A Cyber Federal Deposit Insurance Corporation?

Achieving Enhanced National Security

By Dante Disparte

Of the emerging man-made risks affecting U.S. national security, cyber threats have enjoyed the most attention and resources from national security leaders and policymakers. And yet, cyber threats remain one of the most complex risks to address given their amorphous, highly fluid, and extra-territorial nature. This makes it difficult if not impossible to quantify the national state of readiness and, in these fiscally constrained times, the return on investment from the billions spent each year on cybersecurity. Five gaps conspire to make achieving a state of enhanced cyber resilience complex if not impossible. These include a yawning talent gap to the tune of millions of people; a technological gap predicated on managing a risk that evolves according to Moore's law; a financial and economic gap leaving trillions in value at risk with no generally accepted way to measure this value; an alignment gap in terms of policy harmonization and cooperation inside the United States and around the world; and, finally, a gap in patience and the speed of markets. This article delves into the evolving cyber threat landscape and outlines ways of understanding and bridging these critical gaps.

Shared Risk, Shared Defense

The United States enjoys an undeniable economic and national security advantage from being the birthplace of the internet and, with it, the midwife of the digital age. These advantages have been reaped since the early 1990s, where the road to building a 21st century economy began—connected at every turn, person, node, and device to a worldwide web of risk and reward. The United States has since remained the world's economic supremo and, for a period after the global financial crisis, the only functioning cylinder in the global economy. But will this *pax digitalis* hold or is U.S. national security and economic prevalence waning because of the blowback from our marvelous creation?

Today, it is hard to imagine a world without the internet and without the hyper connectivity it has enabled. Indeed, technology titans such as Facebook's Mark Zuckerberg and Amazon's Jeff Bezos look every bit the part of 21st century business statesmen.[1] Speculation of presidential runs from Silicon Valley's independently wealthy and decidedly pro-digital elite suggests that the line between public policy, the

Mr. Dante A. Disparte is founder and Chief Executive Officer of Risk Cooperative and serves on the board of the American Security Project.

digital commons, privacy, and security may be forever blurred—especially in the eyes of millions of millennials whose newly minted political engagement treats the internet as a utility, and privacy as a tradable right. This is troubling because the world is beset by a growing number of challenges pitting privacy and security advocates against one another, much as we saw with the now infamous case of "Apple vs. the Federal Bureau of Investigation" or in the Snowden leaks, which revealed wide-scale digital eavesdropping on the U.S. public—albeit at the metadata level, as security proponents argue.[2]

Just as privacy and security represent key policy, security, and business tradeoffs, connectivity and national cybersecurity are similarly dialectical choices. On the one hand, the tide of connectivity cannot be reversed. Indeed, with the explosion of connected devices, the so-called Internet of Things (IoT), people seem almost reflexive in their acceptance of a technological front door (and back door) to every tangible item in their life.[3] The annual Consumer Electronics Show (CES), is at once the digital sycophant's dream and the cybersecurity hermit's nightmare, as each connected gewgaw and curio is revealed to a fawning public and a salivating shareholder. According to Gartner, there are 8.4 billion connected devices in 2017, a 31 percent increase over last year. This exponential growth of connectivity, much as we saw with the Dyn exploit that shutdown the websites of major firms such as, Netflix and CNN, IoT will expand both the attack surface area and vectors that can not only take down much of the internet, but exfiltrate sensitive information, cripple critical systems and sow misinformation.[4] Indeed, concerted efforts to exploit our connectivity and obsessive news media cycle still cast a long shadow over the 2016 presidential election and the current administration.[5]

And yet, rolling back the tide of digital connectivity would represent the loss of trillions in economic value in the global economy, accepting that much of what financial markets trade in is notional. Firms like Amazon, which has recently acquired Whole Foods in a $13.7 billion transaction that was quickly netted out by Amazon's share price gains, will command 50 percent of all U.S. e-commerce by 2021.[6] Firms like Facebook have quickly transformed into a service that is fast becoming tantamount to a digital census of more than 2 billion people—growing monthly active users at a rapid rate, many of whom enjoy their solitude in the company of others.[7] Firms like Google are not only synonymous with the web, they have quickly morphed into a modern *keiretsu* under its new *nom de guerre* Alphabet, to deploy their considerable human, technological, and financial capital toward redefining the future. Firms like Apple and Tesla are similarly poised to not only command the present, but very much shape the future—one where the digital divide between man and machine is being bridged by wearables, augmented reality (AR), and artificial intelligence (AI). In this near-future the *uncanny valley* no longer scares us and the very morality, proximity, and humanity of warfare is being lost to drones and digital threats.[8]

Modern commerce is very much a tale of creators and accelerators. Where iconic firms like Ford took more than century to reach $45 billion market capitalization, Tesla—a comparatively young upstart of a mere 14 years of age—has overtaken Ford in valuation despite Ford's 100 year-long head start.[9] With this shift in what can be described as digital industrial production comes a raft of unforeseen exposures, such as those posed by mechanical and process autonomy. Driverless cars and self-driven features are already present in thousands of vehicles on U.S. roads and around the world. Indeed, the concept of self-driven road convoys of large tractor trailers is well beyond the conceptual and piloting stage and now entering commercial viability.[10] With the advent of industrial autonomy comes a profoundly vexing era of redefining

individual responsibility, third party liability and product safety standards—one which many a trial attorney and jurist are preparing to litigate. In the highest order, this new normal should also herald the emergence of digital democrats, citizens and politicians who are not only conversant in technology, but possess the technical virtuosity to steer the world with their vote and vision while navigating the potential disruption of hundreds of millions of jobs, thousands of industries, all asset classes, and national security.

The robber barons of the Industrial Age unwittingly triggered man-made climate change through their ravenous pursuit of a carbon-based economy. Likewise, the early adopters of the internet have gained incalculable wealth while unwittingly opening a Pandora's Box of cyber threats. The proponents of IoT, industrial automation, and AI are exposing the world to an increasingly complex and interconnected new normal that even has many of its greatest beneficiaries, such as Elon Musk, Tesla's CEO, and Eric Schmidt, Google's former CEO and Chairman of its parent company Alphabet, sounding the alarm.[11] While Musk is worried for humanity's very survival, which is why he is so feverishly attacking the internal combustion engine, AI, and commercial space flight, Schmidt has a decidedly more sobering—if somewhat convenient—assessment that data is the new oil, for which countries will likely go to war.[12] The opening salvo of this grim new normal was very much the Sony Entertainment cyberattack in 2014, which experts suggest was perpetrated by North Korea's cyber warfare arm under the banner "Guardians of the Peace."[13]

Sony Entertainment drew the ire of a nation-state by the none too flattering film *The Interview*, which, among other transgressions, depicted North Korea's dictator, Kim Jong-Un as an imbecilic character who was eventually assassinated. Allegedly in response, a full-scale cyber onslaught was launched against Sony Entertainment and, in many respects, its entire value chain in an effort to thwart the film's release. As the release date neared, a very sophisticated business model ransom attack was carried out with the threatened release of sensitive material, crippling systems and, ultimately, threatening movie theaters and movie goers, among others. This attack not only pitted Sony Entertainment against a nation-backed actor, the equivalent of having financial services firm Cantor Fitzgerald go after al-Qaeda after 9/11, it pitted President Obama against Sony's executives, in his public exhortation that they not give in to pressure.[14] In the end, this may have been a Pyrrhic victory for North Korea, as a film that would have been forgotten, is now documented in history books, and millions more viewed it as a result.

While the case was eventually resolved, it augured a new era of cyber risk and the increased likelihood of cyber warfare and terrorism. Our Achilles' heel was laid bare around five critical gaps in our national cybersecurity posture. The first, which was revealed in Sony's case, was the lack of a competent—literate and numerate—cybersecurity talent pool. The second was a clear technological gap not only in the defenses applied in this case, but in the clear double standard in who was to be covered by cybersecurity rules inside Sony and elsewhere. The third was the economic gap that emerged as the financial losses from this event were a mere rounding error in Sony's global earnings, but a material threat downstream in movie theaters and among actors, who not only feared for their privacy, they feared being caught up in the dragnet. The final two gaps are perhaps the most important, especially as the purview of response was in the hands of the U.S. Government and not a private enterprise. That is the lack of alignment on national security policies and how they interplay with the private sector. Finally, as with all man-made risk, of which cyber threats are one, the attacker has the benefit of patience and agency, while our economy blindingly moves forward at the speed of markets.

Talent Gap

Beyond Binary Code

For a risk that often emanates between the keyboard and a chair or through the greedy or nefarious motives of insiders, talented people are a critical link in the chain of cyber resilience. Underscoring how vital a "neural safety network" can be, the exploit of the SWIFT banking system, in which cyber criminals absconded with more than $80 million from Bangladesh's central bank accounts, was halted by an alert clerk at a corresponding bank in Germany. In this case, a heist that was nearing $850 million in attempted withdrawals was stopped because the clerk noticed the word "foundation" was misspelled and promptly alerted authorities.[15] It is difficult to "machine-learn" this level of pattern recognition and intuition, as most machines are learning that humans are error prone and might have forgiven the misspelling allowing the cyber capers to carry on. More than pattern recognition, risk management relies on culture and value systems, which are uniquely human traits.

Globally there is a cybersecurity talent shortfall of 1.5 million people.[16] The United States is not spared from a yawning talent gap of more than 200,000 professionals who are not only needed to fill existing vacancies in one of the fastest growing fields, but are needed to define the standards of the future.[17] This gap is not aided by an inwardly looking immigration and visa policy, which has diminished the U.S. beacon to the world's most promising professionals. Confronting cyber risk head-on is not merely about binary code, although so few have achieved the level of technical virtuosity needed to fully understand cyber threats and how to manage them. Cyber resilience also requires retooling even the most senior business leaders (from the board room on down) and policymakers on how to set up response, governance, and decisionmaking parameters around a threat that does not respect quorum, is infinitely connected, and can spread like a digital wild fire. The emergence of cyber risk governance executive education is a cornerstone of a safer future.

From Hundreds to Millions

Fighting a digital wild fire requires a digital fire brigade. As the WannaCry ransomware demonstrated during a weekend in 2017, cyber threats can spread across borders and across enterprises with blinding speed. Indeed, three days after news broke of this new ransomware payload that was being delivered using the Eternal Blue tool that was exfiltrated from the National Security Agency (NSA), it had affected systems in more than 150 countries.[18] While the attack and its meager ransom gains, payable in digital currencies like Bitcoin, proved to be a dud, it was nevertheless a major wakeup call that cyber risk was again metastasizing. The other gap revealed by the WannaCry attack was that everyone was in effect

Globally there is a cybersecurity talent shortfall of 1.5 million people. The United States is not spared from a yawning talent gap of more than 200,000 professionals who are not only needed to fill existing vacancies in one of the fastest growing fields, but are needed to define the standards of the future.

calling on the same scarce resource for comfort and resolution—namely, skilled cybersecurity professionals or those masquerading as experts due to paycheck persuasion or hubris.

If WannaCry were a rapidly spreading urban fire, there are simply not enough firefighters to keep properties safe. In addition to the lack of talented individuals, those who are out there are often hamstrung by financial constraints and the lack of leadership comprehension of how vital their roles really are. The cyber literate are often not numerate when it comes to defending the business cases that not only justify their existence, but their desired (or, better yet, required) investment levels. This is compounded by the growing "cyber arms race" taking place among nation-states, the public sector, and private enterprise, which is increasingly viewing cyber resilience as a source of competitive advantage. Imagine if volunteer fire brigades that protect all the "commons" of a city, were corralled by the highest bidders to only respond to their localized emergencies? Undoubtedly, this would make for a truly unsafe city and eventually the embers of the least secure would catch fire in the "safer" parts of town. Indeed, it was a heating and cooling vendor that left Target's technological back door open enabling the exfiltration of 110 million personally identifiable records and customer data points.[19] For this, Target's CEO paid the price of a slow descent with a golden parachute, while the firm continues to grapple with earning back customer trust. The same holds true with cybersecurity standards and the war for talent, which negates the reality that cyber threats are a shared risk for which a shared defense is needed. Simply put, cybersecurity, like urban fire safety requires a collective approach.

Bridging the Gap

As with bridging any span between two points, the first step is to understand the distance between them and the depths below. The cybersecurity talent gap is a critical national security priority. Evidence of this is the fact that most agencies of the U.S. Government, including the ones that are supposed to be the most secure, like NSA, which seems to be in a constant maelstrom of breaches and bad news, are in effect outsourcing much of their work to the private sector.[20] It is important to remember that Edward Snowden—a modern Benedict Arnold to some and a Paul Revere yelling "the big state is coming" to others—was a private contractor with top secret clearance. This personnel outsourcing effort is most vigorous in the cybersecurity and national security domains.

All too often we are learning, with calamitous effects, that cyber risk is as much a people-centric threat, as it is a technological one.

The first pillar in bridging this gap must be the emergence of sober leaders in the public and private sectors who treat cyber risk as a systemic threat.[21] These leaders must break down the organizational silos that relegate cyber risk to their often underfunded and unprepared information technology (IT) departments as a purely technological dilemma. These IT leaders in turn labor under the powerful inducements of hubris and paycheck persuasion. All too often we are learning, with calamitous effects, that cyber risk is as much a people-centric threat, as it is a technological one. For this, well-trained people must become a critical link in the common chain of cyber resilience.[22] Attracting this workforce in the United States and from around the world requires confronting the algorithmic hiring patterns

that dominate talent development today. All too often recruiters or machine-learning algorithms are weeding out viable candidates for the lack of undergraduate or graduate education, in the search for "safe bets."

Similarly, the credentialing and skills development options available to the workforce are often too costly, unwieldy, or they labor under impractical, dated curricula that fail to keep pace with a risk that evolves according to Moore's law. Standing up an adequate cybersecurity fire brigade and its rank and file leadership will require tradeoffs and an uncomfortable degree of fluidity of talent and information sharing between the military, government, private sector, and academia. Vitally, a common lexicon around cyber risk governance is beginning to emerge, wherein senior leaders are beginning to realize that they are all too often the only ones left in the smoking crater of these intangible threats. Hitting third rails, like the Sony Entertainment breach or the 2016 electoral malfeasance will enable U.S. national security, public policy, and private sector leaders to begin to course correct and address our cybersecurity talent shortfall.

Technology Gap

Unicorns and Other Mythical Creatures

When it comes to cybersecurity the concept of a perfect technological cure-all is a near impossibility. This calls into question the investment thesis and inflated market valuations of many technology solutions purporting to offer a digital approach to cyber hygiene. This thesis and many aspects of the flood of capital and balance sheets that are on-risk in the cybersecurity market may very well produce a range of correlated losses or a complete crash.

Both the adversaries they face and the technologies that are used to deliver cyberattack payloads have the advantage of patience and Moore's law on their side. Similarly, the Achilles' heel of all technological tripwires is human behavior, which not only drives value-creation in the private sector, it drives decisionmaking and service provision in the public domain. In short, as experts assert, even the best cybersecurity solutions may fall to the four horsemen of human cybersecurity behavior, namely: curiosity, nescience, apathy, and hubris. The counterbalance then is a blended approach to cyber risk management that incorporates a continuum of security, beginning at the values and governance layers and ending with a fortified virtual wall and exit alarms guarding against the exfiltration of sensitive information.

Not Zero-Sum

Just as humans and human behavior can be the weakest link in the cybersecurity chain, over-reliance on technology can be as dangerous by creating a placebo for safety. For many firms, such as JP Morgan Chase, which spends more than $600 million a year on cybersecurity, the amount spent on cyber hygiene has become a proxy for safety.[23] The danger with this approach, however, is that there is a veritable cyber arms and defense race taking place among companies and countries. Rather than viewing cybersecurity as a shared service matching a shared risk, technology solutions have become hyper competitive, hindering interoperability, creating excessive firewalls (real and virtual), and attracting billions in capital from investors and customers chasing yield or reasonable assurances. Notwithstanding this flood of capital in the cybersecurity market, it is safe to assume most organizations in the world are already exposed to latent cyber threats.[24]

The reality with cyber risk and, therefore, cybersecurity technologies, is that it does not have to be a zero-sum proposition. Indeed, as we are seeing all too often with global cyberattacks and patient dark supply chain exploits, the lack of a

common defense leaves many systems vulnerable.[25] Supply chains, critical infrastructure, and the other "commons" the global economy relies on to trade are in the cross-hairs of an insidious, water-like, and incredibly patient menace. Against this threat, technology plays a vital role; however, technology developers and investors must stop chasing unicorns to make handsome short-term returns. Instead, they must emphasize the development and roll out of solutions that are as ubiquitous as the threat. The key attributes of this enduring class of technology solutions is that they fade to the background of human and organizational activity. The more real or perceived interference with the way people work, the higher the likelihood people will find "cheats" around the friction. Like capital, human apathy together with our uncanny ability to not follow rules flows through the path of least resistance.

Supply chains, critical infrastructure, and the other "commons" the global economy relies on to trade are in the cross-hairs of an insidious, water-like, and incredibly patient menace. Against this threat, technology plays a vital role; however, technology developers and investors must stop chasing unicorns to make handsome short-term returns. Instead, they must emphasize the development and roll out of solutions that are as ubiquitous as the threat.

Bridging the Gap

So how do we bridge the multi-billion-dollar technology gap? The first step is to temper the marketing and development standards war raging in the cybersecurity marketplace. The failure of one industry peer, such as a bank with lower security standards, will erode confidence in all banking institutions. Herein lies a major challenge. How many credit unions or community banks can afford stratospheric spending patterns or adhere to onerous regulatory requirements, which are now incorporating steep punitive measures? One solution would be to develop the technological equivalent of a cyber Federal Deposit Insurance Corporation (FDIC).[26] While there are several bodies, such as the National Institute of Standards and Technology (NIST) trying to codify best demonstrated practices for cybersecurity, the challenge is that small-to-medium sized enterprises struggle to overcome a financial and human capital gap to keep pace with these requirements. Furthermore, the changes and best demonstrated practices continue to evolve. The best many business leaders can hope for—subject to IT hubris and paycheck persuasion—is the assurance of a "clean bill of health" from weary IT leaders, who themselves are struggling to keep pace.

A cyber FDIC, like the real FDIC, would be much more than a clearing house for assurance, it would be an entity where risk can be shifted in the aggregate, particularly for smaller and more vulnerable sectors of the economy or for critical infrastructure. Just as identity theft was largely defanged when banks coalesced around a zero-liability proposition

for consumers, the threat of online fraud quickly gave way and the multi-trillion dollar online marketplace was born. As with all risks, we must constantly weigh the costs and benefits of proposed rules and technological solutions and remain especially cautious of so-called technological unicorns promising to be a perfect cyber risk cure-all.

Most of the best practices around cybersecurity are entirely free and based more on education and behavioral hygiene than on technological spending. Keeping technology teams accountable for updating software patches, or teaching employees how to identify a phishing scam or Trojan Horse, for example, are first low-cost lines of defense. The other key is to quickly destigmatize breach reporting through the adoption of an "if you sense or see something, do something" philosophy. Threat intelligence and information sharing are the best ways for people to stay abreast of the rapidly evolving threat landscape, including law enforcement and intelligence officials. Best practices for disaster recovery and business continuity are similarly low-cost and easy to implement, especially given the advent of cloud-based solutions.

At a time when the world and its institutions—from business to government—face a precipitous erosion of trust combined with a constant onslaught of public misinformation, transparency is the greatest cure. For this, emerging technologies like blockchain, which underpin the boom of digital currencies of which Bitcoin is the preeminent digital mint, not only offer a secure alternative to traditional ways of organizing information; they create an unalterable public ledger using a distributed database across thousands of nodes. Another added benefit of this distributed approach is that blockchain can serve as a veritable disaster recovery and business continuity engine, being the equivalent of an informational "seed vault" for what cybersecurity professionals term as the "crown jewels;" or those data points or virtual assets (such as intellectual property) that are

CORE ELEMENTS OF A CYBER FDIC

- Governed by a code of conduct and clear value system
- Destigmatizes threat information sharing
- Aims to cap legal liability—particularly for vulnerable market sectors, such as middle-market companies
- Establishes a public-private structure that serves as a center of excellence
- Establishes proportional risk sharing and premium allocation, as well as the pooling and collecting of risk premia
- Reinsures catastrophic stop-loss coverage in the private market
- Serves as a technology clearinghouse vetting and disseminating emerging risk mitigation tools
- Conducts and benchmarks cyber stress tests
- Identifies and manages cyber threats to systemically important institutions (e.g. critical infrastructure, internet choke points, banking and financial markets among others)
- Trains, develops, and certifies providing reasonable assurance that standards of cyber hygiene are implemented

essential to an organization. While the adoption of this level of e-governance will be uncomfortable for most countries around the world, whose leaders have often profited handsomely in money or longevity from the opacity and byzantine nature of government, the demands of public accountability are growing increasingly restive. Political leaders have a choice then; proactively embrace transparency and accountability and the technologies that can make it so, or have it imposed upon them on the streets and in ballot boxes.

Economic Gap

The Weakest Link

Any discussion of resilience that does not include an economic component cannot be taken seriously. Resilience to complex risk requires a funding strategy should the threats rear their ugly heads. Failure to create a financial backstop often produces adverse long-range impacts hampering economic recovery. The Gulf region of the United States is still struggling to recover from hurricane Katrina and the BP oil spill more than 12 years later. More recently, the damage wrought by hurricane Harvey on Houston, may very well be the costliest natural disaster in U.S. history.[27] The economic consequences of cyber risk are no less complex to address. One of the chief issues in financially quantifying the true costs of cyber threats is that the world's understanding of valuing data and other intangible informational assets is nascent; so much so that only a small handful of thought leaders are building the approach to data valuation. Using a somewhat linear approach, Lloyd's, the world's specialty insurance market, estimates the upper end of the costs of cyberattacks at around $120 billion in a new report.[28] Taking in the second- and third-order costs however, the true figure may be into the trillions, as so much of the world's economic value is not only notional, it is locked in highly fluid electronically tradable instruments.[29]

A (Worthless) Priceless Asset

If Eric Schmidt's prognostications are correct that the world will go to war over data, how will we value the spoils of war? Oil wars by contrast are fought over a natural resource whose economic value is not only universally understood (in part because of scarcity), with common unitary valuation methods and third-party validation, its geostrategic terrain can be readily demarcated. Data enjoys no such parallels, which is where the war comparison ends. Data is undeniably valuable, but not all data is created equal, which is why it has thus far evaded economic or enterprise valuation approaches. Data is neither geographically bound nor is it scarce. Indeed, after the oceans and the sun, it may be the world's most abundant resource given our propensity to share and gather every single tidbit of information on the planet—from the absurd, like Instagram photos of our last meal, to the essential, like nuclear reactor safety readings.

The closest proxy for economic data valuation is to borrow a page from the types of financial stress tests regulators use on systemically important financial institutions (SIFIs). The largest banks in the world are the repository of most of the world's capital, which is why they are constantly in the crosshairs of cybercrime, insider threats, and evolving capital adequacy standards. Following the financial crisis of 2008, regulators adopted more stringent stress tests to see how large banks would respond to shocks. Similar shocks can be employed on organizations to gauge how they would respond if their data assets were rendered unusable and which other assets would be adversely affected. Through this method, we can begin to approximate the enterprise value of data (EvD) for the organization in question. While somewhat crude, this methodology can help organizations, policymakers, and national security leaders begin to modernize and layer their financial hedging strategies.

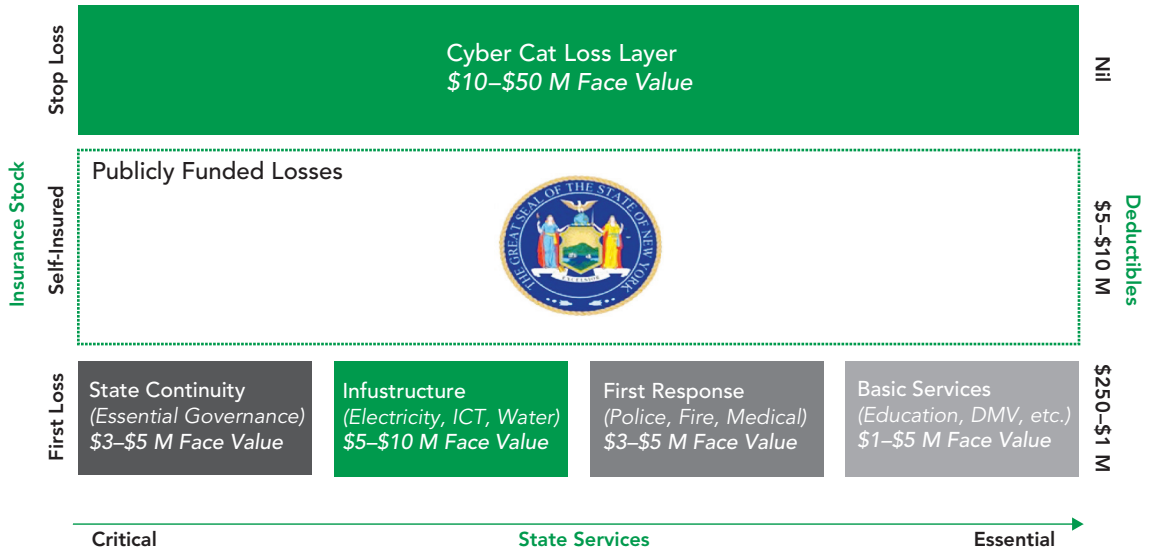
Modern Hedging

Cyber insurance is the fastest growing segment of the insurance market. While the first true cyber policies were placed at Lloyd's nearly two decades ago, insurers have experienced rapid market growth in the past five years. Today, more than 80 insurers are throwing their balance sheets at the cyber insurance segment. Despite this broad market participation on the supply side, the majority of cyber policies sold can be termed "Frankenstein" policies, or, rather, hybrid products where cyber is bundled with some underlying traditional class of insurance. One of the main challenges in guiding insureds through the appropriate risk hedging strategy is that most of the market views cyber risk and its attendant costs in a linear fashion. There is as much a gap on the supply as on the demand sides of the cyber insurance segment.

All too often customers seeking this coverage grapple with the question of "how much insurance to buy?" In most cases the math is troublingly linear. Firms will attempt to tally up the amount of personally identifiable information (PII) in their databases and then estimate a response and breach notification costs per record. On average, this produces a policy face value of $12 million across the U.S. market leaving most customers woefully under-hedged, especially when it relates to business continuity exposures, first party risks (or those events carried out by their staff—e.g. insider threats), and the growing incidence of cyber threats leaping through their virtual barriers causing physical damage losses.[30] All of these unfunded losses conspire to create a raft of litigation on denied cyber insurance claims, which in turn raises premium rates and increases the share of unfunded losses passed on to taxpayers or other parties.

To create a modern hedging strategy, the line between public and private losses must be drawn. After all, the public sector (often treated as a zero-liability entity) is increasingly behind some of the largest breaches recorded. The Office of Personnel Management (OPM), the U.S. Government's veritable human resources department was subject to the exfiltration of more than 21 million Federal employee records.[31] More recently, 200 million voting records for

FIGURE 1: Cyber Cat Loss Layer.



nearly all the U.S. voting public were exposed.[32] Additionally, the cyber exposure to critical infrastructure is fast becoming a real and present danger, from which the United States is not spared.[33] Hedging these costs calls for public–private risk sharing, wherein the concept of a catastrophic stop-loss solution can begin to adequately spread economic risks among willing insurers, making the government the insurer of last resort rather than the first line of defense. Figure 1 illustrates how this structure would be applied across agencies of a U.S. state.

conditions can help reduce the share of these risks passed on to the public.

Zen and the Art of Cybersecurity

If the gaps identified in this report are to be bridged, two vital support beams must be laid. The first is to align policy not only inside the U.S. and across all market sectors, but around the world. The transatlantic disconnect between the United States and Europe did not suffer its greatest blow with Brexit and the attendant EU schism, but rather with the upcoming implementation of the

Eventually the economic costs of cyber risk will have to be defrayed—or mutualized—across multiple stakeholders and market segments. A cyber FDIC that incorporates some share of losses, especially among the most vulnerable firms, cannot only offset costs, it can help spur better threat information sharing.

Bridging the Gap

Bridging the economic gap posed by cyber threats is a clear national security priority. Unfunded losses in the private and public markets insidiously make their way to public funds, either in the form of failed firms and their attendant job loss and costs, or in the form of direct (unfunded) costs to local, state and federal agencies. Eventually the economic costs of cyber risk will have to be defrayed—or mutualized—across multiple stakeholders and market segments. A cyber FDIC that incorporates some share of losses, especially among the most vulnerable firms, cannot only offset costs, it can help spur better threat information sharing. Until then, recalibrating the adoption of standalone cyber insurance with clear terms and

General Data Protection Regulation (GDPR) in Europe in May of 2018. These overarching cybersecurity and privacy rules, while far reaching and laudable for the centrality of individual privacy, adopt a carrot and stick approach to enforcement that may augur the equivalent of cybersecurity trade wars and privacy havens.[34] GDPR empowers EU regulators with a big stick, enabling them to levy fines of up to four percent of a firms' global revenues should they make any transgressions. Cybersecurity norms must be harmonized globally and threat information and the provenance of this stateless menace must be shared among authorities around the world and in near-real-time. The United States should lead this effort having woven the very fabric from which this scourge spreads.

However public policy and military doctrine evolve to respond to cyber threats, the path to enhanced national cybersecurity must be patiently charted. While our markets and personal demands call for immediate gratification, it is important to remember that cyber threats and the criminals, terrorists, and nations that collude with them have the benefit of patience and often lie dormant inside computer systems for years before they are discovered. To fight a patient, amorphous, and stateless menace will be one of the toughest challenges for public, private, and national security leaders. Just as the digital age has empowered ne'er-do-wells, it can also empower a new age of transparency, accountability and, above all, global cooperation to ensure the world's digital commons remain a force for good. Until then, our patience and mettle will be tested. PRISM

Notes

[1] Kate Vinton, "Jeff Bezos Overtakes Bill Gates To Become World's Richest Man," *Forbes*, July 27, 2017.

[2] Dante Disparte, "Apple vs. FBI: Much Ado About Nothing or a Temporary Truce?," *Huffington Post*, March, 31, 2016.

[3] Dante Disparte, "The I of very big T: (IoT Risks)," *Huffington Post*, August 19, 2017.

[4] Nicky Woolfe, "DDoS Attack that Disrupted Internet was Largest of its Kind in History, Experts Say," *The Guardian*, October, 26, 2016.

[5] Dante Disparte, "Free, Fair and (Mostly) Unfettered," *International Policy Digest*, November 16, 2016.

[6] Phil Wahba, "Amazon Will Make Up 50% of All U.S. E-Commerce by 2021," *Fortune*, April 10, 2017.

[7] Josh Constine, "Facebook now has 2 Billion Monthly Users and Responsibility," *TechCrunch*, June 27, 2017.

[8] In 1970 Tokyo Institute of Technology roboticist Masahiro Mori hypothesized that the more human a robot acted or looked, the more endearing it would be to a human being. See: Mashi Mori, "The Uncanny Valley," K.F. *IEEE Robotics and Automation Magazine*, 19 no.2. (2012).

[9] Patti Waldmeir and Richard Waters, "Tesla Overtakes Ford as Investors Bet on Electric Dream," *Financial Times*, April 3, 2017.

[10] James Vincent, "Self-driving Truck Convoy Completes its First Major Journey Across Europe," *The Verge*, April 7, 2016.

[11] Maureen Dowd, "Elon Musk's Billion-Dollar Crusade to Stop the A.I. Apocalypse," *Vanity Fair*, April 2017.

[12] Tess Townsend and Eric Schmidt, "Big Data is so Powerful, Nation States Will Fight' Over It," *Recode*, March 8, 2017.

[13] Dante Disparte, "Welcome to 21st Century Warfare," *The Hill*, January 5, 2015.

[14] Greg Jaffey and Steven Mufson, "Obama Criticizes Sony's Decision to Pull 'The Interview'," *The Washington Post*, December 19, 2014.

[15] Kim Zetter, "That Insane, $81m Bangladesh Bank Heist? Here's What We Know, Wired," May 17, 2016.

[16] Van Zadelhoff, Marc, "Cybersecurity Has a Serious Talent Shortfall, Here's How to Fix It," *Harvard Business Review*, May 4, 2017.

[17] Steven Morgan, "One Million Cybersecurity Job Openings in 2016," *Forbes*, January 2, 2016.

[18] Dante Disparte, "WannaCry on Cyber Monday," *The Huffington Post*, May 14, 2017.

[19] Gregory Wallace, "HVAC Vendor Eyed as Entry Point for Target Breach," CNN, February 7, 2014.

[20] Les Williams, "Solving Government Outsourcing Risk with Private Sector Thinking," *International Policy Digest*, September 23, 2016.

[21] Dante Disparte and Les Williams, "Cybersecurity: The Next Sytemic Threat," *International Policy Digest*, April 12, 2017.

[22] Dante Disparte and Chris Furlow, "The Best Cybersecurity Training you can Make is Better Training," *Harvard Business Review*, May 16, 2017.

[23] Justine Brown, "8 Major Banks Join Forces on Cybersecurity," CIO Dive, August 11, 2016.

[24] Dante Disparte and Franzetti, Andres, "Learning Cyber Insurance Lessons from Life Insurance Underwriting," *Risk Management*, February 13, 2017.

[25] Dante Disparte, "Dark Supply Chains," *Huffington Post*, August 2, 2016.

[26] Dante Disparte, "It is Time for a Cyber FDIC," *Huffington Post*, June 16, 2015.

[27] Dante Disparte, "Hurricane Harvey: When Rain Bombs Go Nuclear," *Huffington Post*, August 29, 2017.

[28] Tim Worstall, "Lloyd's - Extreme Cyberattack Could Cost $120 Billion, as Much as 0.2% of Global GDP," *Forbes*, July 17, 2017.

[29] Dante Disparte and Daniel Wagner, "Do you Know What your Company's Data is Worth?" *Harvard Business Review*, September 16, 2016.

[30] Dante Disparte, "Virtual Threats, Real Consequences," *Huffington Post*, August 26, 2016.

[31] Kim Zetter, "The Massive OPM Hack Actually Hit 21 Million People," *Wired*, July 9, 2015.

[32] Aria Bendix, "GOP Firm Exposed U.S. Voters' Personal Data," *The Atlantic*, June 20, 2017.

[33] Caroline McDonald, "Cyber Blackout Could Cost Insurers $71 Billion, Lloyd's Reports," *Risk Management*, July 22, 2015.

[34] Dante Disparte and Chris Furlow, "GDPR and Information Security Arbitrage," *International Policy Digest*, August 24, 2017.

Photos

Page 52: Lawrence Livermore National Laboratory. Available at < https://www.llnl.gov/news/livermore-berkeley-labs-lead-project-increase-power-grid-cybersecurity>.