COMMISSION ON ENHANCING NATIONAL CYBERSECURITY

Meeting of the Commission on Enhancing National Cybersecurity

PANELIST STATEMENTS

New York University – School of Law

40 Washington Square South, New York, NY

May 16, 2016

Table of Contents

Panelist Statements

Phil Venables

Good Morning Chairman Donilon, Vice-Chairman Palmisano and Distinguished Members of the Commission, I'm Phil Venables and while here today as a Managing Director at Goldman Sachs, the views I'm representing are my own based on over 20 years of working in the cyber- security industry.

I would like to thank you for the opportunity to address the Commission today.

It is my view that the management of technology risks, in particular cyber-security, has become critical to our increasingly digitized and connected society. It is imperative for national and international security and will continue to be ever more a foundational requirement for security in other domains.

It is important to emphasize that cyber-security is not the only technology or information risk. There are many risks in digital business or society, for example, systems and software reliability, predictability, resilience, and capacity. However, cyber-security is and should continue to be our main concern given the potential impact of failure, the increasing number and sophistication of threats and its supporting and supported role in managing all these risks.

I would like to put forth 5 recommendations to create and sustain national cyber-security risk mitigation:

The first would be to integrate cyber security into the fabric of organizations:

- Risk must be integrated. It's imperative to ensure that cyber-security risk management is embedded into the main risk management and strategic processes of organizations from the Board, to risk committees, to the wider processes of strategy formulation, product development, investments and acquisitions; both within the organization and across its extended supply chain
- Technology must also be integrated. My experience and observation is that good technology management / hygiene promotes solid cyber-security and that for a controlled technology environment to be also agile and cost-effective it has to have risk mitigation be designed in – ambient controls
- Resilience and recovery must also be integrated. However, no matter how well risks are managed something may still go wrong, a misidentified risk, a break of a control, a new adversarial technique, an unforeseen circumstance or an insider threat; so it's important to build the muscle memory of effective detection, containment / response, and recovery through continuous scenario planning, drills and exercises.

The second would be that public / private partnerships must be sustained and improved.

- There has been immense progress in establishing and coordinating national cyber- security measures from the sharing of threat intelligence to the coordination of capabilities needed to respond to particular events and incidents
- However, we should recognize that threat sharing alone is not enough and it is important to share, in a suitably anonymized and protected way, actual incident data and the vulnerabilities or other factors that led to those incidents so that everyone can benefit from that experience

- Information sharing with the private sector requires in some cases the handling of classified material necessitating the holding of security clearances, but rather than solely increase the number of cleared individuals within the private sector the bias should be to declassify / desensitize information as much as possible so we can utilize it more readily
- We also need improvements in international as well as cross-sector coordination. While cyber-security is a clear imperative for our national security we should remember that many of our businesses are internationally connected and exposed to multiple threats in the physical and digital world that extends beyond our national borders.

The third recommendation would be to harmonize rules and guidance

- There is a multiplicity of frameworks, standards and guidelines for cyber-security, many of which are effective and practical, but for organizations it can be difficult to decide which to utilize
- We would recommend that we continue to emphasize the NIST Cyber Security Framework and in particular the development of associated profiles subject to appropriate certification schemes
- We should further raise awareness of the need for organizations to more firmly adopt a strong set of baseline of controls, for example the Center for Internet Security's Controls for Effective Cyber-Defense

Fourth, we must improve capabilities amongst people, process and technology

- There needs to be continued emphasis on the embedding of controls into all available technology products and services, as opposed to after the fact embedding of control late in the design or development cycle which is often ineffective and uneconomic : we need secure products not just security products
- Similarly, we should recognize that cyber-security risk mitigation is not solely the responsibility of designated cyber-security professionals but is, perhaps more importantly, in the domain of leadership, risk managers and engineers at all levels of organizations. I would support a national program to embed cyber-security training into all academic and professional training and qualifications: we need more security-minded people not just more security people
- I fully endorse all efforts to deal with the shortage of trained cyber-security professionals to help manage these risks, but I also note that there is a wider issue that is the productivity of the cyber-security professionals we already have and more needs to be done by Government and industry to improve tools, processes and the orchestration of defense across multiple platforms to get the most out of the people we have

And the final recommendation would be to design for defensibility

- Our goal should be to design our technology and information processing environments to be more inherently defendable: able to deflect, be adaptive in response to, and to continue operation and prove resilient in the face of attacks
- Such defensibility includes not only currently available technology, but much active research and development that needs to be brought to market faster with Government help or other incentives

- Additionally much work is needed to assist organizations in transitioning from complex legacy environments to simpler and more defendable environments that are more comprehensively enclaved and less susceptible to one successful attack causing wider compromise; and, finally, it is worth remembering that despite the advantages of mass and constant interconnectedness there may be some things so critical that they should remain isolated under different and higher assurance of control

Thank you again Mr. Chairman for allowing me to provide this input into this important process and I remain committed to assisting further as needed. I'm happy to answer any questions you or the other members may have at this time.

Greg Rattray

JPMC sees providing cybersecurity as a fundamental concern for the firm and its clients. The firm's overall strategic priorities include strengthening cybersecurity. In 2016, we plan to spend over $600 million and we have over 2000 people working on cybersecurity.

We work closely with our industry partners in organizations like the Financial Sector Coordinating Council and the Financial Services ISAC to enhance our defenses and collaborate in strengthening the financial system as a whole. We are also taking a leadership role across industry to examine detection, response, and recovery actions related to significant cyber induced disruptions to sector payment platforms.

We work closely with government partners in Treasury, DHS and FBI among others and participate fully in full range of public – private partnerships.

We fully participate in events like the Hamilton cyber exercise series co-sponsored by Treasury and the private sector to improve our ability to jointly respond to cyber events. We seek to deepen these activities going forward.

We find that while the government has highlighted cybersecurity as a major challenge and established broad programs to engage in partnership with the private sector, these programs do not meet the needs of firm's like ours in terms of enhancing our cyber defense.

We seek to build on the strong partnership we have developed and hope for a prioritized focus on dedicated government support capabilities to large firms like ours that have more resources and have already implemented robust cyber defense programs. We understand the strategic importance of cyber security and are fully invested in continuously improving our cyber defense posture.

Our top priorities are:

1. Information Sharing – producing predictive, actionable cyber threat intelligence driven in part from our requirements and including access to dedicated government classified reporting and services on par with that offered to the Defense Industrial Base through organizations such as the Defense Cyber Crime Center and other sectors such as through the Industrial Controls Systems Computer Emergency Response Team ICS-CERT
2. Intelligence and Disruptive Operations – national-level efforts to provide intelligence and conduct disruptive operations against organized crime in addition to efforts against potential nation-state adversaries. Criminal attacks against financial services companies and associated utilities can have wider ranging national impacts and must be countered
3. Crisis Response and Contingency Planning – improving crisis response capabilities via increased investments in sector exercise programs, establishing joint crisis response protocols, and conducting joint contingency planning for destructive or large scale attacks. We believe systemically important institutions must receive dedicated support in these efforts.
4. Improved Protection of Core Financial Utilities and Infrastructure – improving cybersecurity and fraud prevention integration with core financial utilities (such as Fedwire)
5. Prioritize Improvement of the Cyber Environment - Drive efforts with Internet infrastructure and ecosystem providers (such as email providers, ICANN and Domain Registrars) to reduce malicious activity and improve the environment for clients and customers.

6. Limiting financial sector stress due to a cyber event – ensuring Government resources and leadership attention are devoted to understanding, and addressing as applicable, potential impacts to public and market confidence with clear liquidity guidelines, settlement and cash distribution procedures, updated regulatory guidance and a communications strategy in cases of systemic cyber attacks on financial sector
7. Efficient access to government resources for assistance during disaster response -- expected to result in more effective response and recovery

For these priorities to be effectively implemented, the US Government should make clear across all departments and agencies that prioritized and enhanced support to systemically important firms is authorized and required to protect our nation's critical infrastructure.

Lee Garvin

Officially stated, my personal definition, strategy and role:

Definition of Risk Management: Risk Management is the process of actively and economically applying resources to identify, assess, communicate and manage the risks facing an organization, in order to minimize the impact of foreseen and unforeseen events

Strategies of Risk Management: The strategies that we utilize to manage our risks include; transference to another party, avoidance, reduction, and accepting some or all of the consequences of the risk. These strategies enable the company to better understand exposures that could potentially cause us to miss our objectives

The Role of Risk Management: The department will strive to align the corporate philosophy and day-to-day decision making. This needs to be done without adding unnecessary bureaucracy or inhibiting the ability of the company to make decisions and move quickly

How I see the practical application…

The above can seem a lot to take in. If find that simply stated, you can sum my risk management philosophy up with 2 words – Asset Protection. We look to protect everything that is owned, managed, operated and the employees that do so for the company. This is my department's daily goal. Anything that comes into the conversation relates to the specific endeavor's circumstances and how we are going to protect the assets.

With each specific circumstance, we need to learn the facts of the endeavor. What is the goal? How are we going to achieve the goal? Who internally and externally is involved?

All of this is usually accomplished through a combination of conversations, research, emails, contract reviews and applying what I like to call "the radical application of common sense".

Once we have identified the risk to the assets then we go about mitigating the risk. We use all of the tools typical to any risk manager (reduction, transfer, acceptance and avoidance). My personal opinion is that there is another more powerful tool at our disposal. Education, we have the ability to educate others in our process. For example, if we can properly educate the project leaders on the risks, they will likely act as an extension of my department. When this occurs, corporately we will have an easier time minimizing our exposures.

Philosophically, "no - we can't do that" should not come out of our department. If it has then we would have failed in our communication and education process. It is the work group's job to make educated decisions we need to let them run the business. It is our job to educate them. When all else is done we evaluate the activities at hand and conduct the cost benefit of insuring it.

The education extends well past the project leaders. It extends to the brokers and insurers who issue the policies. These are business partners that are extending a large amount of coverage for our premiums. I want to make sure that we are well beyond a commodity pricing exchange. My position is that we need to educate our brokers, and insurers, as to what our risks are. Most underwriters really want to create and provide solutions to their clients. It helps them provide value. It is incumbent on us to be open and clear so we can "help them help us". During this process we will be evaluating price and coverage in an effort to close down as many holes as we can, provided it is for the right price. I find for the best results, these external relationships need to be just as much of a partnership as it is with our internal business units.

Finally, another aspect of our department hinges on our ease of use. Our department must be quick and easy to work with. If my department is not easy to interact with, or delivers messages in a combative nature, we will have done more harm for the company than missing a "bad"

contractual provision. We need to be solution orientated. My largest fear is to not know what projects or goals we are engaging in. I'd rather take the time to work with and educate an entire company of "risk managers", than create a situation where contracts are signed, and activities are conducted, without our review, just because we are "too difficult" to work with.

Peter Beshar

Good morning Chairman Donilon, Vice Chairman Palmisano, and members of the Commission. I am Peter Beshar, the Executive Vice President and General Counsel of Marsh & McLennan Companies. I am grateful for the opportunity to participate in this important hearing about enhancing our national cybersecurity.

Marsh & McLennan operates through four market-leading brands — Marsh, Guy Carpenter, Mercer and Oliver Wyman. Our 60,000 employees provide advice to clients across an array of industries in the areas of risk, strategy and human capital. As the leading insurance broker in the world, Marsh has a unique perspective on the cyber insurance market.

I would like to focus my remarks this morning on three core points. First, what role can cyber insurance play in enhancing our nation's cyber resilience? Second, how can big data strategies be utilized to assess and mitigate cyber risk? Third, what specific strategies can be deployed by the business community to mitigate cyber risk against critical infrastructure?

The Need for a Public-Private Partnership

As cyber attacks in both the public and private sectors have shown, neither government nor business can solve this problem alone. Much of the focus in the past two years has been on data breaches involving credit cards at large retailers and social security numbers from health care companies.

As events earlier this year in Ukraine and elsewhere have shown, however, we are now confronting a stark new reality of threats against physical assets - including electric grids, dams, telecommunications networks, transportation systems and civilian nuclear facilities. Ubiquitous connections to the Internet have increased vulnerability in the industrial systems that control these physical assets. As the vast majority of critical infrastructure in this country is owned and operated by the private sector, it is vital that government and industry lock arms in confronting this risk.

We need a mindset that we are all in this together and that we are engaged in a race without a finish line.

Why is Cyber Insurance Important?

Throughout our nation's history, the insurance industry has played an important role in developing strategies to mitigate emerging risks. The underwriting process, by identifying a set of best practices across industries, creates important incentives that drive behavioral change in the marketplace.

A brief historical analogy. In 1730, a disastrous fire swept through the city of Philadelphia. Benjamin Franklin stepped into the fray and made it his mission to devise strategies to mitigate the risk posed by fire. Incredibly, Franklin introduced the first all-volunteer fire brigade and invented both the "Franklin" stove and, of course, the lightning rod.

Franklin then took another critical step that is less widely known. He founded the first insurance company in the colonies - the Philadelphia Contributorship. Anyone wishing to become a "subscriber" for insurance coverage had to embrace a specific set of best practices. An example was having an access point from the attic to the roof to reduce the risk of the roof catching on fire. For the first time, premium rates, rather than being uniform, were set relative to the risk posed by each property.

This combination of technological innovation and a defined set of best practices worked. Unlike other major cities of the era, Philadelphia did not suffer another catastrophic fire after 1730.

Franklin had engaged in a textbook example of what we would today call "enterprise risk management."

So, what role can cyber insurance play to mitigate cyber risk? Broadly stated, there are three core types of cyber insurance.

The most basic coverage provides protection for out-of-pocket expenses that a company incurs directly in the wake of a cyber incident. Most commonly, these expenses include the cost to respond to a data breach, including notifying individuals, setting up call centers and providing credit monitoring. This may also include the cost of restoring data or paying "ransomware" demands that have recently plagued the healthcare industry.

Next, "business interruption" coverage protects a company if its computer network is disrupted for a defined period of time, typically at least 8 hours. With this coverage, a company can recover the actual harm it suffers in the form of lost profits or extra expenses. These first two forms of coverage are called first-party coverage.

The final form of coverage is for liability that could result if a third party, a client for example, is economically damaged as a result of the company's breach. This is called third-party coverage.

Why Does Cyber Insurance Matter?

If all that cyber insurance did was pass the risk of harm from one party to another, that would be helpful as a financial matter, but not significant as a policy matter.

Fortunately, the underwriting process creates a powerful set of economic incentives that drive behavioral change in the marketplace. That is the potential that cyber insurance offers.

First, the act of applying for insurance prompts the policyholder to take a number of constructive actions. Companies typically conduct a benchmarking analysis against an established industry standard, whether the NIST Framework, an ISO standard like 27001 or another proprietary system such as Marsh's Information Security and Privacy Self-Assessment.

The policyholder and oftentimes broker assess the company's cyber protocols. Has the enterprise identified its high value assets? Has it implemented two-factor authentication for remote access by employees and vendors? How robust are its software patch management protocols? Does the company have, and has it tested, its incident response plan?

Naturally, the market will differentiate sharply among applicants depending on how the company approaches the people, processes and technology that affect cybersecurity. That differentiation comes in the form of premium dollars. Pricing pressures drive insureds to adopt best practices.

Once a policy has been placed with an insurer, further incentives are created. The insurer is now motivated to help its policyholders either avoid entirely or, at least mitigate, the risk of a cyber breach. Accordingly, insurance companies provide access to experts and a suite of services that include monitoring for anomalous behavior and rapid response capabilities. These services include technical advice from on-call consultants, vulnerability detection to examine network servers, and assistance developing incident response plans.

Given the barrage of cyber breaches in the headlines, these incentives are driving strong economic forces in the market. According to the Betterley Report, the total amount of annual gross written premium in the cyber market reached $2.75 billion in 2015. Experts have estimated that the market could grow to $10 billion in global premium by 2020.

The number of Marsh clients purchasing stand-alone cyber insurance increased by 27% in 2015 after an increase of more than 30% in 2014. In addition, companies are purchasing higher limits. Coverages, which formerly were in the tens of millions, are now climbing up to $500 million for

companies in particularly vulnerable industries. Indeed, the average limit placed for large communications, media, and technology organizations is approaching $100 million.

Utilizing Big Data Strategies to Mitigate Cyber Risks

The insurance industry is data-driven. For long-standing risks, actuaries rely on decades of claim data to set premium rates and reserves. For emerging risks like cyber, insurers need to develop new approaches and techniques to guide their underwriting practices.

In a recent report entitled "Cyber Resilience in the Fourth Industrial Revolution" that Marsh & McLennan issued together with FireEye and Hewlett-Packard, we identified two core approaches that insurers are utilizing.

The first is the more common "inside-out" approach that involves hiring a forensic investigations firm to conduct an on-site assessment of a company's policies, practices and potential vulnerabilities. Experts conduct "penetration" tests and compromise assessments to probe the resilience of a company's security protocols.

An alternative and emerging strategy is an "outside-in" approach that relies on big data methodologies. Without stepping foot inside of a company's offices, the cyber resilience of a company can be assessed by analyzing hundreds of externally available data points. For example, are employees accessing the Internet using an outdated web browser that is more vulnerable to spyware, malware and viruses? Does the company share web-hosting platforms and cloud storage with other companies? What information can be gleaned about a company's IT operating systems from help wanted postings when a company is looking to fill a position in its IT department? Does any data from the company, including stolen passwords, appear in the "dark web"? How does the company's ranking of employee satisfaction on Glassdoor correlate to the risk that a disaffected insider will compromise its data security? How strong is the motivation of a potential hacker to breach a particular company's network?

None of these data points is dispositive. Utilizing algorithms to analyze hundreds of these data points, however, can yield important insights about the relative vulnerability of an organization in comparison to other firms in particular industries.

So, data is critical.

We urge the Commission to recommend that the government engage the finest minds in the tech community to expand the use of big data strategies. In addition, the vision articulated in the Cybersecurity Act of 2015 to create a real-time information sharing platform of cyber threat indicators needs to be made operational.

The Emerging Threat Against Critical Infrastructure

The escalation in the sophistication and potential severity of cyber threats has been stunning. Data breaches relating to credit cards, social security numbers and personal health records have proven to be only the tip of the iceberg. The emerging, and far more troubling, threat is that posed to our nation's critical infrastructure.

The members of this Commission will be all too familiar with recent attacks on critical infrastructure including the German iron plant and the Bowman dam in New York. The attack on the Ukrainian power grid earlier this year represents a significant escalation in that threat. Lloyd's of London conducted an important review of the potential vulnerability of the power grid in the US and concluded that a significant attack on the northeast grid could cause up to $1 trillion in damages. As a measure of comparison, the tsunami in Japan caused approximately $350 billion in economic damages.

We are growing increasingly concerned about the risk that cyber presents to the operations of large corporations across the US and urge this Commission to make protecting our nation's critical infrastructure a key priority.

Given this threat landscape, we recommend that the Commission improve national cyber resilience by facilitating broader use of the SAFETY Act. Adopted in the wake of the attacks on 9/11, the SAFETY Act has played an important role in encouraging companies to develop innovative anti-terrorism technologies. Under the SAFETY Act, a company submits a specific technology, either a product or service, designed for anti-terrorism purposes to DHS. Upon finding that the product has the potential to be effective, DHS grants SAFETY Act protection which limits the legal damages that may result from a failure of the technology. This process encourages innovation while also shielding an organization from catastrophic liability.

Our country now confronts a growing threat of cyber terrorism. In its current form, the SAFETY Act can help companies manage their cyber risk. Power and water utilities, chemical plants and telecommunications providers can mitigate their exposure by submitting their information security protocols and controls for SAFETY Act approval. The SAFETY Act offers particular promise in the area of new technologies for network monitoring.

At present, application of the Act can only be triggered by a declaration by the Secretary of DHS that an act of terrorism has occurred. As there are political ramifications of any declaration of an act of terrorism as well as policy implications under the Terrorism Risk Insurance Act, this requirement might prove unduly limiting in practice. Moreover, particularly in the realm of cyber terrorism, the issue of attribution can be exceedingly complex. Accordingly, we recommend that the Commission consider mechanisms to broaden the application of the SAFETY Act where there is widespread damage to critical infrastructure.

If necessary, a congressional amendment to the SAFETY Act would expand application, subject to legislatively set thresholds, for cyber attacks that threaten material harm to the US economy or national security.

This type of action would likely foster greater collaboration between government and industry. Those industries that own and operate critical infrastructure would have a financial interest in collaborating with security experts on what controls are expected. In turn, government would have greater visibility into an arena where it relies on voluntary collaboration because regulatory authority is more limited.

Here again, the insurance industry could potentially play a constructive role. The SAFETY Act requires DHS to set the limit of liability for each applicant based on the amount of insurance available and the burden to purchase coverage up to that limit. Modeling and analysis performed within the insurance industry can help guide these determinations.

As a whole, the process could lead to companies implementing stronger controls while establishing greater financial certainty in the face of catastrophic risk. Both serve the ultimate goal of building cyber resilience in the private sector.

Conclusion

The federal government has taken a leading role in cybersecurity. The NIST Cybersecurity Framework in early 2014, the Cybersecurity Act of 2015 and now this Commission point to the Administration's commitment to bolster our country's cyber resilience.

Cyber insurance in particular and the insurance industry in general have the potential, in our judgment, to serve as important contributors to enhancing our cyber resilience.

I look forward to answering any questions you might have.

Randal Milch

My name is Randal S. Milch. I am a Distinguished Fellow at the New York University School of Law Center on Law and Security and its Center for Cybersecurity. At NYU I have devoted considerable time to exploring the potential role of cybersecurity insurance in reducing cyber risk. I also previously served as Executive Vice President, Public Policy and General Counsel of Verizon Communications Inc., where I chaired Verizon's Executive Security Council, the body responsible for information security across all Verizon entities. The views I am honored to provide you today are my own.

I want to commend the Commission for investigating the role of cyber insurance as part of its effort to enhance national cybersecurity. Cyber insurance falls squarely within the Commission's objectives and scope of work as laid out in Executive Order 13718 and reflected in the Commission's Charter. A robust cyber insurance market should both "manage and reduce the economic impacts of cyber risk" and "improve access to the knowledge needed to make informed cyber risk management decisions."

Indeed, a well-functioning insurance market is characterized by precisely these two beneficial characteristics. First, insurance (including re-insurance) spreads losses arising from covered risks. Enabling companies to distribute the cost of business risk through insurance is a long-standing and necessary aspect of modern society. Second, the insurance underwriting process can help mitigate risk. As an insurer underwrites a company's risk, it gathers and evaluates pertinent risk information and can provide feedback to the potential insured to help lower its risk profile. Companies have a pressing need to both spread and mitigate cyber risk and fulfilling these goals will yield a positive impact on our national economy. Yet I believe there are several barriers that currently impede the cyber insurance industry from meeting its potential in these areas. I hope the views below assist the Commission as it considers recommendations addressing the cyber insurance market.

A Well-Functioning Cyber Insurance Industry Could Help Reduce Cyber Risk

A robust cyber insurance industry could materially improve overall cybersecurity in at least two ways. First, cyber insurers have an incentive to provide insureds with information that will raise the level of basic cyber preparedness across corporate America. The yearly comprehensive reviews of cyber incidents – such as Verizon's Data Breach Incident Report – consistently reveal that most cyber breaches capitalize on preventable lapses in basic cyber hygiene, including failures to patch known software defects or to implement appropriate password or other authentication regimes; susceptibility to phishing attacks; and insufficient least- access regimes. A well-functioning commercial cyber insurance industry could start and sustain a widespread and steady improvement in these basic cybersecurity measures through its underwriting practices.

Second, cyber insurers are well suited to play a critical role gathering and analyzing information about successful cyber attacks and then disseminating useful information to companies at risk. Insurers have a long history of gathering large amounts of risk and loss data for the very purpose of lowering insureds' risks and the potential for insurance payouts. The insurance industry could thus be a powerful force, in sector after sector, in the effort to identify, analyze and eliminate successful cyber risk vectors, including through the development of cyber standards.

At bottom, a strong insurance industry role in cyber security comes down to incentives. The steps that potential corporate cyber-victims take to protect themselves are lodged in cost centers, not profit centers. Most businesses find it hard to establish competitive advantage by touting their cyber security. And while the burgeoning cyber-defense industry in many instances provides real

assistance through consulting or technical solutions, a defense firm's business drops as the threat drops. If cyber insurance becomes the norm, however, the insurance industry's incentives over the long run should be well aligned with those of the insured in reducing risk. Importantly, ubiquitous cyber insurance could bring these benefits to smaller businesses not likely to have sophisticated internal cyber teams.

Some Current Barriers to a Well-Functioning Cyber Insurance Market

I believe there are a number of barriers keeping the cyber insurance industry from fulfilling its potential to raise cybersecurity standards and reduce cyber risk.

The first concerns the ability to access and to properly analyze pertinent information. An insurer's ability to provide insurance depends critically on information, both about an individual insured's cyber risk profile and about cyber risk generally. An insurer develops the parameters its insurance product – the range of coverage it will offer and the premiums for that coverage – based on as much information as it can gather about the subject risk. The more risk and loss data an insurer can gather and analyze, the better it can determine which risks it will cover and the price of that coverage.

The insurer also needs specific information about an insured to determine as precisely as possible where on the risk profile that insured lands, and therefore what coverage it will offer in return for a specified premium. Theoretically, the better an insurer can understand the insured's risk profile, the more precisely the insurer can provide correctly priced coverage. Equally, the better an insurer understands a company's risk profile, the more accurately it can provide the insured information that might lower risk. In a well-functioning insurance market the signals also flow the other way, with the price of insuring against residual risk helping a company quantify that risk.

Currently there are impediments to the sharing of important and relevant information at both of these levels. At the insured-specific level, insurers complain of too little time with an insured to gain a comprehensive understanding of the company's risk profile. The three-way relationship among insured, the broker representing the insured, and one or more insurance companies potentially writing policies places significant time limitations on precise risk assessment.

The pace at which the cyber threat landscape changes also limits comprehensive insured risk analysis. Insurance renewal efforts frequently begin 120 days before coverage lapses and may involve only a single meeting among insured, broker and insurers. During this time, however, new cyber attacks or newly prevalent attacks can dramatically change the set of inquiries an insurer might have. For instance, until recently a primary cybersecurity concern was point of sale attacks. But the recent surge in ransomware attacks has made that vulnerability a key concern for many companies and their advisors. Thus the mechanics of selling commercial insurance today seem incompatible with getting full cyber risk information about an insured.

The other significant information challenge concerns obtaining detailed information about successful cyber attacks. I am not referring here to the growth of increasingly efficient information exchanges for cyber threat indicators, which are vital as a matter of real-time cyber defense. But common sense dictates that information about how a threat turns into a successful breach is at least as important. What defenses were deployed and failed? What systems – hardware, software and their configuration – turned out to be particularly susceptible to a threat?

In many instances, after-breach reports exist in the form of forensic studies commissioned by the victim company. Usually these reports are created at the behest of the victim's counsel and – these days – with the well-founded fear that litigation or regulatory action is not far off. The forensic reports are thus covered by the attorney-work product privilege. Although there is a good

argument that sharing these reports with a company's insurer does not necessarily waive the privilege, the standard advice of outside counsel is that doing so exposes the company to unnecessary risk.

One response to this problem would be to lower the litigation and regulatory risk breached companies face. Current trends, however, are precisely the opposite. On the private litigation front the risk of damages increased with the decision last year in *Remijas v. Neiman Marcus.* Prior to *Remijas*, the prevalent view was that an individual whose private information had been stolen in a breach but not yet misused did not have standing to sue the breached company. In *Remijas,* the Seventh Circuit reached the opposite conclusion, finding that a fear of future use of stolen information provides Article III standing. On the regulatory front 2015 and 2016 have seen a dramatic increase in federal agency efforts to exact large fines as a way to push companies toward better cybersecurity.

Another response would be to adopt privilege rules that encourage sharing the details of successful cyber attacks. The medical field provides an example. In response to malpractice concerns, hospitals and other medical providers decades ago adopted peer review reporting as a way to reduce medical error. Although many states passed laws to encourage this effort by deeming peer review reports confidential and exempt from discovery, a growing number of exceptions to and limitations on that privilege resulted in the (nearly unanimous) passage in 2005 of the federal Patient Safety and Quality Improvement Act. PSQIA creates a category of privileged information – Patient Safety Work Product – as well as a system of third party organizations – Patient Safety Organizations – designed to collect and analyze that protected data. A federal statutory privilege for after-action cyber investigations could free up valuable information to insurers and others that could raise the general level of cyber protection.

Another issue inhibiting the development of a well-functioning cyber insurance industry is the absence of detailed standards or codes describing highly secure cyber systems. The NIST Framework was a great step forward in providing companies with tools to assess and increase their own cybersecurity, but it is by design a high-level construct. To see the importance of codes for a well-functioning insurance business one can look at the commercial property insurance business, which is structured around the existence of very detailed building and safety codes. In the property market the insured pays the insurer to send an engineer to covered structures, closely inspect them for safety and code issues and produce a report pointing out any improvements that should be made. Insureds welcome these reports and use them to lessen their risks.

It may well be that comprehensive "cyber codes" are beyond reach given the very structure and ubiquity of the Internet. But efforts could be made to develop detailed best practice "codes" for emerging areas of activity. The Internet of Things, for instance, remains a relatively new area of endeavor, and could be constructed with security as a first thought, rather than an after-thought. Many security professionals and firms are of course already working along these lines, but there is no common understanding of how these "building codes for building code" will be agreed on, implemented and enforced, and how or whether the government should be involved in these efforts.

An additional approach could be insurance-backed cyber "safety standards." We are all familiar with the Insurance Institute for Highway Safety, established in 1959 by three large auto insurance associations, and now an independent research organization that, among other things, provides widely embraced vehicle safety ratings. An independent "rating" institute could be of significant assistance to companies, particularly in assessing risks in the parts of the cyber eco-system where providers often markedly limit their own liability through contract, such as with software and

cloud services. A cyber safety rating for these products would allow companies to gauge the risk associated with these foundational parts of their IT infrastructures.

A final issue confronting the cyber insurance industry is grimmer: whether cyber risk successfully can be insured at all. The question arises because cyber insurance is insurance against criminal behavior, and properly modeling the risks associated with criminal ingenuity in cyberspace is potentially too complex to allow the insurance industry profitably to insure cyber risk over the long run. A standard response is that the insurance industry has been providing "crime" policies for years. But there is something very different about the risk a typical crime policy covers – the thieving employee, the bank robber or kidnapper – and the risk of cybercrime. The bank robber, for example, typically pulls off one job at time, infrequently, and is at great personal risk of getting caught. Cyber crime is dramatically different. Cyber criminals stalk many corporate victims at once, persistently and usually from a foreign country and so run only a minimal risk of identification, let alone capture and punishment. And the potential scale of loss in a cyber attack certainly puts cyber risk in an entirely different category. Thus while insurers' sales and marketing departments are bullish on cyber products, it may be that the actuaries in the back room will eventually take a much more dismal view of this line of business.

In conclusion, I again commend the Commission for looking into the role cyber insurance can play in mitigating cyber risk. Harnessing every potential source of help in this fight only makes sense given the current state of cyber intrusions. The insurance industry could be a powerful ally in spreading risk and ubiquitously improving corporate cybersecurity, and the Commission may deem it appropriate to make recommendations to strengthen that possibility. I hope my comments today are of some assistance to that end.

Irving Wladawsky-Berger

The Fact Sheet accompanying the President's Executive Order that established the Commission on Enhancing National Security clearly articulated the challenges we face:

"From buying products to running businesses to finding directions to communicating with the people we love, an online world has fundamentally reshaped our daily lives. But just as the continually evolving digital age presents boundless opportunities for our economy, our businesses, and our people, it also presents a new generation of threats that we must adapt to meet. Criminals, terrorists, and countries who wish to do us harm have all realized that attacking us online is often easier than attacking us in person. As more and more sensitive data is stored online, the consequences of those attacks grow more significant each year. Identity theft is now the fastest growing crime in America. Our innovators and entrepreneurs have reinforced our global leadership and grown our economy, but with each new story of a high-profile company hacked or a neighbor defrauded, more Americans are left to wonder whether technology's benefits could risk being outpaced by its costs."

"The President believes that meeting these new threats is necessary and within our grasp. But it requires a bold reassessment of the way we approach security in the digital age. If we're going to be connected, we need to be protected. We need to join together—Government, businesses, and individuals—to sustain the spirit that has always made America great."

Arguably, nowhere is this challenge greater than in the financial industries. As the famous song from Cabaret succinctly puts it "Money makes the world go round" and it's been doing so from time immemorial. Through the ages, money has been one of the most critical human innovations, facilitating transactions, trade and commerce. It's hard to think of a human innovation that's played such a central role in human affairs through the ages.

By analyzing the earliest recorded transactions, researchers believe that writing evolved in ancient Mesopotamia thousands of years ago, as an innovation to keep track of financial records. Money was later invented as a store of value and a medium of exchange to make trade and commerce more efficient. One of the world's first gold coins, now in the British Museum as part of its money exhibit, was produced over 2,500 years ago in Lydia, Western Turkey, whose last king, Croesus, was immortalized in the saying "as rich as Croesus." For a long time, money was embodied in precious metals like gold and silver, but with the introduction of banknotes, - most likely around 1000 AD in China, - money started to decouple from physical objects with intrinsic value.

Today, money is mostly intangible. Digital funds dominate the vast majority of the money supply, flowing over our digital networks as payments for our increasingly digital economic transactions.

Over the past several decades, the world's financial community has developed a very sophisticated global financial ecosystem, including the global payment infrastructures, the management of personal identities and personal financial data, the global financial flows among institutions and between institutions and individuals, the government regulatory regimes, and so on.

Our existing financial infrastructures has served us well so far, but they're rather complicated, inefficient and inflexible, and we rightfully worry that they're not up to the scalability, security and privacy requirements of our 21st century digital economy, especially when you include an additional few billion people around the world conducting financial transactions over their smartphones, let alone 10s-100s billions of IoT devices of all sorts whose transactions have to be carefully validated given their potential impact on our health and safety.

The financial industry has long been one of the major users of IT, - among the first to automate its back-end and front-office processes and to later embrace the Internet and smartphones. However, banking, and finance in general, has been relatively less disrupted by digital transformations than other industries like IT, media and retail. In particular, change has come rather slowly to the world's financial infrastructure

Transforming this highly complex global ecosystem has proved to be very difficult. It requires the close collaboration of its various stakeholders, including a large variety of financial institutions, merchants of all sizes, government regulators in just about every country, and huge numbers of individuals around the world. All these stakeholders must somehow be incented to work together in developing and embracing new payment innovations. Not surprisingly, change comes slowly to such a complex ecosystem.

This was the case in the industry where I've worked for most of my professional career, - the IT industry. In the early years of the IT industry, different vendors brought to market their own proprietary networking systems, such as IBM's Systems Network Architecture and Digital's DECnet. These worked quite well as long as all communications were within the same company using the same vendor's architecture. But, going across companies and vendors was quite cumbersome. Just sending an e-mail using an IBM application to another user in a different institution using another vendor's application was quite cumbersome.

The Internet changed all that. Once the Internet was widely embraced in the 1990s, it became no harder to send an e-mail between companies as within a company. Everyone was using the same standards, including open source implementations of key protocols. Rather than developing their own proprietary networks and struggling to interconnect with those of others, institutions now collaborated on developing the common Internet architecture, - and Internet based applications like e-mail and the Web, - that they all now used.

Much of the success of the Internet and Web are due to the international organizations created to oversee their evolution, - IETF, the Internet Engineering Task Force, and W3C, the World Wide Web Consortium, founded in 1989 and 1994 respectively. This is also the case with Linux, which emerged in the 1990s as a UNIX-like operating system that over time was embraced by just about everyone. The collaborative governance of Linux, - overseen by the Linux Foundation, - has helped it succeed where similar previous efforts failed. In addition to developing standards and organizing promotional activities, these various organizations make available open source implementations of their software releases, thus encouraging collaborative, open innovation.

Let me remind you that the Internet started out in the late 1960s as a DARPA sponsored project aimed at developing a robust, fault-tolerant computer network. And the Web was first developed by Tim Berners-Lee at CERN in the late 1980s to facilitate the sharing of information among researchers around the world. But, transformational innovations don't always play out as originally envisioned. Once in the marketplace, they seem to acquire a life of their own.

The blockchain first came to light around 2008 as the architecture underpinning bitcoin, the best known and most widely held digital currency. But, as with the Internet, the Web, and other major technologies, the blockchain has now transcended its original objective.

Over the years, blockchain has developed a following of its own as a distributed data base architecture with the ability to handle trust-less transactions where no parties need to know nor trust each other for transactions to complete. Blockchain holds the promise to revolutionize the finance industry and other aspects of the digital economy by bringing one of the most important and oldest concepts, the ledger, to the Internet age.

Ledgers constitute a permanent record of all the economic transactions an institution handles,

whether it's a bank managing deposits, loans and payments; a brokerage house keeping track of stocks and bonds; or a government office recording births and deaths, the ownership and sale of land and houses, or legal identity documents like passports and diver licenses. Over the years, institutions have automated their original paper-based ledgers with sophisticated IT applications and data bases.

But while most ledgers are now digital, their underlying structure has not changed. Each institution continues to own and manage its own ledger, synchronizing its records with those of other institutions as appropriate, - a cumbersome process that often takes days.

A 2014 report by the Bank of England argues that the time might well have now come for the ledger to now follow the collaborative, distributed, standards-based approach of those earlier innovations. The classic ledger, - "a process that has not changed since the 16th century," - may now be evolving toward a blockchain-based distributed ledger, a major technological innovation not only for payment systems but for the finance industry as a whole.

Sometimes, the emergence of an innovative disruptive technology can help propel change forward. The Internet proved to be such a catalyst in the transformation of global supply chain ecosystems. Could blockchain technologies now become the needed catalyst for the evolution of the global financial ecosystems? Could it prove to be a kind of Next Big Thing?

Much, much work remains to be done. Blockchain is still at the bleeding edge, lacking the robustness of legacy payment systems. Distributed ledger systems have only been around for less than a decade, and are thus quite immature compared to the existing, decades-old financial infrastructures. The evolution of our complex, global financial infrastructures will be a tough and lengthy undertaking, no matter how innovative and exciting the new technologies might be.

It's too early to know if the blockchain will join the pantheon of Next Big Things and become a major transformational innovation. As we've seen with other such successful innovations, - e.g., the Internet, the Web, Linux, - collaborations between universities, research labs, companies and government agencies are absolutely essential. So are close collaborations among technology developers and users in order to get the architecture right, agree on open standards, develop open source platforms and set up governance processes embraced by all.

In a short number of years, blockchain technologies have made a lot of progress. It will be fascinating to see how it all plays out in the years to come.

Alex Pentland

Today's "data ecology" is transforming due to the exponential growth of mobile and ubiquitous computing, together with big data analysis. These shifts are having a dramatic impact on people's personal data sharing awareness, sensitivities and on their cybersecurity. Recently have reached critical mass in privacy concerns and awareness on the use of personal data, partially due to media exposure of cybersecurity breaches and intelligence scandals. The surge of mobile transactions, micropayments, and connected sensors in both private and public spaces is expected to further exacerbate this tension.

We need a "new deal on data" where security concerns are matched with transparency, control and privacy, and are designed into the core of any data-driven service [1]. In order to demonstrate that such a sustainable data ecology is possible we have developed Enigma, a decentralized computation platform enabling different parties to jointly store and run computations on data while keeping the data completely private [2]. Enigma enables a sustainable data ecology by supporting the requirements that data be *always encrypted,* with computation happening on encrypted data only, by allowing owners of the data to control access to their data precisely, absolutely, and auditably, and by reliably enabling payment to data owners for use of their data.

From the user's perspective, Enigma is a cloud that ensures both privacy and integrity of their data. The system also allows any type of computation to be outsourced to the cloud while guaranteeing the privacy of the underlying data and the correctness of the result. A core feature in the system is that it allows the data owners to define and control who can query it, thus ensuring that the approved parties only learn the output. Moreover, no other data leaks in the process to any other party.

The Enigma cloud itself is comprised of a network of computers that store and execute queries. Using secure multi-party computation (sMPC or MPC), each computer only sees random pieces of the data, a fact that prevents information leaks. Furthermore, queries carry a micro-payment for the computing resources as well as to those users whose data is queried, thus providing the foundation for the rise of a sustainable, secure data market.

To illustrate how the Enigma platform works, consider the following example: a group of data analysts of an insurance company wishes to test a model that leverages people's mobile phone data. Instead of sharing their raw data with the data analysts in the insurance company, the users can securely store their data in Enigma, and only provide the data analysts with a permission to execute their study. The data analysts are thus able to execute their code and obtain the results, but nothing else. In the process, the users are compensated for having given access to their data and the computers in the network are paid for their computing resources.

Three types of entities are defined in Enigma, and each can play multiple roles (see Figure 1). *Owners* are those sharing their data into the system and controlling who can query it; *services*, if approved, can query the data without learning anything else beyond the answer to their query; and *parties* (or *computing parties*) are the nodes that provide computational and storage resources, but only ever see encrypted or random bits of information. In addition, all entities are connected to a blockchain as described below.

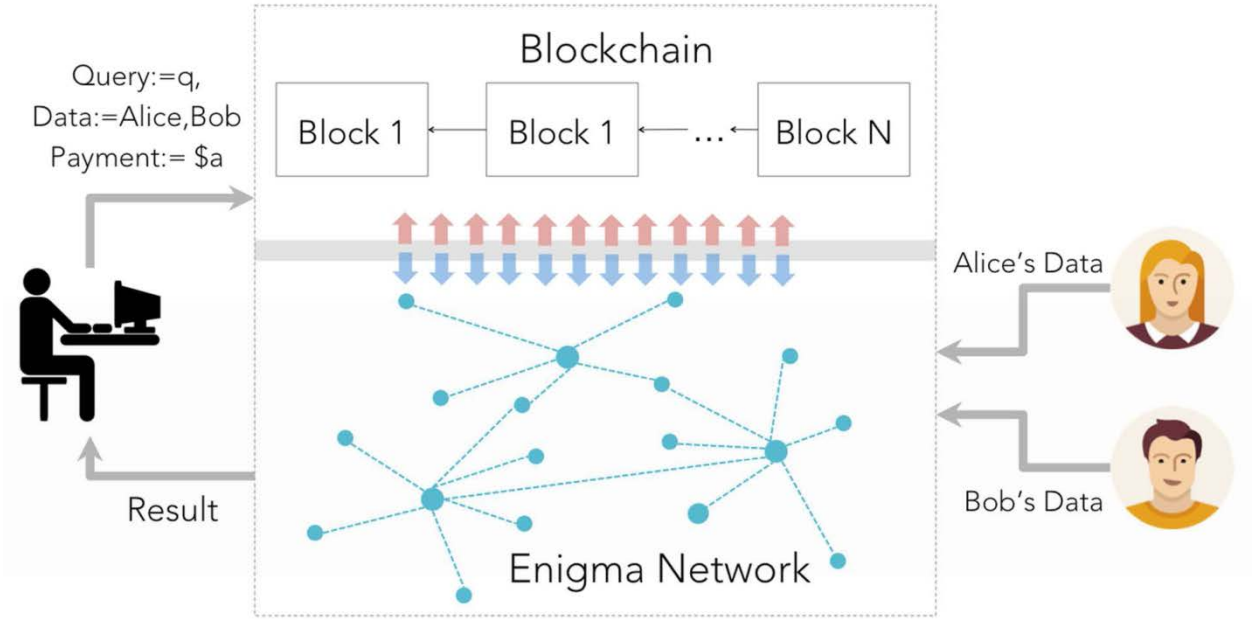

Figure 1. Overview of Enigma's decentralized platform.

When owners share data, the data is split into several random pieces called *shares*. Shares are created in a process of secret-sharing18 and perfectly hide the underlying data while maintaining some necessary properties allowing them to later be queried in this masked form. Since users in Enigma are owners of their data, we use the blockchain as a decentralized secure database that is not owned by any party. This also allows an owner to designate which services can access its data and under what conditions, and so parties can query the blockchain and ensure that it holds the appropriate permissions. In addition to being a secure and distributed public database, the blockchain is also used to facilitate payments from services to computing parties and owners, while enforcing correct permissions and verifying that queries execute correctly.

In summary, a sustainable data ecology requires that data be *always encrypted,* and that computation happen on encrypted data only. It also requires that owners of the data control access to their data and use of their data precisely, absolutely, and auditably. Finally, it requires that data owners are reliably paid for use of their data. Enigma accomplishes these requirements, providing an existence proof that a sustainable, secure data ecology is possible. The major question about this ecology is one of policy: what the trade-off between user security and access by law enforcement and intelligence services? In the current Enigma system this trade-off is handled by leaving metadata encrypted but visible. Other trade-offs are possible, including full anonymization or building in the ability for court-ordered investigators to penetrate anonymity though zero-knowledge proofs (which Is different than back-door approaches).

For additional information see http://trust.mit.edu

[1] Pentland, A. Reality mining of mobile communications: Toward a new deal on data. *World Economic Forum Global IT Report 2008*, Chapter 1.6, (2008), 75-80.

[2] Zyskind, G., Nathan, O., and Pentland, A. (2015). Decentralizing privacy: Using blockchain to protect personal data. In Proceedings of IEEE Symposium on Security and Privacy Workshops, 180-184.

Jerry Cuomo

Eighty years ago, IBM helped the United States government create the Social Security system, which, at the time, was the most complex financial system ever developed. Today, as financial transactions become increasingly digital and networked, government and industry must once again combine forces to make the financial systems of the future more efficient, effective and secure than those of the past.

And, just as an individual's Social Security number became the key to proving identity and accessing that system for generations of Americans, today's institutions must collaborate to create new methods for establishing identity and managing other aspects of digital transactions.

At IBM, we believe that blockchain technology is becoming an essential tool as business and society navigate this shift--with the potential for transforming commerce and the interactions between governments and individuals. Blockchain has inherent qualities that provide trust and security, but, to fulfill its promise, the core technology must be further developed using an open source governance model to make it deployable on a grand scale.

There's a critical role for government here—both to enhance national competitiveness and national security. The federal government must invest in scientific research to accelerate progress. The National Institute of Standards and Technology can help shape standards for interoperability, privacy and security. And government agencies can become early adopters of blockchain applications. In addition, government has a key role to play in certifying the identities of participants in blockchain-based systems.

Blockchain came to prominence because it's the core technology underlying the infamous Bitcoin cryptocurrency, but, while Bitcoin is an anonymous network, industries and government agencies are exploring the use of blockchain in networks where the participants are known. We call this a "permissioned blockchain."

Here's how it works: A blockchain is a distributed ledger shared via a peer-to-peer network that maintains an ever-expanding list of data records. Each participant has an exact copy of the ledger's data, and additions to the chain are propagated throughout the network. Therefore, all participants in an interaction have an up-to-date ledger that reflects the most recent transactions. Once a transaction is entered in the ledger it can't be changed. Cryptography and digital signatures are used to prove identity, authenticity and enforce access to the shared ledger. Blockchain makes applications fast, efficient and inherently secure.

IBM is playing a central role in the development of a permissioned blockchain. We're a founding member of the Linux Foundation's open-source HyperLedger Project, where we're helping to build the foundational elements of business-ready blockchain architecture; with a focus on privacy, confidentiality and auditability. We have joined consortia that are developing industry-specific blockchain implementations. And we're pioneering the use of blockchain in our own operations.

Blockchain has tremendous potential to help transform business and society, but it's so strikingly different from what people are used to that many business and government leaders are adopting a wait-and-see attitude. We applaud judicious caution, but, at the same time, we believe that organizations and institutions that don't quickly assess the potential of blockchain and begin experimenting with it risk falling behind as the world undergoes what we see as a tectonic shift.

There are four areas where we believe government, technology companies and industries should work together to advance blockchain to enhance national security:

Proof of Identity. The Social Security number has been a mainstay of our society for decades, but

it's not secure and certifiable enough to serve as the building block of identity in a blockchain ecosystem. So we believe a new identity management system must be created. For guidance, we might study the Unique Identification Authority of India, which is in the process of issuing 12-digit identity numbers to all 1.2 billion Indian residents. An individual's "Aadhaar" number is linked to biometric and demographic information and can be used for everything from setting up a bank account to accessing government services.

Data provenance: To make organizations and individuals comfortable exposing their data through the use of blockchain applications, the systems must automatically track every change that is made to data, so it's auditable and completely trustworthy. Just as an identity-management system certifies individuals and organizations that participate in a blockchain, the data provenance mechanism provides a fingerprint for the data itself—complete with time stamps and annotations. A participant can rest assured that what they see is accurate, up to date, and untampered with. The same goes for government regulators or law enforcement.

Secure transaction processing: While the parties in a transaction managed using blockchain are known to other participants in the system, the actual details of the transaction should be visible only to those involved (or others who are granted permission). So we have to enable the entities that monitor blockchain transactions to verify that contracts are being fulfilled but without revealing confidential information to them. This will require the use of techniques that fall under the heading of multi-party computation. One of the most intriguing of them, called full homomorphic encryption, makes it possible to verify information without having to de-encrypt it—which would leave it vulnerable to tampering, theft or prying eyes. The technique is still several years from being practical, but it's on the way.

Sharing intelligence. Amid a rising tide of cyber-crime and fears of cyber-terrorism, the White Hats of the world are under pressure to change the game. Blockchain has the potential to do just that. Not only is it inherently more secure than other types of networks and financial management systems, but blockchain has the potential to be used by multiple parties to share cyber-threat intelligence. Today, for fear of being exposed, many financial services firms are reluctant to share information about cyber-attacks. However, with blockchain, they could confidentially share information in real time that, when combined with data from other companies, could be used to spot patterns and quickly develop countermeasures.

While government should not seek to control these new financial systems, it has an important role to play in helping them to take off and in safeguarding them. Think of this as a new social compact, where business, with input from government, architects the future of financial services. At IBM, we look forward to working with our partners in government, industry and academia to get this done.

Greg Baxter

The global finance system is a critical infrastructure built on trust, and integral to the effective and progressive functioning of society. A structural breach of that trust would have severe economic and social implications. As a bank, our highest priority is to maintain that trust: by protecting our client's assets, both money and data, and by protecting the integrity of the global financial system. In an increasingly digital and global world, the ways in which we serve and protect our clients is changing significantly, but the underlying need for trust and integrity remains absolute.

The digital revolution is transforming financial services. With it, comes significant opportunities to provide access to financial tools and products that can facilitate individual and collective progress and prosperity. Our research with Imperial College London concluded that a 10% increase in the use of digital money, that is electronic transfer of fiat currency rather than paper based, can lead to 220 million people coming into the formal financial sector globally, resulting in $1TN in new flows for the formal economy, $100BN in increased tax collections, and significant efficiency and security benefits for all stakeholders. However, the migration to digital also brings new, sophisticated and rapidly growing cyber risks.

The migration of financial services to digital is well underway. The vast majority of corporate banking flows are already digital, and, with the significant efforts of the Fintech industry, the digitization of many consumer flows is gaining momentum. Investments in financial technology have grown exponentially, rising from $1.8 billion in 2010 to $19 billion in 2015 — with over 70% of this investment focusing on the "last mile" of user experience in the consumer space. The US leads this investment, followed by China, the UK and Sweden. Most of the focus has been on payments and lending. While the U.S. and Europe are still at an early stage of disruption, China is already past the tipping point and we see India as the next big disruption opportunity. We project that for North America, retail banking disruption will grow from 1% of industry revenues today, to affect ~10% of revenues by 2020 and ~17% by 2023. While most investment has focused on improving the client experience, without changing the underlying financial product or platform, we are now starting to see more innovation occurring in the core product and underlying financial "rails".

As innovation changes experiences, journeys, products and platforms, there is a shift in financial services from vertical products to horizontal services, integrated into open, digital ecosystems. While banks may have traditionally operated and protected "core" platforms and saw "edge" devices as channels, with distinct cybersecurity implications, the new reality is a much broader ecosystem with many more points for digital access and cyber threats.

To protect people and their assets requires new ways of identifying and authenticating customers and devices, new approaches to managing and using payment credentials and more sophisticated monitoring capabilities.

Advances in biometric technologies, emerging behavioral analytics and adaptive techniques that merge these new capabilities are promising in terms of increasing authentication without substantially deteriorating client experience.

Tokenization of payment credentials, so we no longer store or transmit static payment details, but instead create dynamic, single use payment tokens, bound by time, location and value should radically reduce the risk of stolen credentials. It should also eliminate the need to store payment details in the rapidly growing number of places and things where payments are made.

Static tokenization is already being deployed in new mobile payment products, and marks an important first step. Importantly, in a world where privacy and security are often argued to be incompatible, tokenization is a great example of a technology that enhances both security and privacy.

While the proliferation of payment nodes creates additional points of vulnerability, it also creates millions of information points. Every node in the network needs to become an intelligent node and be aware of up-stream and down-stream threats in a heterogeneous digital ecosystem. The use of big-data along with advanced analytics provides the potential to collect this data across the entire network and to respond in real time to new threats. Security becomes a collective responsibility, inclusive of every node on the network, inclusive of every player in an ecosystem. In a more open and inclusive ecosystem, collaboration and collective accountability will be critical to solving cyber issues. There can be no free riders.

Beyond protecting the assets and transactions of clients, there is a more systemic threat that we need to tackle. An attack on the national or global payments system represents a far greater threat to the economy and society. Sophisticated actors who do not want to steal assets, but to attack companies or destroy the underlying system. Defending against such a broad and sophisticated set of actors, with significantly different objectives and incentives, requires an extremely sophisticated defensive capability, and one where many businesses will be ill- equipped to respond.

There are three areas where the Government may be able to provide additional support to the private sector:

1. **Intelligence sharing** – increasing the speed and quality of two-way information flows, which is essential for developing an intelligence led approach to cyber protection, and mounting a holistic defense
2. **Research and development** – We need to dramatically increase the speed and scale of cyber innovation in both the private and public sector. This will require increased investments in research and development, which may require increased financial incentives and capability support.
3. **Workforce development** – One of the most critical issues facing corporations is a shortage of cyber trained personnel. We need to increase and maintain the available workforce, which may require greater educational capacity and incentives.

While not included in the above list, the potential role of the Government to provide a pro-active defense for critical companies that come under cyber attack should also be evaluated. We may need to look to real-time threat intelligence and response across public, private and governmental agencies accompanied by a legal framework required to implement such programs. And given the global nature of the internet, and the borderless nature of cyberspace, our solutions and partnerships need to stretch beyond the USA.

In a world of exponential technological change, we need a commensurate commitment and investment to stay ahead of the security frontier. New threats will emerge, some we can already imagine, such as the impact of quantum computing on current cryptographic algorithms, and some we cannot. Solving these will require coordinated cyber resilience undertaken as a public/private partnership in coordination with governments, to build national, institutional and individual capabilities.