The degree of gravity with which we view the cyber threat is a matter of perspective, experience, interaction, and awareness. Whether we view it as a criminal act or terrorism or a hybrid is an important point for discussion. Resolving that question helps frame how we perceive those responsible for cyberattacks and facilitates resolution regarding punishment for their actions. That question has relevance for law enforcement, prosecutors, defense attorneys, and the judiciary. Our focus, as the title suggests, is on cybersecurity cooperation in an effort to minimize the impact of an attack. Cooperation, as we shall come to see, raises concerns in different quarters. Some of that concern is legitimate. It needs to be addressed and compellingly responded to. A cooperation model is intended to offer institutionalized mechanisms for preventing—or at least minimizing—the harm posed by the mere threat of an attack, much less an attack itself.
Introduction

It is commonly accepted today that cyber threat is a reality. The degree of gravity with which we view it is a matter of perspective, experience, interaction, and awareness. Whether we view it as a criminal act or terrorism or a hybrid is an important point for discussion. Resolving that question helps frame how we perceive those responsible for cyberattacks and facilitates resolution regarding punishment for their actions. That question has relevance for law enforcement, prosecutors, defense attorneys, and the judiciary. There are also moral considerations relevant to this discussion in the context of responsibility and accountability.

An additional reality, historically, is a lack of cooperation among distinct—yet interconnected—communities that have much to gain by banding together in the face of a grave threat. A retrospective analysis of how potential targets of cyberattacks, and those with a vested interest—and capability—to minimize the threat, fail to join forces paints a disconcerting picture. That picture, in a nutshell, reflects an unwillingness—for a variety of reasons—to recognize the benefits of a unified response to cyberattacks.

This reluctance or hesitation is not new to 2018; my research while engaged in cybersecurity writing projects made that very clear. In other words, the lack of cooperation noticed in 2018 is not a recent development, quite the opposite: a review of the relevant data, literature, and anecdotal evidence over the years convincingly highlights an—for lack of a better term—institutionalized lack of cooperation. In considering different reasons for the success enjoyed by cyber actors, their nefariousness is enhanced by a consistent failure of potential targets to recognize the benefits of adopting a cooperation model. Given the persistent, committed, and unrelenting efforts of those committed to engaging in cyberterrorism/cyberattacks, the failure to consistently commit to cooperation models is noteworthy, and troubling. Noteworthy because it reflects a consistent pattern; troubling because it facilitates continued harm to society, broadly defined.

Cyber threat has relevance for law enforcement, prosecutors, defense attorneys, and the judiciary. There are also moral considerations relevant to this discussion in the context of responsibility and accountability

That historical pattern explains, in part, the success of cyberattacks. It reflects a failure to fully develop defensive measures that would minimize, if not mitigate, the harm perpetuated by the effects of cyberattacks. Recognizing the consequences of a lack of cooperation stands out when reviewing cybersecurity issues over the years; developing, and implementing, cooperation models reflects a positive—and much-needed—measure to more effectively respond to a clear threat. Those twin realities are at the core of the discussion in the pages ahead.

Framing an issue has importance in determining resources allocated to countering, mitigating, and minimizing threats. Similarly, resolving the terrorism–criminal law–hybrid dilemma is relevant in determining operational measures that can be implemented against the actor, or actors, responsible for a particular attack. However, as important as that discussion is, it is not the one pursued in the pages that follow. Our focus, as the title suggests, is on cybersecurity cooperation in an effort to minimize the impact of an attack. Cooperation,
as we shall come to see, raises concerns in different quarters. Some of that concern is legitimate. It needs to be addressed and compellingly responded to.

To undertake a discussion regarding cybersecurity requires defining the term. As is always the case in such matters, reasonable minds can reasonably disagree. That is a given and understandable.

I define cyberattacks as a “deliberate, nefarious use of technology intended to harm individuals, communities, institutions, and governments.” While this proposed definition is subject to disagreement, it is assumed that “harm”—regardless of whether an attack was successful—is a largely agreed-upon notion.

For cyber to be effective, there need not be an attack, nor must it be successful. Given the omnipresence of cyber—the mere fear of such an attack—we are, individually and collectively, spending significant resources, time, and energy on minimizing the potential impact of an attack. Much like counterterrorism, significant efforts are allocated to both preventing an attack and, were one to occur, to its impact and consequences. The point of inquiry is how do we most effectively protect ourselves; are we doing so presently; and are there more effective, creative mechanisms for doing so. It is safe to assume that those same questions are asked, in the reverse, by those dedicated to deliberately harming civil society, broadly and narrowly defined.

In a nutshell, it is cooperation among distinct potential targets and among different law-enforcement agencies and between targets and law enforcement. Concisely stated, it proposes that the impact of a cyberattack can be minimized by instituting cooperation models. It is intended to offer institutionalized mechanisms to prevent—or at least minimize—the harm posed by the mere threat of an attack, much less an attack itself. Given the consequences of an attack, and the resources required to minimize its impact, the proposed cooperation model is intended to minimize costs, direct and indirect alike, of cyber. The model is predicated on an assumption: preventing an attack, or at the very minimum making a concerted-determined effort, is preferable to absorbing the costs of a successful attack.

As I have come to learn, there are corporate executives who subscribe to a distinctly different argument: it is more cost-effective to absorb a hit rather than invest in sophisticated protection models. I have met with executives whose corporations were the targets of successful attacks who subscribe to this theory. For me, this rationale reflects short-term thinking focused on narrow economic considerations, suggesting a lack of understanding regarding benefits accruing from proactive protection and cooperation models. These people also articulated concerns regarding public image, customer anxiety, and an upper hand that competitors might gain. From a strictly business perspective, narrowly defined and applied, such an approach...
is, perhaps, understandable. The argument made was rational, neither impulsive nor spur of the moment; from my interactions, it was also clear that my interlocutors considered this perspective reflective of best-business practices.

This is something that is not to be casually dismissed with a wave of the hand. Nevertheless, their argument reflects narrow tactical considerations, focused internally, devoid of examining the larger picture and possible benefits that may accrue. Whereas information sharing, in an effort to minimize harm, was presented to these executives as a positive, their (inward looking) perspective led them to perceive information sharing as a negative, with significant impact on their product and positioning.

It is important to add that law-enforcement officials perceived the cooperation model as a positive, enhancing their efforts, albeit with one caveat: clearly articulated hesitation by federal law-enforcement officials to cooperate information share with their state and local counterparts. Whether this is institutionalized hesitation or limited to specific individuals is unclear; exploring this question did not lead to clarity one way or the other.

In this article I hope to convince readers of the shortsightedness of such an approach and to highlight the benefits of the proposed cooperation model.

For cyber to be effective, there need not be an attack, nor must it be successful

The question, in a nutshell, is: what is the most effective means for enhancing cybersecurity?

To convince the reader of the viability of such a proposal, we must examine the costs of cyber, threat and attack alike. That is, there must be a benefit accrued to acceptance of a cooperation model. That benefit must outweigh any attendant costs, otherwise the proposal is a nonstarter from the very outset. Similarly, concerns must be allayed that cooperation is not an “own goal,” whereby positive intentions have harmful, unintended consequences that mitigate the value of cooperation. The working premise, as discussed below, is that cooperation is a positive, should be viewed accordingly, and that models need to be developed to facilitate its successful implementation.

This will not be easy as was made clear to me both while writing my book, Cybersecurity: Geopolitics, Law, and Policy, and then reinforced while conducting a tabletop exercise. Notwithstanding the arguments posed—some understandable, others best characterized as “head scratchers”—I believe that the proposed cooperation model deserves careful attention in the face of relentless cyberattacks. As the cliché goes: “The best defense is a good offense.”

The discussion below will be divided into the following five sections: “What does Cooperation Mean”; “Cooperation Among Whom”; “Cooperation to What Extent”; “The Good, the Bad and the Ugly of Cooperation”; and “Final Word.”

What does Cooperation Mean

Cooperation has many definitions and meanings. Context, times, culture, and circumstances play an important role in both defining the term and its actual implementation. Cooperation can be permanent, transitory, or situational; it can be predicated on formal arrangements and informal understandings alike. Cooperation, whether bilateral or multilateral, is at its best when the parties believe the relationship is mutually beneficial.
That does not suggest that such an agreement—formal or informal—is cost-free. It is not. But that is the reality of any agreement for the implication is that certain “freedoms” are voluntarily relinquished for a perceived benefit. One has only to recall the writings of Hobbes, Locke, or Rousseau to recognize the costs—and benefits—of creating and joining a community.4

That is the essence of cooperation. In joining a community, and cooperating with its members, we seek safety, security, and protection. That is generally perceived to be a positive; in return, we give up individualism, a certain degree of free will, and some independence. For some, that is an unacceptable cost, not outweighed by benefits that may be procured by the positives that emanate from cooperation. Fair enough.

However, as history suggests, in the main the benefits of cooperation outweigh perceived, or actual, costs. Exceptions exist. Of that there is no doubt. However, the notion of “banding together” for a common enterprise or undertaking is generally perceived to be preferable to “going it alone.” To facilitate—if not enhance—effectiveness, an agreement of cooperation must include:

1. consensus regarding common goals;
2. mechanisms for assessing continued costs–benefits;
3. mechanisms for withdrawing from the agreement;
4. established parameters of the agreement;
5. agreed-upon implementation mechanisms of the agreement.

Needless to say, the underlying predicate is that parties enter into the agreement voluntarily, recognizing a need for such an arrangement, and recognizing that the alternative is not beneficial. As we move forward in this discussion, these principles serve as the basis for our recommendation that cooperation be an integral aspect of minimizing the threats posed by cyberattacks, whether viewed as a crime, terrorism, or a hybrid.

To put flesh on the bones: the cooperation model I recommend would benefit private and public entities alike. This model would, similarly, require—obligate—corporations that have been hacked to institutionalize reporting mechanisms to law enforcement and customers alike. The intersecting vectors between the public (broadly speaking), municipalities, law enforcement, and corporations (public and private alike) are numerous.

This complexity reflects the multiplicity of threats and vulnerable targets alike. To implement this recommendation is, as I have come to learn, counterintuitive for many affected parties, including corporations (not surprisingly) and law enforcement (surprisingly). The notion, as discussed below, of perceiving this as a collective security model combined with legitimate self-defense (both adopted from international law) was met with skepticism.
Corporate resistance reflected concern regarding potential loss of revenues and unintended consequences in the guise of advantages gained by competitors; law-enforcement hesitation was premised on two different rationales: an unwillingness among federal law-enforcement officials to cooperate with local officials and the lack of resources available to address cyberattacks. The first argument is a nonstarter; the second requires recognition that cybercrimes demand sufficient allocation of resources to position law enforcement as a more effective partner in what must be a collective effort to minimize the threat posed by nefarious actors (see below for a discussion of the Cybersecurity Information Sharing Act, 2015).

How to achieve the corporation model? There are a number of alternatives and options, some reflecting voluntary measures, others legislatively imposed. In the ideal, the former would “rule the day”; however, as was made clear in numerous conversations, that is, unfortunately, unlikely. Which gives rise to a proposal to legislatively mandate cooperation models, imposing a duty on potentially impacted targets of cyberattacks (the list of potential targets is outlined under “Cooperation Among Whom,” below).

A word of caution: suggesting congressional intervention, beyond existing requirements, is a source of great discomfort, particularly for the private sector and ideological concerns, and particularly for libertarians who strongly reject such measures. Both are legitimate, and potent, stumbling blocks in seeking to advance such legislation. This potency is magnified by the reality of politics, particularly in the divisive environment that presently defines the US.

**Corporate resistance reflects concern regarding potential loss of revenues and unintended consequences in the guise of advantages gained by competitors**

Reporting requirements, as illustrated by the Sarbanes–Oxley Act of 2002,² are the bane of many corporate leaders. One corporate executive described the legislation as imposing unwieldy burdens, costs, and obligations on corporations. According to this executive, his team was comprised more of compliance officers than production officers.

Without doubt, that imposes unwanted—perhaps unwarranted—costs on corporations. Nevertheless, the risks and threats posed by cyberattacks justify exploring mechanisms obligating cooperation. That is, if voluntary cooperation is not possible, then the discussion needs to be expanded to the possibility that cooperation be mandated.

The 2015 Cybersecurity Information Sharing Act (S. 754), introduced by US Senator Richard Burr (R-NC) and signed by President Obama on December 18, 2015, was an important measure for it “authorizes cybersecurity information sharing between and among the private sector; state, local, tribal, and territorial governments; and the Federal Government.” The legislation sought to accomplish four important goals; namely it:

— requires the federal government to release periodic best practices. Entities will then be able to use the best practices to further defend their cyber infrastructure;
— identifies the federal government’s permitted uses of cyber threat indicators and defensive measures, while also restricting the information’s disclosure, retention and use;
— authorizes entities to share cyber-threat indicators and defensive measures with each other and with DHS [the Department of Homeland Security], with liability protection;
— protects PII [Personally Identifiable Information] by requiring entities to remove identified PII from any information that is shared with the federal government. It requires that any federal agency that receives cyber information containing PII to protect the PII from unauthorized use.
or disclosure. The U.S. Attorney General and Secretary of the Department of Homeland Security will publish guidelines to assist in meeting this requirement.7

In the same vein, on July 6, 2016, the European Parliament adopted the Directive on Security of Network and Information Systems (the NIS Directive), which provides legal measures to boost the overall level of cybersecurity in the EU by ensuring:

— Member States’ preparedness by requiring them to be appropriately equipped, e.g. via a Computer Security Incident Response Team (CSIRT) and a competent national NIS authority;
— cooperation among all the Member States, by setting up a cooperation group, in order to support and facilitate strategic cooperation and the exchange of information among Member States. They will also need to set a CSIRT Network, in order to promote swift and effective operational cooperation on specific cybersecurity incidents and sharing information about risks;
— a culture of security across sectors which are vital for our economy and society and moreover rely heavily on ICTs, such as energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure. Businesses in these sectors that are identified by the Member States as operators of essential services will have to take appropriate security measures and to notify serious incidents to the relevant national authority. Also key digital service providers (search engines, cloud computing services and online marketplaces) will have to comply with the security and notification requirements under the new Directive.8

The question is how to build off both these important measures and increase the levels of cooperation among different communities, creating an infrastructure that most effectively minimizes the possible consequences of a cyberattack. This requires integrating sectors, vectors, and interest groups. To do so most effectively requires recognition that existing cooperation measures, as well-intentioned as they maybe, fall short. The “why” was made clear to me; the challenge as we move forward in this discussion is determining whose cooperation must be more effectively institutionalized.9

It is to that question that we turn our attention.

Cooperation Among Whom

From the general to the specific. In the cybersecurity realm, the number of targeted, if not impacted, targets include the following (this is not an all-inclusive list):

— individuals who are the targets of identity theft;10
— individuals whose privacy is compromised when, for example, health-care providers are hacked;
— corporations (of all sizes) whose data is compromised;
— the financial industry, including banks, investment houses, stock markets;
— municipalities whose infrastructure (that is, traffic signals, water systems) is compromised;
— hospitals, thereby endangering patient welfare and the safety and protection of health records;
— militaries, when weapon systems are compromised;
— airlines and air-traffic-control systems;
— government agencies and offices.
The impact of cybercriminals is increased by the incapacity of their potential targets to recognize the advantages of adopting a cooperative model.

In the west wing of the White House, then US President Barack Obama announces changes in his government’s cybersecurity policy following a cyberattack on the Pentagon in which information on the F-35 fighter was stolen. May 29, 2009.
On July 6, 2016, the European Parliament adopted the NIS Directive, which provides legal measures to boost the overall level of cybersecurity in the EU.

Fiberoptic and copper Ethernet cables. The Department of Culture, Communication and Sports is working with the British Ministry of the Interior on a white paper to oblige technology giants to disclose how they manage the offensive and illegal material published by their users.
This list, while not inclusive, is sufficiently broad to highlight the range of potential cyberattack targets. It emphasizes the significant number of people, institutions, corporations, and critical infrastructure at risk from a cyberattack. The notion of “risk” is essential to the cooperation discussion; devoid of potential risk, the impetus for entering into an agreement is significantly minimized, if not entirely eviscerated.

However, the reality of cybersecurity is that it is a world of clear, but unknown, unseen, undiscernible threats until the attack actually occurs. The cyber threat must be phrased as “when will an attack occur” rather than “if an attack will occur.”

The list above reflects the broad range of potential targets. It also highlights the scope of secondary victims, impacted by a particular attack. Furthermore, it accentuates the important question of “to whom a duty is owed.” Cooperation must not be viewed as “nice to have,” but rather as a means necessary to protect intended, and unintended, victims alike of a cyberattack. To state the obvious: the number of individuals impacted by a hack into any of the entities listed above is staggering. Not only is the financial cost extraordinary, but the crippling of a municipality, the impact on a hospital, the danger incurred by air travelers, the consequences faced by those requiring services provided by government agencies are literally overwhelming.

That in and of itself should make cooperation among the above an obvious measure. I propose we consider this proposition through the lens, by extrapolation, of international law. Doing so, enables us to examine cooperation as both self-defense and collective security. In the context of cooperation among potential victims of a cyberattack, this proposed duality provides an intellectual—and perhaps practical—framework. It highlights two important realities: the necessity of self-defense and recognition that joining forces is an effective means of enhancing protection.

Cooperation, or mutual security, does not imply agreement on all issues nor does it suggest a perfect confluence of interests, values, and goals. It does, however, reflect recognition that certain threats, given their possible consequences, warrant finding a sufficient meeting ground even when the parties may have otherwise competing interests. The two principles—self-defense and collective security—can be viewed as complimentary of each other. On the one hand, individual action is justified; on the other, recognition that certain instances require cooperation in order to facilitate protection.

Article 51 of the United Nations Charter states:

Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defense shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.
Article 5 of the NATO Treaty states:

The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area. Any such armed attack and all measures taken as a result thereof shall immediately be reported to the Security Council. Such measures shall be terminated when the Security Council has taken the measures necessary to restore and maintain international peace and security.\footnote{14}

Applied to the cyber domain, the two principles reflect an integrated approach that enables the meeting of what should be a primary interest of the potential targets of a cyberattack: either preventing it in the first place, or, in the event of an actual attack, minimizing its impact. From the perspective of the potential victim, for instance a customer of a large financial interest, this would reflect recognition of the duty to protect and reflect implementing measures to meet that obligation. Much in the same way that governments are obliged to protect their civilian population.

The concept of “customer as partner” in combating cyberterrorism whereby a triangular relationship is created between the corporation—the client/customer—law enforcement is far more effective than unnecessarily minimizing—if not denying—the threat.

![Diagram of customer as partner relationship]

For a corporation, it is cheaper\footnote{15} to react or handle a hack as opposed to spending money on defense and protection. The number of corporations which, in the aftermath of a hack—successful or otherwise—come forward immediately and say “we’ve been hacked, we are vulnerable, let’s learn from this” is minimal. That is a lost opportunity for both that company and others. It represents a double victory for the hackers\footnote{16}: successful penetration and failure of corporations to learn from each other. While each corporation has interests it must protect, there are sufficient similarities and common values that would facilitate—and welcome—sharing information regarding successful or attempted penetration.

Nevertheless, the reality is that most corporations are extremely hesitant to come forward and acknowledge that they have been hacked. To that end, they are not forthcoming with customers, shareholders, and law enforcement. In addition, they are inhibiting or preventing other corporations from protecting themselves. Perhaps there is a shame element that, despite enormous expenditures on firewalls and IT teams, vulnerability still exists. However, given
the nefariousness of cyberattackers, and the damage caused, it would behoove corporations to put aside that shame factor, and be much more forthcoming.

To that end, it is recommended that failure to share information be deemed a criminal act. The framework provided by the Cybersecurity Information Sharing Act provides the platform for doing so. The reasons for this recommendation are articulated below.

— *Let us consider customers* As a customer of a company that has been hacked, you *immediately* want to know that your privacy is at risk. It is your right to know that “*someone who you did not authorize*” is in possession of your social security number, your health information, and other information of a deeply personal nature. Corporations must have the *immediate* obligation to notify their customers.

— *Let us consider shareholders* Shareholders have significant financial interests at stake. That said, there are significant financial considerations in determining when—and how—to inform shareholders of an attempted or successful cyberattack. Clearly, corporations carefully weigh the impact of a negative response. Nevertheless, corporations must have the absolute responsibility to be as forthcoming as possible to shareholders, and immediately.

— *Let us consider law enforcement* The faster information is provided to law enforcement regarding a cyberattack, the more effectively law enforcement can begin the process of identifying who is responsible. The attacked corporation, ostensibly, has a vested interest in assisting law enforcement; nevertheless, repeated delays in reporting suggest conflict within corporations regardless of ostensible benefits accruing from immediate reporting and information sharing.

To facilitate an institutionalized reporting process we turn our attention to enhanced cooperation among parties directly affected by a cyberattack on a corporation.

**Cooperation to What Extent**

A comment and response in the tabletop exercise referenced in the introduction emphasize the complexity of this issue. The dialog can be summarized as follows:

— Amos N. Guiora (ANG): When do you inform customers that you have been hacked, thereby potentially compromising their privacy?
— CEO: Only when the matter is resolved; never while addressing the potential hack.
— Participant/customer: I would want to know as soon as you (the company) know; that way I can take measures to protect myself.
— CEO: My focus will be on resolving the issue rather than informing customers.
— Participant/customer: Meaning you will not enable me to protect my privacy even though you know it is potentially compromised?
— CEO: Correct.
— ANG: Would you inform competitors (in the same industry) that you have been hacked in order to give them “heads up”?
— CEO: No.
— ANG: Why?
— CEO: They’d use it to their benefit, thereby weakening my financial position.
— ANG: Would you inform law enforcement, local or national?
— CEO: That wouldn’t be a priority.
I found the CEO impressive in his candor; it was also clear his company’s cyber protocol was sophisticated, reflecting much thought and understanding. That is to his credit. However, I was similarly struck by an unwillingness—well articulated—to cooperate with three distinct actors: customers, competitors, and law enforcement. His answers reflected a “go it alone” approach. This was reinforced when a participant shared with me the following: a chief information security officer (CISO) stated he would share information during an attack only with those corporate entities that he knows and trusts personally.

Business considerations, financial interests, competition, and trade secrets are offered as primary reasons for such an approach. On the other hand, long-term strategic thinking suggests a different approach is essential to successfully countering cyberattacks. That long-term, more strategic approach is primarily predicated on the recognition of a “common enemy” and “combining forces” will significantly enhance the development of more effective countermeasures. The cooperation model suggests cooperation between corporations and between corporations and law enforcement.

Interaction with law-enforcement officials highlighted the lack of cooperation on three distinct levels regarding cybersecurity: corporation-to-corporation, corporation to law enforcement, and law enforcement to law enforcement.

What should corporations do upon discovering that a penetration has occurred?

— conduct an honest assessment of “damage done;”
— take every measure to protect existing data;
— as quickly as possible inform clients and customers;
— immediately inform law enforcement and work hand in hand with them to minimize the damage;
— inform the public;
— cooperate with other corporations, both in order to minimize internal harm and to prevent future attacks.

Undertaking these measures requires sophistication, teamwork, and an ability—and willingness—to analyze internal vulnerabilities, which requires possessing both the necessary tools and competent team members. The willingness, as important as it is, must be complemented by a requisite skill level. Immediate reactiveness, which requires integration of teamwork, competence, and willingness, minimizes future harm. However, the primary takeaway from examining how corporations react to successful hacking is a failure to
respond quickly. Whether the failure to respond quickly is deliberate or not is an open question; nevertheless, it demonstrates the challenges in not being able to identify the penetration quickly, and a failure to inform the customer. Both issues—the challenges and informing the client—were commented on by a reader of an earlier draft who noted the following:

Today we are dealing with determined and talented threat actors (hackers), highly skilled and motivated with time and nation-state backing to perform their tradecraft (hack) on a targeted system. Yes, some corporations may have appeared to be easy, but that is the news reporting too. The news is not going to report on a corporation’s internal change management, vulnerability management, asset management (hardware/software), IT security processes... these entities are silos/departments that have to come together in order to work a hacking event. And with some recent hacks, the threat actors deliberately obfuscate their activities in order to avoid detection. They are ahead of any system alerting on activity; this is above and beyond virus protection as they portray a normal user on the network, something virus protection does not pay attention to. Whether to inform a customer while an investigation is ongoing, well that is a double-edged sword. Till the full extent of the exposure is determined, advising customers can harm the investigation efforts, especially if you want to see if the threat actor is still active in the system, which is one way of catching him. And the corporation has to determine the full extent of the customer exposure. As we have seen with Equifax [which suffered a data breach in 2017], it had to advise the public over and over about further details of the hack.18

Regulatory requirements in the financial industry are now settling on how long you can wait till you advise the public of a hack, and the customers “should” be notified prior to the news/public. The consequences are significant: continued vulnerability; continued threat to customers; potential civil liability in the context of insufficiently protecting customer information/privacy; and liability for failing to notify the customer of the breach and the consequences to the customer.

While focusing on possible lawsuits is understandable, the more important issues are the failure to protect and the failure to inform. The reasons are clear:

— potential customers will hesitate to “bring their business” once they discover failure to protect/failure to inform;
— existing customers may take their business elsewhere if they conclude all reasonable measures were not taken to protect their privacy;
— the broader public will view the corporation negatively in the context of a failure to eliminate cyberattacks and minimize cyber risks BUT the most powerful criticism will be failure to tell the truth.

What, then, does that mean for corporations? In stark terms, corporations need to be much more forthcoming. I think there are clear benefits accrued to a corporation in publicly discussing when it has been breached. While the public will express concern in the aftermath of a reported attack, the more long-term reaction will be an appreciation for “speaking the truth.”

Additionally, the knowledge of how a breach occurred, when shared with the public, could prevent a future breach in a different corporation in a similar manner. This change in behavior can have a large positive impact that could potentially affect millions of consumers.
Towards a New Enlightenment? A Transcendent Decade

That truth needs to address the following:

— an acknowledgment of the penetration;
— list of measures undertaken to immediately address the penetration intended to protect customers;
— list of measures intended to protect customers in the future;
— reaching out to other corporations in the context of “information sharing;”
— implement aggressive counter-cyber-measures.

There is risk in this “open” approach; however, from a cost-benefit perspective, the “upside” ultimately outweighs the “downside.” While an element of vulnerability results from openness and candor, an approach emphasizing implementation of measures to prevent future attacks, and honesty with customers and the public, reflects the following: (1) better customer protection; (2) better critical infrastructure protection; and (3) better protection of “larger interest.”

Most corporations are extremely hesitant to come forward and acknowledge that they have been hacked. To that end, they are not forthcoming with customers, shareholders, and law enforcement.

Risk mitigation predicated on honesty and proactive aggressive measures is a win-win. From a legal perspective, in terms of minimizing potential impacts of civil suits, a policy of candor and honesty predicated on “we are taking measures to minimize exposure of personal information and learning from it and working hand in hand with customers” will mitigate the possibility of law suits against corporations. Such an approach indicates, from the corporation’s perspective, a willingness to engage different audiences, particularly customers and law enforcement.

For law enforcement to be able to effectively protect corporations, it requires a fundamental change in the context and concept of cooperation and it requires corporations to be more forthcoming to law enforcement.

The following caveat was offered by a reader:

Are you thinking ‘law enforcement’ has the cyber talent to discover vulnerability and how to address it? Who would be the one that could do this: local, state, or federal? The issues when LE [Law Enforcement] is involved: LE is mostly after the ‘who’ committed the hack, whereas the
corporation is focused on getting back into business. Those are competing agendas, one reason LE is not called immediately is that the company is trying to do this work without the distraction of LE. Just because they are LE, does not mean they have the cyber talent readily available to perform an investigation quickly. And depending on the business, the corporation might not have the ability to not be open for business while an investigation is happening.20

This cooperation will facilitate law enforcement’s understanding of where the hack was, where the specific vulnerability was, and would enhance addressing the points of vulnerability. This can only occur if corporations are much more forthcoming. In that sense, the burden is on them. The failure to work hand in hand with law enforcement prevents development—much less implementation—of a sophisticated, corporate–law enforcement cooperation model. Because of the vulnerability to individuals resulting from a successful cyberattack, there is a pressing need for “out of the box” approaches to law enforcement.21

Cooperation will facilitate law enforcement’s understanding of where the hack was, where the specific vulnerability was, and would also enhance addressing the points of vulnerability

However, the condition to that approach is the willingness of corporations to view law enforcement as full partners, both preemtively and reactively. To that end, a corporate governance model for cybersecurity is required; while presently untapped, the burden on its development rests with corporations. Law-enforcement officials repeatedly articulated a willingness to closely work with corporations in the development and application of that model, which would emphasize; 22

— threat identification;  
— vulnerability minimization;  
— resource prioritization;  
— cost-benefit analysis;  
— asset protection;  
— enhanced understanding of points of vulnerability;  
— minimizing impact of future attacks.  

So, what do corporations need to do?  
Corporate leaders can sit around the table and have endless discussions about points of vulnerability, but the single most effective mechanism to truly understand those points of vulnerability is by conducting sophisticated simulation exercises either in-house or with experts to identify where the corporation is vulnerable.

I would warmly recommend law enforcement have a seat at the table along with other corporations and government officials. Otherwise, the exercise will be akin to an echo chamber, largely ineffective in terms of articulating and implementing an effective cybersecurity policy. I fully understand and respect that for many corporate leaders the idea of institutionalized cooperation with law enforcement, government entities, and other corporations/competitors raises red flags.23
Former managing director of Equifax, Richard Smith, prepares to testify before the United States’ Senate’s Banking, Housing, and Urban Affairs Committee on October 4, 2017. Smith resigned after it became known that cyber pirates had attacked the credit-standing firm and stolen information on almost 145 million US citizens.
However, given the cost, impact, and nefariousness of corporate security hackers, I do not believe that there is any alternative other than to rearticulate the corporate cybersecurity model.

The following are questions to consider for understanding the nature, and extent, of cooperation.24

— Should corporations be responsible for their own cybersecurity?
— Should the government force corporations to have a cybersecurity policy?
— Should corporations be required to share relevant cybersecurity information with other corporations, including competitors?
— Should corporations be required to report to law enforcement when they have been attacked?
— Should corporations have a duty to report a cyberattack to shareholders?

As the discussion above illustrates, cooperation is not a “given.” Far from it. However, dismissing it out of hand is too easy. The challenge is to create workable models whereby a proper balance is created that protects the distinct stakeholders without causing unintended financial harm to a cooperating entity. Re-articulated: the challenge, in determining the extent of cooperation, is to convince corporations that cooperation—with customers, law enforcement, and competitors—is advantageous, both tactically and strategically.
Tactical benefit reflects short-term gain; strategic benefit results in long-term gain. The two are not necessarily synonymous. They can be mutually exclusive. In considering adoption of a cooperation model, the dilemma can be posed as a cost-benefit thought experiment.

To move the ball forward it is essential to consider four different corporations: the two charts below are intended to facilitate understanding of the relationship between corporations and cooperation.

Data Breach in a Corporation
(Corporation with Significant Protection)
Corporation A assumes great responsibility in the amount of information it accesses. Therefore, Corporation A invested significant money and time in cyber protection. It works closely with law enforcement, engages in employee trainings, and actively employs several data experts to protect it against a cyberattack.

Now, despite all its best efforts, Corporation A has been breached. Similar to Target or eBay (which suffered data breaches in 2013 and 2014 respectively), over 100 million customers have now been affected by the breach. The question then becomes, what is the next step, and who has a responsibility in the aftermath of the attack? But, since Corporation A took significant measures to protect itself from a cyberattack, and fell victim anyway, the question becomes should the compensation or retaliation be greater since it took steps to try to prevent the event?

Either way, the first thing that must occur when a company is the victim of a cyberattack is notification to law enforcement. Although companies may not want to report, for fear of customer doubt or repercussion, this must be a legal obligation. Without notification to law enforcement, law enforcement is unable to create patterns or algorithms that could prevent future attacks.

The next thing to consider is whether Corporation A has absolved liability because it took
the necessary precautions and, through no fault of its own, still fell prey to a cyberattack. This is difficult to answer and one that may not be fully answered until additional, relevant legislation is put into place.

**Corporation B** Corporation B, like Corporation A, is one of the largest corporations in America. From that, Corporation B assumes great responsibility in the amount of information it accesses. However, Corporation B has not invested significant money or time in cyber protection. Rather, its Board of Directors, which is actively aware of the threat of cybersecurity, voted to delay any financial or personnel investment in the pursuit of cyber protection because it is expensive, and the corporation is in the business of making money. This issue is the pinnacle of the protection versus profit debate.

Now, imagine Corporation B has been breached.

Similar to Target or eBay, over 100 million customers have now been affected by the breach. The question then becomes, what is the next step, and who has a responsibility in the aftermath of the attack? As mentioned earlier, the United States government may take it upon itself to get involved when corporations exist of a certain size, as it has done previously. But the question becomes, since Corporation B did not take significant measures to protect itself from a cyberattack, and fell victim, should the compensation or retaliation be less since it did not take steps to prevent the event?

Law enforcement should have a seat at the table along with other corporations and government officials. Otherwise, the exercise will be akin to an echo chamber, largely ineffective in terms of articulating and implementing an effective cybersecurity policy.

As mentioned before, either way, the first thing that has to occur when a company is the victim of a cyberattack is notification of such an attack to law enforcement. Usually, most companies do not want to report, whether from fear of customer doubt or shareholder perception, or other repercussions; this needs to be a legal obligation. The next thing to consider is whether Corporation B is increasingly liable for its negligence.

Unlike Corporation A, its liability cannot be absolved in any way because it did not take necessary precautions. Despite likely recommendations from the Chief Intelligence Officer, or other employees in the corporation, Corporation B chose profit over protection, and became an easy target. The question then becomes, due to its negligence, should the compensation or protection post-attack be less? That is a question that will need to be determined by future legislation.

**Corporation C** Corporation C, unlike Corporations A and B, is one of the smaller corporations in America, a small-town business held closely by a few family members. From that, Corporation C assumes significantly less responsibility in the amount of information it accesses.

However, like Corporation A, Corporation C has invested significant money and time in cyber protection. It works closely with law enforcement, engages in employee training, and actively employs a data expert to protect itself against a cyberattack.

Despite Corporation C’s best efforts, it has been breached. However, unlike Corporations A and B, the breach does not affect over 100 million customers. Rather, the breach affects simply 5,000 individuals. The question still becomes, what is the next step, and who has
a responsibility in the aftermath of the attack? It is safe to assume that the United States
government is less likely to get involved when the breach is so minimal, as compared to the
Corporation A and B scenario.

However, the question to be asked is, since Corporation C took significant measures to
protect itself from a cyberattack, and fell victim anyway, should it be compensated or sup-
ported in some way, more so than a company that made no effort to protect itself against a
cyberattack?

Corporation C, despite its small size in comparison to Corporations A and B, must still
have a legal obligation to report to law enforcement when it is the victim of a cyberattack.
After which, the next question to consider is whether Corporation C absolves liability
because it took the necessary precaution and, through no fault of its own, still fell prey to a
cyberattack.

Corporation D  Corporation D, unlike Corporations A and B, but similar to Corporation C, is
one of the smaller corporations in America, a small-town business held closely by a few family
members. From that, Corporation D assumes significantly less responsibility in the amount
of information it accesses. However, like Corporation B, Corporation D has not invested
significant money or time in cyber protection.

Rather, the corporation decided to delay any financial or personnel investment in the
pursuit of cyber protection because it is expensive, and the corporation is focused on mak-
ing money. This issue, as demonstrated with Corporation B as well, is the pinnacle of the
protection versus profit debate.

Due to Corporation D’s lack of effort, it has been breached. However, unlike Corporations
A and B, the breach does not affect over 100 million customers. Rather, the breach affects
simply 5,000 individuals. The reasoning and considerations now become very similar to the
questions that occurred with the breach in Corporation C. The question still becomes, what
is the next step, and who has a responsibility in the aftermath of the attack?

It is safe to assume that the United States government is less likely to get involved when
the breach is so minimal, as compared to Corporations A and B. But the question becomes,
since Corporation D did not take significant measures to protect itself from a cyberattack,
and fell victim, should the compensation or retaliation be less since it did not take steps to
prevent the event?

Corporation D, despite its small size in comparison to Corporations A and B, must still
have a legal obligation to report when it is the victim of a cyberattack. The next question to
consider is liability. Unlike Corporations A and C, its liability cannot be absolved in any way
because it did not take necessary precautions.

Despite likely recommendations from the Chief Intelligence Officer, or other employees
in the corporation, Corporation D chose profit over protection, and became an easy target.
The question then becomes, due to its negligence, should the compensation or protection
post-attack be less? That is a question that will need to be determined by future legislation.

The Good, the Bad, and the Ugly of Cooperation

Easier said than done.

That oft-repeated maxim applies to the corporation model that is the underlying premise
of this article. Corporation is not cost-free. There is understandable concern regarding vul-
nerability, exposure, and unwarranted risk, perhaps with minimal “upside.”
The CEO referenced in the section “Cooperation to What Extent” was eloquent in his conciseness; cooperation, for him, is an absolute nonstarter. I heard a similar theme from other corporate leaders. To my surprise, a similar refrain was articulated by federal law-enforcement officials when asked whether they would cooperate with local enforcement. The answer was brief, and embarrassing: “We don’t cooperate with local law enforcement.” Embarrassing because the brief, actually brusque, answer was given to local law-enforcement officials at a meeting in my presence. However, in its brevity the official highlighted an important—albeit troubling—concern: the extent to which law enforcement cooperates among itself, much less with external entities.

This struck me then, and continues to this day to reflect short-term arrogance, putting one’s own “turf” ahead of the public good. In a recent meeting with federal law-enforcement officials, I was assured such a response would be met with great disfavor by senior officials. I hope that is the case.

Assurances aside, it is important that cooperation—among local, state, and federal officials—be institutionalized, not left to the whims and fancies of particular officials. That seems to serve the public interest and public good which is the primary obligation of law enforcement. Institutionalizing cooperation—among the various stakeholders—requires time, dedication, and resources. It is not a “given” for actors representing different cultures, norms, and mores to immediately—and instinctively—have protocols in place easily facilitating cooperation. This will require a concerted effort.

Assurances aside, it is important that cooperation—among local, state, and federal officials—be institutionalized, not left to the whims and fancies of particular officials. That seems to serve the public interest and public good which is the primary obligation of law enforcement

Resources must be allocated for such implementation; common language must be found; common goals need to be identified; understandable hesitation, reticence, and skepticism must be held in abeyance. This requires a dedicated effort by all involved; the motivation for doing so must focus on the larger good, rather than temporary costs and burdens. Otherwise, the undertaking falls flat.

Conversely, the positives of cooperation far outweigh the conflicts and tensions. This is viewed from the perspective of public safety. That, frankly, must be the most important consideration in weighing-up the adoption of a cooperation model.

Final Word

The theme of cooperation has been the centerpiece of this article. That is not by chance.

I served as legal advisor to a congressional task force under the auspices of the House Committee on Homeland Security addressing US Homeland Security policy. The principle of cooperation was uppermost in my mind in the development—and implementation—of effective cyber countersecurity. The discussion in this paper is intended to facilitate the reader’s understanding of the need to develop institutionalized cooperation and, simultaneous to that, recognizing the difficulty in such an effort.
Former United States National Security Agency surveillance center in Bad Aibling, south of Munich. In June 2013, Edward Snowden’s revelations of massive surveillance programs by the NSA thwarted diplomatic relations between the United States and its European partners.
The reasons are varied; whether financially driven, as is the case with corporations, or “turf” and budget, as was explained to me by law-enforcement officials, the consequences are clearly predictable. The beneficiary of a consistent lack of cooperation is the wrongdoer; the victims are plentiful. The lack of cooperation theme was consistently expressed to me while writing my book. It was repeated when conducting the tabletop exercise. In all three instances—the US Congress, book research, exercise—those with whom I engaged were uniform regarding cooperation, whether proactive or reactive: the notion does not fit their “model.” The mantra was repeated a sufficient number of times.

This was in direct contrast to a meeting I held in Israel with a leading cyber expert. The conversation on that occasion was extraordinarily insightful, shedding light on the intersection between national security and cybersecurity. More importantly, it highlighted the crucial role government can—and should—play with respect to cyber. Our conversation focused on questions of law and policy; the technical matters, while undoubtedly important, were not at the forefront of what we discussed. What particularly impressed me—in the context of cooperation—was the enormous benefit accrued when public and private sectors joined forces and cooperated.

That is not intended as a gloss over inevitable tensions, jealousies, and competition between the two. It was, however, in sharp contrast to the discussions I had with US law-enforcement officials. The difference between the two approaches was jarring. The consequences are obvious. It is for that reason that the theme of cooperation occupies such importance in my book: Cybersecurity: Geopolitics, Law, and Policy.

The principle of cooperation should prevail in the development and implementation of effective cyber countersecurity

Many of us have been victims of harm, whether on a personal, professional, or community basis. Our vulnerability to cybercrime is well documented; there is no need to repeat the litany of incidents, ranging from the irritating to the truly catastrophic.

It is clear that individuals in groups, worldwide, are dedicated to continuously seeking ways in which to use cyber to their advantage and to our disadvantage. There is, truly, an “us–them” with respect to cyber. The harms posed by cybercriminals and cyberterrorists are significant; of greater concern are the future harms they are, undoubtedly, planning to impose on society. Of that, I have no doubt.

There is a profound lack of consensus regarding the question of government involvement. Perhaps as a direct reflection of my background in the Israel Defense Forces, I am—frankly—baffled—by the hesitation repeatedly expressed to me regarding the role of government in cyber protection. I believe that cyberattacks need to be perceived as similar to physical attacks.

The consequence of that, for me, is clear: an attack on an American corporation warrants government response. While that requires the cooperation discussed above, the benefits—short and long term alike—significantly outweigh any negative consequences regarding government “over” involvement. Frankly, the stakes are too high to resort to tired clichés and irrelevant mantras regarding privacy concerns. That is not to minimize the question of privacy—NSA leaks disturbingly highlight the reality of government intrusion—but it is to suggest that cyber threats require a balanced and nuanced approach. Summarily dismissing government involvement is shortsighted and ultimately counterproductive.
Hand in hand with government involvement is the question of self-defense and collective self-defense. In actuality, the two are directly related and cannot be separated one from the other.

Self-defense is a critical question in the cyber discussion. The inquiry is whether the nation state owes a duty to corporations and individuals who have been victimized by a cyber attack. It is not an abstract question, but one rather intended as a concrete query.

There are great risks in imposing “response” burdens on the nation state in the aftermath of a cyberattack. This is possible only if the cooperation model is adopted. If all potential—and actual—targets of a cyberattack are to be “stuck” in a noncooperation paradigm, then the forces of darkness are the obvious winners. That is clear.

Nevertheless, enough opposition has been consistently articulated—by the private and public sector alike—that it must give pause. That opposition, and certainly skepticism, are legitimate and cannot be dismissed with a casual wave of the hand. And yet.

And yet, the persistent threat posed by potential cyberattacks, not to mention the actual impact in the aftermath of a successful attack, warrants careful consideration of a proposal to legislatively mandate cooperation requirements and obligations. Given the consequences of a successful attack, cooperation among the different actors outlined in this paper would have the potential to minimize the consequences of a particular impact.

At the very least, cooperation would contain the consequences by ensuring that other impacted entities—yes, competitors—would be positioned to implement, proactively, protection measures while simultaneously ensuring that law enforcement—national and local—be fully engaged in minimizing the fallout.

There are different mechanisms for determining the viability of such an undertaking. As was made clear to me in the tabletop exercise, communication and dialog are excellent starting points. To bring the different actors together, to explore how to respond and—hopefully—minimize the fallout of an attack is an important step. It is recommended that such exercises include a wide range of participants, including elected officials, law enforcement (local, state, and national), corporate leaders (large and small; private and public), municipal officials, representatives of consumer advocacy groups, and members of the public.

Such an undertaking will enable the community—defined broadly and narrowly—to determine what is the best mechanism to ensure cooperation in the face of a cyberattack.

That is a discussion we must have. Postponement in exploring cooperation models is far from “cost-free”; quite the opposite: it comes with great cost. The existing measures provide an effective platform from which to build. The challenge to do so is great. The time to do so is now.
Acknowledgments

I owe many thanks to the following individuals who graciously read through previous drafts and made insightful comments and suggestions that significantly strengthened the final product; needless to say, all mistakes, errors, and omissions are exclusively my responsibility:

Anne-Marie Cotton, Senior Lecturer in Communication Management, Artevelde University College, Ghent (Belgium), Jessie Dyer JD (expected 2019), S. J. Quinney College of Law, University of Utah, Brent Grover, President, Brent Grover & Co, Professor Daniel Shoemaker, University of Detroit Mercy, Judy A. Towers, Head of Cyber Threat Intelligence, SunTrust Bank.

Notes

1. A reader of an earlier draft suggested this statement applies to 99% of business executives with whom he has interacted.
3. Due to “Chatham House” rules, the identities of participants and their comments may not be noted; the exercise was conducted under the auspices of the National Cyber Partnership.
4. For a thoughtful discussion regarding the Social Contract, please see https://www.iep.utm.edu/soc-cont/.
10. Domestic issues: not only stealing ID but also property, as illustrated in this commercial: https://www.youtube.com/watch?v=_CQA3X-qNgA.
11. A reader of an earlier draft noted: “A lot of people would say that cybersecurity is nothing more than risk management”; e-mail in my records.
12. Illustrated by the Belgian agency: https://www.youtube.com/watch?v=jop2I5u2F3U.
15. A reader of a previous draft noted the following points: based on which evidence? What about negative impact on reputation? Loss of confidence? Intangibles compared to financial figures of costs to redesign the “firewalls”? However, brand equity has become an important element too.
16. A reader of a previous draft noted: wonderfully developed by Andrew Ehrenberg (London School of Economics) in his double jeopardy theory applied to big companies versus small ones; the small ones are twice “victims” of their size; although they invest, the big are investing more = they have to invest proportionally X more to get a smaller result.
17. In accordance with Chatham House rules.
18. E-mail exchange with reader; e-mail in author records.
19. See articles by Finn Frandsen, Timothy Coombs, Robert Heath, Winni Johansen on this theme, for example: “Why a concern for apologia and crisis communication?” Frandsen and Johansen have just published their latest theoretical developments in: Organizational Crisis Communication: A Multivocal Approach.
20. E-mail exchange with reader; e-mail in author records.
21. The following caveat was offered by a reader of an earlier draft: “Besides awareness—this also takes a lot of time… We are only in the foothills of producing the talent and people in LE rarely have the bandwidth to incorporate another skill set”; e-mail in my records.
22. A reader of a previous draft noted: this is a good statement, but I have not seen LE be business savvy enough to perform the articulation of the items in the list. This is where industry regulators step in with the knowledge to provide these items, not LE. And they are advising DHS as they are setting the same standards in the list.
23. A reader of a previous draft noted: this is being done as we speak in the US financial sector, and the businesses were candid in their “whys” of remediation processes while all of us that represented regulators/LE were waiting to be told. Also for a company to determine a hack has occurred instead of just a system cliched can take days to determine, especially if the threat actor has modified system logs and deleted their code/actions/steps. Making things look like normal system issues is a sophisticated threat actor. Hoping this ability does not become easy for an “everyday Joe” threat actor.