able to improve the Volcker rule, both generally and in its application to FBOs in particular.

**Enhanced Prudential Standards**

In implementing enhanced prudential standards for foreign banks with a large U.S. presence, we sought to ensure that firms hold sufficient local capital and liquidity-and have a risk management infrastructure-that is commensurate with the risks in their U.S. operations.

And in general, that approach is meeting many of the broad goals the Federal Reserve set out to achieve.

Today, foreign banks with large U.S. operations are less fragmented, maintain local capital and liquidity buffers that align to the size and riskiness of their U.S. footprint, and operate on equal footing with their domestic counterparts.

Our current approach aligns with other jurisdictions that host a large and complex foreign bank presence.

For example, the European subsidiaries of U.S. banking firms have long been subject to Basel-based standards imposed by the European Union and the United Kingdom as host regulators.

In addition, European regulators are contemplating a holding company structure for the local operations of foreign banks to reduce fragmentation
and ensure effective local supervision, similar in many ways to Federal Reserve rules.

In adopting the enhanced prudential standards, however, the Board has acknowledged both the uniqueness of FBOs—as the U.S. operations are a small part of a larger firm—and the diversity of foreign bank operations in the United States.

The Board contemplated from the outset that circumstances may require application of the rule's requirements to be adjusted in light of an individual firm's structure or risk profile.

The Board has exercised this authority in the past, and I want to stress that we will continue to provide flexibility where appropriate to accommodate these differences.

For instance, in implementing enhanced risk management standards, we have focused on outcomes—a strong control environment for foreign bank operations in the United States—while providing some flexibility in how those outcomes are achieved.

We have allowed the global risk committee to serve as the risk committee for the U.S. operations rather than require the creation of a standalone committee.

Further, for foreign banks with large U.S. branches but no IHC, the Board has acknowledged the challenges associated with the location of the risk committee.

The Board has accordingly allowed risk committees at U.S. holding companies as well as managerial committees located in the United States, provided that the global board provided appropriate oversight.

We are committed to continuing this outcomes-focused approach and to refining it where needed.

Further, we recognize that effective stress testing regimes can take many different forms, specifically when interpreting the home-country stress testing requirements of the Dodd-Frank Wall Street Reform and Consumer Protection Act. The Board has acknowledged, for example, that a foreign bank's internal capital adequacy assessment process (ICAAP) may meet the minimum
standards, provided that the firm's ICAAP is on a consolidated basis and reviewed by the home country regulator.

In addition, while we believe that the IHC requirement serves a valuable role in ensuring consistency of regulation across U.S. operations of an FBO, the Board has reserved authority to approve multiple IHCs if circumstances warrant based on the FBO's activities, scope of operations, structure, home country regulatory framework, or similar considerations.

For example, the Board's enhanced prudential standards rule contemplates allowing multiple IHCs in cases where home country legal requirements inhibit the combination of certain bank and nonbank operations.

In practice, and in several instances, the Board has permitted a foreign bank to maintain certain U.S. subsidiaries outside of its IHC, so long as the foreign bank did not have practical control over that subsidiary.4 In addition, the Board recently approved an application by a foreign bank for a second IHC.

Part of our rationale for approving the dual IHC structure was the enhancement of recovery and resolution options of the global firm. In granting the exception, the Board applied enhanced prudential standards to the two IHCs in the same manner that would apply to a single IHC, to maintain a level playing field and align incentives for the safe and sound operation of both IHCs.

This approach allows us more flexibility in addressing firm-specific structure needs, while maintaining the goals of the enhanced prudential standards more generally. We will continue to consider future applications based on the merits of the case.

Finally, to the extent that foreign banks have decided to reduce the scope of their U.S. operations to reduce the application of some of the enhanced prudential standards, the Board has accommodated requests for extended transition periods, so as to avoid unnecessary investments in infrastructure that ultimately would not be required by regulation.

We are committed to tailoring our regulatory and supervisory regimes to align with the risk posed by financial institutions to the U.S. financial system. We are also continuing to evaluate whether our rules are sensitive to changes in the risk profile of banking organizations. We want our rules both to increase in stringency as firms' risks grow and, just as important, to decrease in stringency when firms have actively reduced their risk profiles.
The Volcker Rule

Let me turn now to the Volcker rule. Not to put too fine a point on it, but I believe the regulation implementing the Volcker rule is an example of a complex regulation that is not working well.

The fundamental premise of the Volcker rule is simple: banks with access to the federal safety net—Federal Deposit Insurance Corporation insurance and the Federal Reserve discount window—should not engage in risky, speculative trading for their own account.

Whatever one's view of this basic premise, it is the law of the land. Taking that premise as a given, we have to ask how to improve the framework of the implementing regulation to make it more workable and less burdensome in practice from both a compliance and supervisory perspective.

I think we all can agree that the implementing regulation is exceedingly complex. As one example of specifics, among many, the statute and implementing regulation's approach to defining "market making-related activities" rests on a number of complex requirements that are difficult or impossible to verify objectively in real time.

As a result, banks spend far too much time and energy contemplating whether particular transactions or positions are consistent with the Volcker rule.

Some of you may quite sensibly be asking, "If the deficiencies of the regulation are so apparent, how did we get here?" Despite the best of intentions in crafting the regulations, no one seems to be happy with the complex rule we wound up with.

This has a very positive consequence: I have heard nothing but support from all of my regulatory colleagues for the proposition that the regulation is overly complex and would benefit from streamlining and simplifying to improve its workability in practice.

We are actively working with our fellow regulators in seeking ways to further tailor and to reduce burden, particularly for firms that do not have large trading operations and do not engage in the sorts of activities that may give rise to proprietary trading. We also appreciate the broad extraterritorial impact of the rule in its current form for foreign banks' operations outside of the United States.
To that end, we have, with the full cooperation of all five Volcker regulatory agencies, picked back up the process that was begun last fall to engage in a rulemaking process subject to the Administrative Procedures Act and develop a proposal for public comment that would make material changes to the Volcker rule regulations.

In that process we will take account of our own experience with the regulations since implementation, and we also want to take account of the views of market participants and other interested parties with views on the Volcker rule, including what is working and what is not. We expect this process will proceed with dispatch.

We must also work within the confines of the statute. For example, a number of my current and former Federal Reserve Board colleagues have expressed support for Congress providing an exemption from the Volcker rule for community banks, which is something I also support.

Short of a statutory exemption, we can only do our best to mitigate burden on community banks that generally do not engage in the types of activities the Volcker rule was intended to cover.

Statutory changes likely would make our work of streamlining more straightforward and complete, but we have a fair bit that we can accomplish even absent such changes.

What are some of the improvements that we are thinking about that would be possible within the regulation itself? As an initial matter, it should be clearer and more transparent what is subject to the Volcker rule's implementing regulation and what is not.

The definition of key terms like "proprietary trading" and "covered fund" should be as simple and clear as possible. It should not be a guessing game or require hours of legal analysis of complex banking and securities regulations to determine if a particular entity is a covered fund.

It should not happen—although it has happened—that our supervised firms come to us and ask questions about whether a particular derivative trade is subject to the rule, and we cannot give them our own answer or a consistent answer across the five responsible agencies. Supervisors need to be able to provide clear and transparent guidance on what is covered by the Volcker rule and what is not. This would benefit not only the firms, but the supervisors at the agencies as well.
Again, a good example is the exemption for market making-related activities, which is one of the key exemptions from the prohibition on proprietary trading.

The rule contains a gaggle of complex regulatory requirements, but the statute contains merely one—that the market making-related activities are designed not to exceed the reasonably expected near-term demands of clients, customers, or counterparties, otherwise known as RENT'D.

We are considering different ways to use a clearer test for RENT'D. We want banks to be able to engage in market making and provide liquidity to financial markets with less fasting and prayer about their compliance with the Volcker rule.

As I noted earlier, we also understand that the Volcker rule has had an extraterritorial impact on FBOs. With respect to foreign banks, there are at least a few places where we would like to revisit the application of the final rule based on concerns raised by market participants and others over the past four years of implementation.

In particular, there are certain foreign funds—funds that are organized outside the United States by foreign banks in foreign jurisdictions and offered solely to foreign investors—that are subject to the Volcker rule due to Bank Holding Company Act control principles.

Last summer, the banking agencies, in consultation with the Securities and Exchange Commission and the Commodity Futures Trading Commission, issued guidance that effectively stayed enforcement of the Volcker rule to these foreign funds in light of the technical and complex issues they raise. I expect we would continue this period of stay while we continue to consider these important issues.

The statute also contains exemptions for FBOs to allow foreign banks to continue trading and engaging in covered fund activities solely outside the United States.

The regulation again has a complex series of requirements that a foreign bank must meet to make use of these exemptions. We have heard from a number of foreign banks that complying with these requirements is unworkable in practice, and we are considering ways to address this impracticality.
One possibility that has been suggested by market participants is a simple approach that focuses on the risk of the booking location.

Of course, we would have to consider whether this is possible in light of the language of the statute and principles of competitive equity, but the suggestion is illustrative of the possibility of a more workable approach.

As a final but no less important matter, we are considering broad revisions to the Volcker rule compliance regime. **We would like Volcker rule compliance to be similar to compliance in other areas of our supervisory regime.**

As I noted earlier, we appreciate the broad extraterritorial impact of the rule in its current form on foreign banks' operations outside of the United States.

Accordingly, we will be looking for ways to reduce the compliance burden of the Volcker rule for foreign banks with limited U.S. operations and small U.S. trading books.

**Conclusion**

As I have described previously, the Federal Reserve is actively reviewing post-crisis financial reforms in an effort to better understand which reforms are working well and which ones can be improved to **reduce regulatory burden** and improve the efficiency, transparency, and simplicity of the regulatory framework without compromising a safe and sound financial system.

In that effort, we recognize the importance of foreign banks to the U.S. economy and have a strong interest in ensuring our regulations are appropriately tailored to their U.S. footprint and risks to U.S. financial stability.

Our goal is to maintain a regulatory framework that helps to ensure a strong and stable banking system in an efficient manner that **does not result in excessively burdensome costs** to the banking industry or the economy as a whole.

The areas I have discussed today are important components of the exercise of improving our regulations as they apply to FBOs, and are part of a larger overall agenda to critically evaluate and improve our regulations to
promote financial stability while fostering the conditions for solid economic activity.

Some of these exercises will require more effort and time than others, but each one of them is a high priority for us at the Federal Reserve. I look forward to hearing your views as we make progress toward these improvements.
Making globalization work

William C Dudley, President and Chief Executive Officer of the Federal Reserve Bank of New York, at the Central Bank of Brazil, São Paulo.

Thank you, Ilan, and thanks to the Central Bank of Brazil for organizing this event. It is a pleasure to have the opportunity today to talk about the issue of globalization. As always, what I have to say today reflects my own views and not necessarily those of the Federal Open Market Committee or the Federal Reserve System.

Although the debate about the benefits and challenges of globalization is not new, it has recently come into sharper focus. This debate is important to all of us, and I think it is particularly relevant to Brazil given its importance in the global economy.

Globalization means different things to different people. In my remarks today, I will focus on the role of globalization as a force for international economic integration and economic development. I will highlight three themes:

First, the important role that trade plays in promoting higher standards of living globally.

Second, how changes in trade can create challenges for industries and their workers when they lose competitiveness. Insufficient attention has been given to this issue. We must do better in addressing the very large costs that can be imposed on particular communities and households.

Third, the answer to those challenges is not greater protectionism. Instead, we need to provide greater support to displaced workers so they can obtain the skills needed to find new well-paying jobs. We also need to ensure that there are strong global institutions and international cooperation to help manage the effects of globalization. This includes responding to the
challenges stemming from financial globalization—the flow of capital across national borders.

These issues are important to me as a central banker, as they affect the long-term health and productivity of the U.S. economy, the economic opportunities available to our people, and the efficiency and stability of the global financial system.

The debate around globalization, particularly in advanced economies, reflects many factors. Undoubtedly, the global financial crisis and subsequent slow recovery have been significant.

But, just as important have been longer-term trends, such as growing income inequality, the loss of middle-income jobs, and the rise of large emerging market economies such as China and India.

Although the debate about globalization is not new, I believe we are at a particularly important juncture. If support for liberalized trade and an integrated global economy were to suffer a significant setback, the consequence could be slower economic growth and lower living standards around the world.

While considerable effort has gone into liberalizing trade and developing the existing set of trade agreements, that does not mean they cannot be improved upon.

I have no doubt some trade agreements could be enhanced or updated. Some may not adequately address recent changes in the global economy—such as the rise of digital trade—and may need to be refreshed. And, important trade barriers still remain that should be addressed.

In particular, from a U.S. perspective, the access of U.S. firms to some foreign markets and the protection of intellectual property rights are issues that deserve close attention.

But, in addressing these issues, we should take care to preserve the vital benefits of trade to higher standards of living in both advanced and emerging market economies.

Our focus should be on further strengthening an open trade regime, and, as appropriate, amending and improving these agreements.
The Pace of Globalization

To begin, let me briefly describe the pace of globalization as a reminder of what is at stake. Global economic integration has increased dramatically in recent decades.

Trade in goods and services, for example, has grown from nearly 40 percent of global GDP in 1990 to 54 percent in 2016.

Over the same period, the stock of foreign direct investment has increased from roughly 10 percent of global GDP to 36 percent.

Put simply, national economies and financial systems have become more integrated and interdependent.

This rapid growth in trade reflects falling trade barriers, declining transport costs, and improved information and communication technology.

These trends have enabled the development of complex global supply chains that allow companies to manage their production more efficiently.

Emerging market economies now make up a much larger share of global trade, the global economy, and global growth.

As an illustration, emerging market economies have accounted for 70 percent of global economic growth since the crisis—double their share from two decades ago.

This growth has provided much-needed support to world economic activity, as advanced economies have recovered slowly from the crisis.

Rising economic integration is also evident when we examine the trade relationship between Brazil and the United States.

Bilateral trade flows in goods have risen from $17 billion in 1994 to nearly $57 billion in 2016.

The United States is Brazil's second-largest export market, and an important destination for manufactured goods.

In 2016, the stock of U.S. direct investment in Brazil was $64 billion, up from $18 billion in 1994.
Recent initiatives announced by the Brazilian authorities-including a large and transparent infrastructure concession program and greater foreign participation in the oil and gas and aviation industries-underscore the potential for further increases in foreign direct investment.

To read more:
https://www.bis.org/review/r180314a.pdf
Brief thoughts on the financial regulatory system and cybersecurity

Randal K Quarles, Vice Chairman for Supervision of the Board of Governors of the Federal Reserve System, at the Financial Services Roundtable 2018 Spring Conference, Washington DC.

Thank you very much for having me here at the Financial Services Roundtable's spring meeting. I am pleased to speak with you all about our financial regulatory system: both the broad principles that have been directing my approach to evaluating the regulatory system, as well as cybersecurity, which is a topic of great import to financial system participants and their regulators.

Efficiency, Transparency, and Simplicity of Regulation

As I have said before, we have an opportunity to improve the efficiency, transparency, and simplicity of regulation. We have spent the past decade building out and standing up the post-crisis regulatory regime, and as a result we have made critical gains. The financial system is undoubtedly stronger and safer. We have robust capital and liquidity levels, an effective stress testing regime, and improved resolvability of our largest firms.

But at the same time, it is our responsibility to ensure that those rules are effective. And if we identify rules that are not working as intended, we should make the necessary changes. With the benefit of hindsight and with the bulk of our work behind us, now is a natural and expected time to evaluate the effectiveness of that regime.

Our efforts toward implementing those principles are underway. Federal Reserve Board staff members continue the review that I have previously outlined. The goal is to consider the effect of past regulatory initiatives on the resiliency of our financial system, on credit availability and economic growth, and more broadly, their costs and benefits. I am confident that that
review will reveal some clear ways that we can improve the core post-crisis reforms.

**Cybersecurity**

Let me now turn from regulation to supervision, and more specifically, to the topic of cybersecurity, which continues to be a high priority for the Federal Reserve.

The Federal Reserve is committed to strategies that will result in measureable enhancements to the cyber resiliency of the financial sector.

Given the dynamic and highly sophisticated nature of cyber risks, collaboration between the public sector and private sector toward identifying and managing these risks is imperative.

While we know that successful cyber attacks are often connected to poor basic information technology hygiene, and firms must continue to devote resources to these basics, we also know that attackers always work to be a step ahead, and we need to prepare for cyber events.

Many of you provide services that are critical to maintaining the functionality of the financial system. Those critical services should be highly resilient. But at the same time, some of the solutions in place to improve the resiliency of those critical services may actually contribute to a cyber event.

One example would be the replication of bad data across data centers. As the Federal Reserve thinks about its financial stability mandate, this concern will be a particular focus. Solutions will not come easily, but I am confident that with strong public and private efforts, solutions will emerge.

The Federal Reserve also focuses on the sharing of threat information and collaborates with a number of partners toward protective mechanisms. We work with other domestic agencies as well as international authorities, and we have partnerships between the public and private sectors to introduce and participate in programs that combat the increasingly frequent and sophisticated cyber threats.

Specifically, we collaborate with government and industry partners to plan and execute cybersecurity tabletop exercises focused on identifying areas where sector resilience and information sharing can be enhanced. We also participate in community and industry outreach forums and actively share
threat intelligence with sector partners including the Financial Services Information Sharing and Analysis Center (FS-ISAC). And we encourage financial institutions to work collectively through arrangements such as FS-ISAC so that threat information can be shared promptly and effectively.

Collaboration among many stakeholders on cybersecurity is critical to progress. The Federal Reserve has been working with, and will continue to work with, other financial regulatory agencies on harmonizing cyber risk-management standards and regulatory expectations across the financial services sector.

Specifically, we are focused on aligning our expectations with existing best practices, such as the National Institute of Standards and Technology’s Cybersecurity Framework, and identifying opportunities to further coordinate cyber risk supervisory activities for firms subject to the authority of multiple regulators.

We support industry efforts to improve harmonization across the sector, which are complementary to achieving our regulatory safety and soundness goals.

**Conclusion**

The Federal Reserve continues to work toward improving both post-crisis regulation and our approach to cybersecurity.

I hope that my intention to lay out the broad principles guiding us as we move forward was helpful. And while many of the areas will require additional work and may not have fast results, the Federal Reserve is committed to getting it right, and I look forward to those efforts.
Increasing Product Complexity: What’s at Stake?

Commissioner Kara M. Stein, remarks at SEC Speaks

Good morning. Thank you, Bill [Hinman] for that kind introduction.

As always, it is a pleasure to be with you today at SEC Speaks.

Before I continue, I will remind you that the views I express here today are my own and may not necessarily reflect those of my fellow Commissioners, or of the staff of the Commission.

It’s my understanding that this is the 47th year of SEC Speaks. Much has changed in our capital markets since 1972. Computers now allow investors to access a myriad of investment options from common equity to complex financial instruments within minutes.

Both large and small investors have more investment options at their fingertips—and I mean that literally—than ever before. Computers also allow financial products to be developed and sold more quickly than ever before. This high rate of financial innovation and engineering can be beneficial, but it also can present challenges.

I still remember the ashen faces of the Secretary of the Treasury and the Chair of the Federal Reserve when they came to the Senate Banking Committee seeking authorization for a massive federal government intervention during the financial crisis. Financial engineering of complex institutional investment products (such as credit default swaps and collateralized debt obligations) were at the heart of the financial crisis.

Now, over a decade later, we live in the ‘era of the possible.’ Advances in financial innovation and engineering have enabled the development of new and even more complex financial products. These advances have also allowed the rapid proliferation of these products into the hands of retail investors.
We know we can build products that take advantage of our technological and engineering capabilities. But the question should not be: “Can we develop and sell to investors a product that does XYZ?” The question ought to be “Should we develop or sell to investors a product that does XYZ?”

Allow me for a moment, to take you back in time more than 100 million years—to the Jurassic and Cretaceous periods—when dinosaurs roamed the earth. You can imagine that these remarkable forms of life looked spectacular from a distance, but up close they were probably quite frightening. Steven Spielberg’s movie, Jurassic Park, paints the picture well.

To the park guests, the prehistoric animals were jaw-droppingly majestic, at least from a distance. Up close, however, some of the dinosaurs were unpredictable, if not outright scary. The scientists that created them did not fully understand their capabilities, the unintended effects, or the collateral damage that would inevitably ensue.

The scientists failed to control the park because of what boiled down to a misunderstanding of their highly engineered breeding process. As Dr. Alan Grant noted in the movie, “life found a way.”

By referencing Jurassic Park, I am not suggesting that every complex product is equivalent to a tyrannosaurus rex or velociraptor—that is, something scary, dangerous, and unpredictable.

All investments have at least some risk. And I recognize that there is a sliding scale of complexity.

But what I would like to do is ask whether certain products are appropriate for all investors? How are these products being sold, particularly to retail customers? Even if the disclosure is perfectly clear, does it appropriately inform investor decision-making? If the Jurassic Park guests really understood what could go wrong, do you think they would go on the tour?

Although strategies involving derivatives may date back to at least the 6th century B.C., when the Greek philosopher Thales bought options on olive presses, they have gotten much more esoteric and complex since then.

Products, strategies, and structures using derivatives can range in complexity now, from covered call strategies on the “simpler side” to the far more exotic.
Things like straddles, strangles, iron condors, iron butterflies, twin-win notes, worst of notes, and buffered super track notes come to mind. It seems like the more odd the name, the more complex the product.

To read more: https://www.sec.gov/news/speech/stein-sec-speaks-increasing-product-complexity
Artificial intelligence (AI) in finance - six warnings from a central banker

Prof Joachim Wuermeling, Member of the Executive Board of the Deutsche Bundesbank, at the 2nd Annual FinTech Conference, Brussels.

1 Don't miss out on the opportunities of AI in finance -

AI in finance could impact on the functioning of our financial system in a profound way. Some suggest that AI is enhancing the power of the human brain in the same way that electricity enhanced the power of the body 150 years ago. Hence, it could become a big thing in finance.

Artificial intelligence and big data are currently the strongest and most vivid innovation factors in the financial sector. Using AI in finance may trigger dramatic improvements in many businesses. AI elevates the role of data as a key commodity. Used wisely, big data make outcomes more reliable and may improve financial mediation. Process chains can be organised in new ways. "The scope and nature of banks' risks and activities are rapidly changing," as a recent Basel Committee analysis puts it.

This evolution towards increased use of non-human intelligence is not something that has just occurred in the last few years. The first invention of neural networks, a central pillar of most AI systems, dates back to the year 1943.

Until a few years ago, the main users of big data and AI in the area of finance were certain hedge funds and high-frequency trading firms. In recent times, the application of AI in finance has begun to spread widely, via "normal" banks, FinTechs and other financial service providers, to the general public.
Since 2011, HFT has accounted for about 45-50% of all trading in US equities. The figures for the main European indices are in the same region (with about 40% for German DAX futures).

Taken together with all other "normal" algorithmic trading activities, we currently estimate the amount of algorithmic trading to be in the realm of 80-90% of the entire trading volume for equities (and somewhat less but still very high in other market segments).

A single normal trading day generates about 3-6 million data points about prices, order deletions and modifications in DAX futures alone. No human can analyse these amounts of data simply by looking at them in an Excel spreadsheet. More sophisticated and sometimes also AI-driven techniques are necessary to do the job.

AI profoundly changes the functioning of our financial system in at least three areas: products, processes and analysis. This is true for both front office functions (e.g., customer business, trading) and back office functions (e.g., executing trades, risk management, market research). Special-purpose AI can solve specific problems, e.g., in customer engagement, financial management or cybersecurity.

Applications focused on market operations cover various core areas, e.g., trading, portfolio composition, backtesting and validation of models, market impact analysis, modelling trading of large positions and stress testing. Dynamic portfolio adjustment, depending on the macro environment, may be strengthened by AI.

With the help of AI, various human shortcomings in dealing with finance can be mitigated. As behavioural finance has taught us, biases, inertia and ignorance lead to the malfunctioning of markets. AI allows humans to reach out beyond their intellectual limits or simply avoid mistakes.

2 - but beware of the risks

But opportunities are always accompanied by risks. As regards the financial system, if too much trust is put in "intelligent" systems, the stability of financial markets may be at stake. The workings of AI can be a mystery; it can trigger loss of control, make fatal errors, and have a procyclical effect due to its mechanistic functions.

Pattern recognition has its limits. This can be dangerous particularly in crisis scenarios. An autopilot would never have been able to land a jet on
the Hudson River. Nor can algorithms stabilise in periods of financial stress.

Looking at the recent turbulence in equities and the market for VIX-related financial products, it can be concluded that the events of 5 February share many similarities with a "flash crash".

Unfortunately, as with the original flash crash of May 2010, we have only limited knowledge about the direct drivers that triggered the event. It can be assumed that algorithmic market participants were quite active during the relevant period.

But as to which strategies were applied and to what effect, we have no knowledge so far. The rise in volatility in the S&P 500 then nearly instantly affected the VIX industry, making it not the cause but more the first victim of this market event, with losses up to 95 % on assets. We do not expect this phenomenon to disappear in the future. On the contrary, more of these flash events are to come.

AI is still in its infancy. Continuous processes for the entire AI lifecycle still have to be defined and scaled for business needs. That means that AI must be embedded in the process of acquiring and organising data, modelling, analysis and delivering analytics.

The skills gap, particularly with regard to data science and machine learning expertise, is the foremost challenge. At this stage, non-human intelligence is far from replacing the human brain in any respect. Computers are like school pupils dividing numbers mechanically without having understood what they were doing.

3 Consumers should take care: they remain the risk-takers

What makes this development so significant is the fact that it is not just occurring at the level of systemic institutions, markets and stock exchanges. With robo advisers, for example, AI can directly influence and control the daily financial decisions of customers and ultimately their personal wellbeing. Society has barely begun to understand the economic, ethical and social implications of AI.

While client interaction is made more convenient by mobile banking, chatbots or virtual customer assistants, banks can find out more about customer habits and provide them with tailor-made financing.
Consumers may be rated by AI when applying for a mortgage. Pooling data points from internal transactions, social networks and other sources provides a more meaningful picture of banks' borrowers. But denials may be hard to understand. It may become even harder to challenge a decision made by algorithms.

The proper functioning of the applications is not a given. Simple flaws, cyberattacks and criminal behaviour render the systems extremely vulnerable. Consumers should be cautious. They need to be protected. Laws may have to be modified to cover new threats. Responsibility and liability in the case of malfunctioning machines have to be clarified.

4 FinTechs should not ignore the legitimate concerns of society and supervisors

Agile tech companies are driven by an admirable energy and inspiration. By nature, they take risks. They create an idea, build a prototype and try it out immediately in the real world. Regulation, supervision, obligations and requirements must make them extremely nervous.

But the wellbeing of society depends on rules. The public demands cybersecurity, data privacy, consumer protection and financial stability. FinTechs should not brush aside the concerns of their stakeholders. Business can only flourish if it is broadly accepted by citizens.

FinTechs usually pick up specific elements of the work chain of finance or create new features. Using technology, they modularise and customise products as a third party or standalone provider.

FinTechs are part of the finance sector but are not necessarily supervised. As long as they carry out tasks for supervised entities, these institutions are responsible for the behaviour of the FinTech.

5 AI needs new forms of supervision

"Artificial intelligence" may sound glamorous from a technological perspective, but in banking supervision, the well-established principle of "same business, same risk, same rules" has so far proved to be a sound standard for innovations. Whether they employ AI themselves or outsource it to FinTechs, from the supervisors' point of view responsibility remains entirely with the bank.
For German supervisors, IT governance and information security nowadays are equally as important as capital and liquidity requirements.

All financial institutions should address the risks posed by new technologies. Banks have to implement effective control environments needed to properly support key innovations.

This includes the requirement to have appropriate processes for due diligence, risk assessment and ongoing monitoring of any operations outsourced to a third party.

The European MiFID II includes the requirement that firms applying algorithmic models based on AI and machine learning should have a robust development process in place.

Firms need to ensure that potential risks are considered at every stage of the process.

Regulators increasingly have to apply AI-supported analytical methods themselves to recognise vulnerability patterns, scan lengthy reports or analyse incoming data.

In any case, we must strike a balance between financial stability and avoiding barriers for potential new entrants, products and business models.

Alongside technological progress, regulators have to constantly reassess the current legal framework, supervisory models and resources.

6 Central banks should embrace AI

Central banks have access to huge amounts of very valuable data stemming from market operations, supervision, payments and statistics.

They are well positioned to tap the benefits of AI so they can enhance their ability to fulfil their mandate for price stability and the stability of the financial system.

Machine learning is already being used at the Bundesbank in different narrow segments.
The experiences of all users have been good without exception. While monitoring the technical progress, we are currently discovering further use cases and defining our AI foundation, strategy, organisation and processes. Here is a list of examples, which is by no means exhaustive:

**In risk management,** *neural networks* assess and evaluate the financial soundness of the markets. Market research is supported by adopting web mining techniques and machine learning in content analysis, topic modelling and clustering of relevant articles.

**In statistics,** machine learning enables new methods for data quality management, eg in the context of securities holdings or the classification of company data.

Furthermore, the informational content of seasonality tests is assessed by a random forest machine learning technique.

**For our IT user help desk,** the handling of routine requests via automated chatbot responses could be a useful support measure.

We use social media data to detect trends, turning points or sentiments. Machine learning methods can be applied for variable selection purposes in econometric models.

**ANNEX: Use case - monitoring of real estate markets**

An interesting data source is internet platforms. For example, some rental and housing platforms have the potential to improve the analysis and monitoring of real estate markets via the provision of information such as list prices and structural and locational characteristics of the property market at a disaggregated level.

This is mainly based on the assumption that these data contain information on the expectations and interests of economic agents with respect to future decisions.

In such contexts, a wide range of topics or "search strings" are often potentially relevant. This can result in many different, highly correlated time series.

Furthermore, the "textual analysis" method is increasingly applied in research, as large amounts of "unstructured" information on businesses and the economy are available electronically on the internet.
In order to operationalise textual data for econometric analysis, machine learning algorithms can be helpful.

Learning methods can be applied to classify textual documents into different categories which can then be used to draw statistical inferences.
DHS Cyber Incident Response Teams Act of 2018

A BILL To authorize cyber incident response teams at the Department of Homeland Security, and for other purposes.

The Center shall maintain cyber hunt and incident response teams for the purpose of providing, as appropriate and upon request, assistance, including the following:

(A) Assistance to asset owners and operators in restoring services following a cyber incident.

(B) The identification of cybersecurity risk and unauthorized cyber activity.

(C) Mitigation strategies to prevent, deter, and protect against cybersecurity risks.

(D) Recommendations to asset owners and operators for improving overall network and control systems security to lower cybersecurity risks, and other recommendations, as appropriate.

(E) Such other capabilities as the Under Secretary appointed under section 103(a)(1)(H) determines appropriate.

CYBERSECURITY SPECIALISTS. — The Secretary may include cybersecurity specialists from the private sector on cyber hunt and incident response teams.

Note: House lawmakers have passed legislation that would codify into law the cyber incident response teams that help protect federal networks and critical infrastructure from cyberattacks.

The bill is sponsored by House Homeland Security Committee Chairman Michael McCaul (R-Texas).
To read more:
http://docs.house.gov/billsthisweek/20180319/HR5074.pdf
Progress Update on Cyber Lexicon

This note, delivered to G20 Finance Ministers and Central Bank Governors for their meeting in March 2018 in Buenos Aires, provides a progress update on the FSB’s work to develop a cyber lexicon.

G20 Finance Ministers and Central Bank Governors, in their March 2017 Baden-Baden Communiqué, noted that the malicious use of Information and Communication Technologies (ICT) could disrupt financial services crucial to both national and international financial systems, undermine security and confidence and endanger financial stability.

<table>
<thead>
<tr>
<th>Date</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feb.-15 May 2018</td>
<td>Lexicon (including exemplary documents) development by working group.</td>
</tr>
<tr>
<td>12-13 March 2018</td>
<td>In-person meeting of working group (Basel).</td>
</tr>
<tr>
<td>March-April 2018</td>
<td>Industry engagement and public outreach.</td>
</tr>
<tr>
<td>15 May 2018</td>
<td>Draft lexicon delivered by working group for internal FSB review.</td>
</tr>
<tr>
<td>15 May-early July 2018</td>
<td>Revision to, and consideration of, lexicon within the FSB, including whether to publish the lexicon and undertake public consultation on it.</td>
</tr>
<tr>
<td>Early July 2018</td>
<td>Public consultation initiated if determined appropriate by FSB Plenary.</td>
</tr>
<tr>
<td>21-22 July 2018</td>
<td>Progress update to FM&amp;CBG meeting, including potential submission of the lexicon/exemplary documents and/or consultation document.</td>
</tr>
<tr>
<td>Late Nov. 2018</td>
<td>Final lexicon delivered to G20 Summit.</td>
</tr>
</tbody>
</table>

With the aim of enhancing cross-border cooperation, the FSB was asked, as a first step, to perform a stocktake of existing relevant released regulations and supervisory practices in G20 jurisdictions, as well as of existing international guidance, including to identify effective practices.

The FSB published this stocktake on cybersecurity regulations, guidance and supervisory practices on 13 October 2017.
In October 2017, G20 Finance Ministers and Central Bank Governors at their Washington DC meeting welcomed the FSB stocktake report, asked the FSB to continue its work to protect financial stability against the malicious use of ICT and noted that this work could be supported by the creation of a common lexicon of terms that are important in the work being pursued.

This note provides a progress update on the FSB’s lexicon work, including a description of the objective of the work, the process for creating the lexicon and a description of next steps with an indicative timeline in order to deliver the lexicon to the November 2018 Buenos Aires G20 Summit.

To read more: 
March 2018 Puzzle Periodical - a, b, c - Variable Alphabet Equation

Can you solve this alphabetical equation?

Puzzle created by Wendell W., NSA Mathematician

Consider the following equations:

\[ a^2 \times b \times c^2 \times g = 5,100 \]
\[ a \times b^2 \times e \times f^2 = 33,462 \]
\[ a \times c^2 \times d^2 = 17,150 \]
\[ a^3 \times b^3 \times c \times d \times e^2 = 914,760 \]

Find positive integers a, b, c, d, e, f, and g, all greater than 1, that satisfy all the equations.

The solution?
Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

Ronald S. Ross, Patrick Viscuso, Gary Guissanie, Kelley L. Dempsey, Mark Riddle

The protection of Controlled Unclassified Information (CUI) while residing in nonfederal information systems and organizations is of paramount importance to federal agencies and can directly impact the ability of the federal government to successfully carry out its designated missions and business operations.

This publication provides federal agencies with recommended requirements for protecting the confidentiality of CUI:

(i) when the CUI is resident in nonfederal information systems and organizations;

(ii) when the information systems where the CUI resides are not used or operated by contractors of federal agencies or other organizations on behalf of those agencies; and

(iii) where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or governmentwide policy for the CUI category or subcategory listed in the CUI Registry.

The requirements apply to all components of nonfederal information systems and organizations that process, store, or transmit CUI, or provide security protection for such components.

To read more: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf
Security Recommendations for Hypervisor Deployment on Servers

Ramaswamy Chandramouli, Computer Security Division
Information Technology Laboratory

The Hypervisor is a collection of software modules that provides virtualization of hardware resources (such as CPU/GPU, Memory, Network and Storage) and thus enables multiple computing stacks (basically made of an OS and Application programs) called Virtual Machines (VMs) to be run on a single physical host.

In addition, it may have the functionality to define a network within the single physical host (called virtual network) to enable communication among the VMs resident on that host as well as with physical and virtual machines outside the host.

With all this functionality, the hypervisor has the responsibility to mediate access to physical resources, provide run time isolation among resident VMs and enable a virtual network that provides security-preserving communication flow among the VMs and between the VMs and the external network.

The architecture of a hypervisor can be classified in different ways. The security recommendations in this document relate to ensuring the secure execution of baseline functions of the hypervisor and are therefore agnostic to the hypervisor architecture.

Further, the recommendations are in the context of a hypervisor deployed for server virtualization and not for other use cases such as embedded systems and desktops.

To read more:
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-125A.pdf
Former employee jailed for intentionally damaging computer network

A disgruntled former Canadian Pacific Railway (CPR) employee was sentenced last week to a year in prison for intentionally causing damage to CPR’s computer network.

It is unclear whether train services were affected, but the incident is reported to have cost the organisation approximately $30,000.

In December 2015, the employee resigned from CPR after being informed that he would be fired for insubordinate behaviour. However, before returning his laptop and remote access authentication token to the organisation, the disgruntled individual accessed CPR’s core computer network switches, through which critical data flows.

He strategically deleted files, removed admin accounts or changed their passwords, returning the laptop after wiping its hard drive of any evidence of his actions.

This meant IT staff were unable to access the switches, forcing them to reboot the network, causing a system outage. Forensic investigations of systems allowed the damage to be traced back to the individual concerned.

This case is a good example of how disgruntled, former employees can pose a cyber threat to organisations.

Such insider threats are not unique to the rail sector. Public and private organisations in every sector need to be vigilant to such threats.

It highlights the importance of ensuring IT privileges and account access is suspended when a staff member’s employment is due to be terminated, preventing malicious cyber activity from being conducted.
Disclaimer

The Association tries to enhance public access to information about risk and compliance management.

Our goal is to keep this information timely and accurate. If errors are brought to our attention, we will try to correct them.

This information:

- is of a general nature only and is not intended to address the specific circumstances of any particular individual or entity;
- should not be relied on in the particular context of enforcement or similar regulatory action;
- is not necessarily comprehensive, complete, or up to date;
- is sometimes linked to external sites over which the Association has no control and for which the Association assumes no responsibility;
- is not professional or legal advice (if you need specific advice, you should always consult a suitably qualified professional);
- is in no way constitutive of an interpretative document;
- does not prejudge the position that the relevant authorities might decide to take on the same matters if developments, including Court rulings, were to lead it to revise some of the views expressed here;
- does not prejudge the interpretation that the Courts might place on the matters at issue.

Please note that it cannot be guaranteed that these information and documents exactly reproduce officially adopted texts.

It is our goal to minimize disruption caused by technical errors. However some data or information may have been created or structured in files or formats that are not error-free and we cannot guarantee that our service will not be interrupted or otherwise affected by such problems.

The Association accepts no responsibility with regard to such problems incurred as a result of using this site or any linked external sites.
Sarbanes Oxley Compliance Professionals Association (SOXCPA)

1. **Membership** - Become a standard, premium or lifetime member.

   You may visit:  
   www.sarbanes-oxley-association.com/How_to_become_member.htm

2. **Monthly Updates** - Subscribe to receive (at no cost) Sarbanes-Oxley related alerts, opportunities, updates and our monthly newsletter:

   http://forms.aweber.com/form/30/1922348130.htm


   You must follow the steps described at:  
   www.sarbanes-oxley-association.com/Distance_Learning_and_Certification.htm

   For instructor-led training, you may contact us. We can tailor all programs to your needs.

4. **Authorized Certified Trainer, Certified Sarbanes Oxley Expert Trainer Program (SOXCPA-ACT / CSOET)** - Become an ACT. This is an additional advantage on your resume, serving as a third-party endorsement to your knowledge and experience.

   Certificates are important when being considered for a promotion or other career opportunities. You give the necessary assurance that you have the knowledge and skills to accept more responsibility.

   To learn more:  
   www.sarbanes-oxley-association.com/SOXCPA_Authorized_Certified_Trainer.html