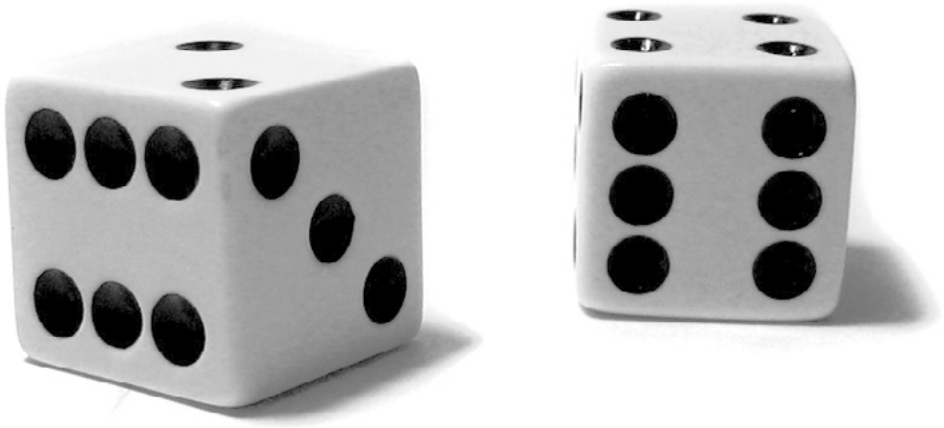
Risk Matters

A SEMI-ANNUAL PUBLICATION | SUMMER 2017

RC ANSWERS:
How to prepare for healthcare changes?

Meet Our Featured Risk Leader

Quantifying the true costs of cyber vulnerability



" Most cyber risk occurs between the keyboard and a chair."

Risk Cooperative

Contents

"Principles matter most when it's least convenient."

COLUMNS

FEATURES

Risk Matters

Risk Cooperative
1140 Connecticut Ave., NW
Suite 510
Washington, D.C. 20036

+1 202.688.3560
info@riskcooperative.com

Risk Matters is published semi-annually by Risk Cooperative to move risk from being a cost to becoming a catalyst for change, new initiatives and greater resilience around the world. With this and our latest curated content, we aim to advance the standards of practice of the risk and insurance profession.

Foreword

Risk is not going away. In fact, it is safe to say man-made risk, whether in the shape of accelerating climate change or rampant cyber threats, are challenging conventional approaches to risk management.

In this debut edition of Risk Matters, our semi-annual journal devoted to advancing the standards of practice on risk, readiness and resilience, we pay close attention to cyber risk. All too often, cyber risk is consigned to IT and cybersecurity leaders as a purely technical challenge. And yet, through one costly event after another, we realize that in order to get ahead of this complex menace, many of the defenses we can draw on are in fact free.

Adhering to corporate value systems, abiding by a culture of accountability, information sharing (without consequences) and implementing good cyber hygiene are generally low cost, high impact ways to address cyber risk. And yet, in the search for a purely technological panacea, many forgo the governance and "people between the keyboard and the chair" for technology investments. They do this at their own peril.

Each edition of Risk Matters will curate content and wide ranging analysis from Risk Cooperative's team of experts, as well as our featured guests and risk leaders. We hope you enjoy this and future editions of Risk Matters.

Dante Disparte is the founder and CEO of Risk Cooperative, and co-author of the book "Global Risk Agility and Decision Making"

Featured Risk Leader

Tom Ridge, is Chairman of Ridge Global, a security consulting firm Ridge founded following his tenure as the first Secretary of the U.S. Department of Homeland Security, where he worked to create an agency that facilitated the flow of people and goods, instituted layered security at air, land and seaports, developed a unified national response and recovery plan, protected critical infrastructure, integrated new technology and improved information sharing worldwide. As the 43rd governor of Pennsylvania, Ridge implemented an aggressive technology strategy that helped to fuel the state's advances in economic development, education, health care and the environment. At present, Gov. Ridge serves on the board of the Institute for Defense and as chairman of the U.S. Chamber of Commerce's National Security Task Force.

TOM RIDGE IS THE CHAIRMAN OF RIDGE GLOBAL

Gov. Ridge created Ridge Global with the goal of leveraging his expertise, experience and unrivalled network of former officials, technical advisors and business leaders to provide solutions to cyber security, international security and risk management issues. With Gov. Ridge's guidance, the Ridge Global team works works with C-suite executives and corporate directors to reduce enterprise risk and to build more resilient organizations through innovative preparedness, protection, response and education capabilities.

Providing accurate assessments of policy and technology trends, partnership and acquisition strategies and understanding each organization's competitive position enables Ridge Global to assist clients in exploring adjacent markets, expanding into new business capabilities, and executing strategic plans.

A noteworthy accomplishment is the launch of the first-ever online cyber-risk oversight certificate program, which bringstogethertheprofessional-development capabilities of the National Association of Corporate Directors (NACD); Ridge Global's experience as a leading risk advisor to C-suite executives and board leaders; and the deep, cyber-technical expertise of the world-renowned CERT Division of the Software Engineering Institue (SEI) at Carnegie Mellon University to deliver a cyber education and resource program that addresses the specific cyber-risk oversight responsibilities of board members and executives. "Earning this credential enhances the ability of directors to bridge enterprise gaps that may exist between business and IT leaders on cybersecurity," said Gov. Ridge.

This kind of innovative and insightful approach to solving the real-world challenges of risk preparedness is why Risk Matters names Gov. Tom Ridge our debut Risk Matters Featured Risk Leader.

By the Numbers

CYBER SECURITY IS ONE OF THE TOP ENTERPRISE RISKS OF 2017.

[1] theverge.com/2017/5/14/15637888/authorities-wannacry-ransomware-attack-spread-150-countries
[2] lloyds.com/news-and-insight/risk-insight/library/technology/countingthecost?utm_source=Lloyds_posts&utm_medium=social&utm_campaign=emergingrisks_cyence
[3] Insurance Information Institutes 2015 cyber writings report
[4] 2017 Ponemon Cost of Data Breach Study

Summaries

INSURANCE: COST OR CATALYST? | PUBLISHED 01.09.2017

Written by Dante Disparte
Originally published on Huffington Post

When you think of insurance as a catalyst, not unlike the original insured's at Lloyd's, the advent of a risk-transfer process enabled journeys and shipping routes that would have otherwise never occurred. Like the early days in a bustling London coffee house that launched one of the world's most enduring institutions, it is now time for risk-makers and risk-takers to join forces in tackling emerging threats, unlocking new markets and in creating value.

Read the full article: huffingtonpost.com/entry/insurance-cost-or-catalyst_us_5873bff0e4b08052400ee4ad

SIMPLE ETHICS RULES FOR BETTER RISK MANAGEMENT | PUBLISHED 11.08.2016

Written by Dante Disparte
Originally published on HBR.org

For far too long, managing risk has been seen as an esoteric business function — designed to control losses and adhere to compliance standards. But as more organizations fall prey to complex intangible risks, from unwanted disclosure due to rampant cyber threats to breaches of conduct driven by skewed incentive systems, the aperture of risk management is expanding from protecting the balance sheet to promoting ethical leadership and values-based decision making.

Read the full article: hbr.org/2016/11/simple-ethics-rules-for-better-risk-management

10 MAXIMS FOR ACHIEVING RISK AGILITY | PUBLISHED 10.12.2016

Written by Dante Disparte
Originally published on Huffington Post

With the growing number of firms falling prey to cyber risk, governance failures and market forces, there is a need for greater agility in how decisions are made and risks confronted. Yahoo!, with its record-breaking cyber breach estimated at more than 500 million records, and Wells Fargo are but two of the latest firms to face complex challenges and an unwanted public excoriation. Like VW's emissions scandal or the warning signs that could have prevented the Germanwings disaster, it is time for senior business leaders and their boards to change the way they think about risk and therefore how they respond to it.

Read the full article: huffingtonpost.com/dante-disparte/10-maxims-for-risk-agilit_b_12289238.html

Links to all RC published articles, interviews, and engagements are located under Insights on riskcooperative.com

RISK MATTERS | SUMMER 2017

Featured Analysis

THE WORLD NEEDS A DARPA-STYLE PROJECT TO PREVENT PANDEMICS | PUBLISHED 04.24.2017

Written by Tom Ridge and Dante Disparte
Originally published on HBR.org

When the Blizzard of '78 hit the Northeast, it caught the region by surprise. Some meteorologists had predicted only a minor snowstorm, and forecasts were still unreliable enough that many people simply went about their regular business. When the hurricane-force storm hit, traffic came to a complete standstill due to the fast-accumulating snow – even the plows were stuck — and thousands of cars were abandoned. Not all the stranded people would survive. It took over a week – and help from the National Guard – to clear the roads again.

Today, even as weather events have become more extreme due to climate change, we're in many ways more prepared for them: scientists' forecasting techniques have gotten better, and governors and mayors have standard practices for handling preparation and cleanup for all but the most severe events (think Hurricane Katrina or Superstorm Sandy). The private sector has also played an important role: today if there's a blizzard, tornado, or flash flood in your area, your smartphone will notify you so that you can shelter in place until the risk has passed.

While advances in tracking weather-related risks have improved public safety and resilience, we have made far less progress on enhancing global resilience to biological risks and pandemic threats. As the bipartisan Blue Ribbon Study Panel on Biodefense highlighted, U.S. levels of readiness and global coordination are woefully inadequate. And the U.S. is not alone in this; it's is a global problem.

Over the last few decades, the world has had several near-misses on a true global pandemic, from the Ebola outbreak in West Africa to various strains of avian influenza to, most recently, the rapid spread of Zika. We're also facing a new and perilous generation of drug-resistant pathogens. What these near misses tell us, quite simply, is that we are not ready for a global pandemic. Fixing this should be one of the top public health priorities today for leaders in science, government, and private industry.

In public health, it is much easier to play offense than it is to play defense. Playing offense well, however, is going to require a lot more coordination – both internationally and within national borders. We believe an important first step in this effort is for the U.S. and governments around the world to develop an equivalent to the Defense Advanced Research Projects Agency (DARPA), that focuses cross-sector efforts on advancing biological and pandemic risk readiness.

Why should the public sector lead the way? Because the long-term horizon and trade-offs required to develop scalable responses to pandemic threats are exactly the type of problem too big to be solved by any one sector. Government can play a unique role in catalyzing the kind of cross-sector collaboration needed. Here's what the public sector, private sector, and research/science communities could do to work better together:

Government
The U.S. federal government has allocated $6 billion to research efforts on these threats. That may sound like a lot, but it pales in comparison to the amount spent on cyber security, airport screening, or border security. It's not enough. And it's not as effective as it could be, because the money is allocated in a disaggregated manner. In addition to homing in on targeted research and development efforts, governments have a unique obligation to work with the international community, such as the World Health Organization, to ensure a common response framework is in place, particularly in fragile states, whose health systems are underdeveloped. Our strength lies in global collaboration, widespread early warning systems that do not sow panic and deep cross-sector collaboration. With this we can begin to put unseen threats into focus so the U.S. and the global community can manage them.

Private sector
Resilience to biological and pandemic threats is not singularly a matter for public health officials, governments, and the military. After all, militarizing the Ebola response was among the costliest of interventions we have had and, arguably, will complicate future health interventions. It should be our last line of defense, not our first.

Biodefense and pandemic risk mitigation are also a matter for deep private sector involvement. As Bill Gates warned at the Munich Security Conference, millions of lives are at risk and the economic consequences pale in comparison to other global threats. Zika has cost the economies of Latin America and the Caribbean an estimated $18 billion; the last Ebola outbreak cost more than 11,000 human lives and more than $32 billion in economic ripple effects.

The private sector must also break the cycle, particularly in the pharmaceutical industry, of only prioritizing blockbuster drugs and other commercially viable investments. In the long run, the proposition of global market collapse due to biological and pandemic risks cannot be offset by the potential rewards of the next big lifestyle drug. Resilience to societal threats must become a collective societal priority, even if the economics seem intangible. Those with the resources, financial and otherwise, have a special obligation to focus on the many grave challenges posed by an increasingly complex and interconnected threat landscape.

In short, we must adopt a global "invest now or pay later" economic philosophy. Amid this uncertainty, there are great rewards to be reaped by innovators and entrepreneurs who recognize the challenges of robust bio and pandemic defense as a unique market opportunity.

Science/technology community
As with DARPA, the science and technology community are the unsung heroes in improving global biodefense and pandemic risk readiness. But unlike advanced military research, which is conducted under strict secrecy, the scientists working on improving our defenses to emerging threats must have a charter that encourages open collaboration and transparency. All too often research and technology investments, particularly those in the private sector, follow a zero-sum approach. Coordinating grant efforts and capitalizing these initiatives should be as much about scientific and technological breakthroughs, as they should be about enhancing global public awareness to simple preventive measures like washing hands.

We realize that there is no shortage of major problems facing the world, from climate change to armed conflict. But pandemics, with their unique combination of speed and deadliness, deserve far more attention than they're currently getting. They need to be a top priority. We also understand that calling for more collaboration, particularly more international collaboration, during a time of rising

RISK MATTERS | SUMMER 2017

Featured Analysis

populist and nationalist sentiments may seem quixotic. However, pandemics do not recognize national borders. Rather than deglobalization, trade barriers, and isolationism, we need global collaboration, coordination, and investment. Allowing these risks to fester, as too many governments did in the early days of the Ebola crisis, will only reveal how interconnected and vulnerable the world really is. In a globally connected economy, you cannot decouple the fortunes of companies from countries, or countries from one another.

The next pandemic is going to be a lot harder to predict – and a lot deadlier — than the next superstorm. Let's not allow it to catch us flat-footed.

hbr.org/2017/04/the-world-needs-a-darpa-style-project-to-prevent-pandemics

IN THE LAME DUCK, HOW CONGRESS MAKES CYBERSECURITY A NON-PARTISAN PRIORITY | PUBLISHED 11.14.2016

Written by Andres Franzetti
Originally published on Forbes.com

With a lame duck session of Congress looming, federal lawmakers are scrambling to push key legislative items through last-minute. One key area of concern is cybersecurity.

Recent headlines have exposed a wide array of victims, ranging from both corporate to government entities. Stoking concerns is the ongoing controversy surrounding Russian hacking of Democratic presidential candidate Hillary Clinton's campaign emails and the DNC, in a perceived effort to influence the outcome of the U.S. presidential election. Against this backdrop, several members of Congress have introduced amendments to the National Defense Authorization Act (NDAA) to strengthen cybersecurity. Yet, is this enough?

It is without a doubt that the nature of war has changed. For centuries, war has been waged on battlefields and televised around the clock. Now, the theatre of war has shifted and is being waged on computer servers, in homes and at places of work. Not even our most secure government institutions are exempt—exposing troves of private, classified and sensitive information, putting at risk our economic, social and national security.

Foreign aggressors are brazenly infiltrating U.S. institutions and political elections systems—like the recent breach of state voter registration databases in Arizona and Illinois where more than 200,000 voter records were stolen by Russian hackers—shaking the nation's long-relished standing as an impenetrable global superpower.

Several cybersecurity amendments have been introduced to the NDAA, including a Senate amendment that directs the president to elevate Cyber Command to a Combatant Command (currently it lies subordinate to strategic command). This elevated status will allow resources to be deployed strategically, enabling faster responses to potential threats.

Senator Richard Blumenthal, one of seven senators who sponsored the amendment, stated, "Cyber attacks are an ever-growing threat to our national security." Blumenthal continued, "As the Internet touches more aspects of our work and daily lives, our military must be equipped to defend and protect our nation. Elevating CYBERCOM to a Combatant Command will enhance its ability to protect Americans from cyber threats."

Yet, the hard truth is that even with this elevated status of Combatant Command, our cyber infrastructure and resilience is still vulnerable. The hard truth is we have fallen behind and have become yet another nation that's vulnerable, ill-prepared and struggling to protect itself against foreign cyber militants.

The current administration is now evaluating a counter response to stymie the recent attacks. However, in this new age of cyber warfare, one thing has been made abundantly clear: Past attacks against U.S. targets have exposed our unpreparedness, identifying and shutting down infiltrators at a pace that's ineffective in mitigating damage, and leaving our citizens exposed and vulnerable.

Knowing this, highly sophisticated foreign hackers are waiting in the wings, plotting their next offensive, and looking to seize on our complacency in protecting our IT infrastructure.

It's unclear what final cybersecurity measures will take shape in the final NDAA, as the bill is currently being reconciled between the two chambers, but what is clear is that what has been offered does little to nothing to help prepare our frontlines and most vulnerable assets. Foreign aggressors are shifting their focus to smaller, independent businesses, state governments and other soft targets that can trigger disastrous ripple effects across our economy.

To become truly cyber resilient, we need a proactive national mandate, not just a reactionary and retaliatory mentality. Just as in any other time of war, the country must come together to develop a national response, moving beyond the stagnate political climate in Washington, and invest in increasing the cyber preparedness of our states.

State governments, businesses and communities across the country must be united in making the case for a unified, national response, built around four pillars crucial to protecting Americans.

1. Cyber security must be looked at as a national security risk, not a state-level issue. Amendments offered to the NDAA, such as the Senate amendment, help to address this issue by elevating the status of cyber risk; however, it falls short in that it focuses its powers in mostly reactionary measures. Much like our infrastructure, cybersecurity must be viewed in the light of national security. States need the support of the federal government to not only combat these threats, but to endure their financial consequences. Many states have limited budgets and lack the necessary resources to deal with this threat on their own. They often cannot develop and sustain a viable strategy to deal with as fast-moving targets as cyber

Featured Analysis

threats, leaving many aspects of their infrastructure and municipalities at risk.

2. Standardized levels of security, protocols and cyber resilience programs must be enacted nationwide. A select few states have taken the initiative to enhance their cyber resiliency by establishing statewide cybersecurity programs. Working in conjunction with the private sector, they are assessing their vulnerabilities and taking measures to beef up their front-line defenses and monitoring. While commendable, this uncoordinated approach will result in a dizzying patchwork of standards and responses. Additionally, the rollout on a state-by-state basis leaves large parts of our interconnected IT infrastructure at risk. Standardized requirements need to be enacted to ensure each state can withstand an attack and its key services and infrastructure remain intact.

3. Cyber warfare is an ever-evolving enemy, so too should be its response. Hackers lurk in the shadows, often lying dormant for months or years within an organization's system before being detected, as noted in the OPM report where intruders were stated to have been in their systems for nearly a year. As such, merely enacting security protocols or conducting an annual sweep is not enough. Ongoing training and systems monitoring need to be a central pillar of any cyber readiness strategy. While hackers are becoming more sophisticated daily, so too is the technology being designed to combat them. Local governments need to leverage the innovative technologies being developed by the private sector to keep pace with an ever-shifting enemy, and to limit the damage a possible attack can have.

4. Governments cannot deal with this alone—an alliance between the public and private sectors is needed. Cyber-attacks have the potential to levy crippling consequences to millions of Americans, from financial costs to irreparable reputational damage. Whichever cybersecurity measures are attached to the NDAA must work with private sector companies at the state level to help bridge the talent and resource gap. They must look to partner with industry experts and leverage innovative risk mitigation tools, including insurance, to address the threat and costs to mitigate breaches. Early identification and response of a breach is the key to not only making our nation safer, but also to reducing the costs associated with its remediation. Leveraging the insurance markets can offset the financial burden of an attack to the private sector rather than at the state and, ultimately, the taxpayer level.

Cybersecurity has emerged as a national priority, and this election cycle has elevated the national discussion as presidential candidates spar on a daily basis about security breaches from foreign aggressors. Federal lawmakers have an opportunity in the lame duck to move beyond partisan gridlock to put the American people first, and develop a bipartisan national response that's coordinated among all levels of government.

America has always been viewed as a resilient nation, able to endure and withstand attacks to the homeland—now it's time that we extend that same resiliency to our cyber infrastructure.

forbes.com/sites/realspin/2016/11/14/in-the-lame-duck-how-congress-makes-cybersecurity-a-non-partisan-priority/#2b4b939e1469

CYBER SECURITY – THE NEXT SYSTEMIC CRISIS?

| PUBLISHED 04.12.2017

Written by Dante A. Disparte and Les Williams
Originally published on International Policy Digest

In the summer of 2007, an unexpected threat was on the horizon for the U.S. and global economy. August 2007 marked an opening salvo in how systemic risk can affect the global economy. As the Brookings Institute so eloquently observed in "The Origins of The Financial Crisis," the crisis "had its origins in an asset price bubble that interacted with new kinds of financial innovations that masked risk; with companies that failed to follow their own risk management procedures; and with regulators and supervisors that failed to restrain excessive risk taking." Many of these very elements and correlations are inflating the growing cyber security bubble and many of the same "fox watching the chicken coop" tendencies are influencing this systemically important market.

The Federal Reserve estimated that the Great Recession cost the U.S. $14 trillion in economic activity. State unemployment insurance trust funds borrowed a total of $50 billion from the Federal Government to replenish their coffers as jobless claims soared. Plummeting home values saw approximately 11.6 million households owing more than their homes were worth by the end of the recession. These types of systemic correlations exist in the fast-growing cyber security market, which encompasses a wide range of interconnected services, such as IT security, crisis response, compliance, and, perhaps most importantly, the cyber insurance market, which attaches to the balance sheets of more than 80 insurers – and through them to the economy writ large.

In the aftermath of the Great Recession, several measures were put in place to prevent such a catastrophe from occurring. However, this "Monday Morning Quarterbacking" should give us pause; what other crises are looming on the horizon where measures can be proactively implemented to prevent or mitigate the next big one? While August 2007 was a specific timeframe that can be referenced as the "beginning" of the Great Recession, an equally insidious threat has been menacing the global economy ever since, namely systemic cyber risk.

Experian, Yahoo!, Target, Sony Pictures, Evernote, the U.S. Military, the Federal Government, the Virginia Department of Health, TJ Maxx, AOL, CitiGroup, BNY Mellon, EBay, Anthem, JP Morgan Chase, the 2016 presidential election. These are but a small handful of the entities and events that have fallen prey to cyber security threats. While the causes of the Great Recession can largely be traced to greed on Wall Street, the lack of sufficient oversight by regulators, and the breakdown of risk management procedures within organizations, the causes of cyber threats are similarly the result of human behavior and poor risk management. Money, attention and inattention, fame, political influence, the promotion of ideologies, and public disclosure are some of the root causes of breaches. Critically, just like protecting vital financial systems, underinvestment can also serve to amplify cyber risks and their attendant losses of both the acute and attritional variety.

The systemic financial risks that caused the Great Recession and cyber threats share several important traits; the staggering costs they can levy on an economy, their correlations across sectors, the ability to lay dormant festering for many years and the heavy toll they can have on people. Indeed, AIG's new personal cyber insurance policy is a gamble that this personal fear will manifest in yet

Featured Analysis

another growing segment of the booming cyber insurance market, where gross written premiums are estimated to increase from $2.5 billion in 2015 to $7.5 billion in 2020. Cyber insurance is the fastest growing segment of the otherwise mature insurance industry. All the major players are jumping into the cyber fray and the race to achieve competitive differentiation may lead to the very types of financial innovations that mask risk, but do not in fact offset it. By this measure, in a catastrophic cyber loss impacting multiple sectors at once, the limited pool of IT security talent will be tantamount to the limited pool of liquid capital that all parties were clamoring for during the financial crisis.

When it comes to mitigating cyber risk, far too much energy is being placed on privacy and compliance (both are important), and far too little is being paid to business continuity and systemic risk. Insurers are aware of this market focus, which is why the majority of cyber insurance policies base their actuarial models – limited as they are – on a price-per-record approach when it comes to personally identifiable information (PII). The real exposure in the market is more akin to catastrophic losses or the type of systemic risk we saw during the financial crisis. The exponential growth of connected devices, the internet of things (IoT), along with all other points of connection across industries, economies and countries, makes cyber risk a systemic threat. Unlike managing systemic financial institutions, such as the big global banks at the center of the financial crisis, it is hard to identify the points of failure that contribute to systemic cyber risk.

The recent attack on DYN, an essential provider of internet monitoring, control and domain registration, underscores how global connectivity is at once an asset and a liability in the modern economy. DYN was taken down in a successful denial of service attack, which was carried out by employing an army of connected devices, including home webcams that directed overwhelming traffic to DYN's servers. Large swaths of the internet were affected in this attack, including household names like Twitter, Netflix and Spotify, among others. A similar attack on financial trading platforms, systemic banks, stock exchanges or critical infrastructure would certainly have a more calamitous outcome than millions of frustrated web surfers.

Learning from our past is an intelligent way to prepare for the future, hence the importance of applying lessons learned from the financial crises to the ongoing issue of systemic cyber risk. Similar to banking regulations put in place to more effectively manage risk, regulations must be implemented to understand and combat cyber threats, while at the same time enhancing cyber resilience. Not unlike the concept of identifying systemically important financial institutions (SIFIs), when it comes to cyber resilience, examples like the DYN cyber-attack, underscore how seemingly insignificant enterprises can have broad ramifications. Should regulators develop a list of systemically important entities when it comes to managing cyber risk? Should those entities, like their financial counterparts, be required to create so called "living wills" providing disclosures on how to address their distress or failure? Is there a cyber equivalent of the "Volcker Rule" that would firewall certain activities? What hedging mechanisms can be put in place to serve as a financial back-stop to the cascading financial losses that can emanate from systemic cyber risk?

Insurance is clearly a part of this resilience equation. However, insurance that merely covers third-party risks and customer notification costs will hardly address the next trillion-dollar crisis – let alone one that can spread across sectors instantaneously.

Perhaps the biggest lesson learned from the financial crisis, wherein we privatized gains and socialized losses, is that unhedged systemic risks will be borne by tax-payers. Just like the uninsured represent a heavy burden on the healthcare system, uninsured or underinsured organizations will needlessly burden the system and potentially imperil the economy.

intpolicydigest.org/2017/04/12/cyber-security-next-systemic-crisis/

THE RISE OF CYBER-ATTACKS & HOW TO PROTECT AGAINST THEM | PUBLISHED 01.20.2017

Written by Daniel Wagner and Dante Disparte
Originally published by Professional Investor

Governments, institutions, and individuals are not paying enough attention to the growing threat of cyber terrorism, argue Daniel Wagner and Dante Disparte.

This article published in CFA UK's magazine Professional Investor (PI) suggests that despite the fact that cyber-attacks occur with greater frequency and intensity around the world, many either go unreported or are under-reported, leaving the public with a false sense of security about the threat they pose and the lives and property they impact. While governments, businesses and individuals are all being targeted on an exponential basis, infrastructure is becoming a target of choice among both individual and state-sponsored cyber-attackers, who recognize the value of disrupting what were previously thought of as impenetrable security systems. This has served to demonstrate just how vulnerable businesses, cities and countries have become, and the growing importance of achieving global risk agility in the face of such a threat.

Executive Summary

- While governments, businesses and individuals are all being targeted on an exponential basis, infrastructure is becoming a target of choice among both individual and state-sponsored cyber-attackers, who recognize the value of disrupting what were previously thought of as impenetrable security systems.

RISK MATTERS | SUMMER 2017

Featured Analysis

- Governments, businesses and individuals must devote greater resources to becoming more cyber-vigilant, which means they must devote more resources toward anticipating and protecting against attacks. Governments and businesses need to also engage in more public-private partnerships in order to adequately address the issue.

- Governments around the world have plans in place to deal with the consequences of natural disasters, yet none have disaster relief plans for a downed power grid. Clearly, this must change. The same may certainly be said of the need for businesses to put cyber-risk on the front burner, stop presuming it is someone else's problem, and devote the resources necessary to seriously and effectively combat the problem.

As an example of the growing vulnerability of critical infrastructure, in December 2015 a presumed Russian cyber-attacker successfully seized control of the Prykarpattyaoblenergo Control Center (PCC) in the Ivano-Frankivsk region of Western Ukraine, leaving 230,000 without power for up to six hours. This marked the first time that a cyber weapon was successfully used against a nation's power grid. The attackers were skilled strategists who carefully planned their assault over many months, first doing reconnaissance to study the networks and siphon operator credentials, and then launching a synchronized assault in a well-choreographed dance. The control systems in Ukraine were surprisingly more secure than some in the U.S., since they were well-segmented from the control center business networks with robust firewalls (Wired, 2016), emphasizing just how vulnerable power systems are globally.

If that is the case for a sophisticated power station, does an ordinary business stand a chance if hackers choose to penetrate its security system? Cyber-attacks are difficult to prevent, given the relative ease with which hackers can find a single system vulnerability, and the impossibility of plugging every conceivable security hole. Cyber-security professionals are in essence playing an endless game of cat and mouse, whereby a would-be attacker attempts to enter a system while security professionals attempt to defend a computer system from attack by applying continuous patches. The adversary then quickly moves to exploit the latest discovered vulnerability. That is why many computer security programs produce patches numerous times per day – even for home computers.

Cyber-Vigilance and The Need for More Resources

High profile cases of cyber-attack are increasingly becoming the norm. The U.S. government had little difficulty finding evidence to assign blame to China for the theft of personal information of more than 22 million government employees from the computer systems of the Office of Personnel Management in 2015. Similarly, it did not take long for the U.S. to determine that North Korea was responsible for the cyber-attack against Sony in 2015. Cyber-attacks essentially give nations of all sizes, degrees of wealth and resources a seat at the table of the super powers, affording them a disproportionate amount of clout. While China, the U.S. and Russia lead the world in cyber-attacks, virtually every government engages in such attacks, and nearly every country has it share of computer hackers.

International treaties intended to address the problem have limited impact because of the inability to hold signatories accountable and the difficulty associated with accurately determining the identity of responsible actors. Enhanced information sharing, combined with a mandate to swiftly and accurately release information regarding attacks to impacted citizens, provide a sensible foundation for designing a protocol to effectively address future attacks, yet very few governments routinely engage in this practice.

Clearly, governments, businesses and individuals must devote greater resources to becoming more cyber-vigilant, which means they must devote more resources toward anticipating and protecting against attacks. They need to also engage in more public-private partnerships in order to adequately address the issue. The European Union has recently implemented the "Network and Information Security Directive", which forces member states to adopt more rigid cyber-security standards, and creates an avenue for the 28 member states, and the operators of essential services such as energy, transportation, and healthcare sectors to communicate. Other nations are in the process of acting accordingly. However, no nation allocates sufficient resources to adequately respond to the increasing threat of a cyber-attack against critical infrastructure, nor does any nation have a truly comprehensive plan to prevent or meaningfully react to the outcome of such attacks.

Taking Precautions

Taking precautions against cyber-attacks has become essential, particularly among financial institutions, which are frequently targeted for attack. Serious incidents have occurred this year across the globe, including among banks in Vietnam, Ecuador and the best known example – Central Bank of Bangladesh, in which $81 million was successfully stolen. For financial institutions, cyber-attacks have become so serious that in October of this year, the U.S. Treasury Department's Financial Crimes Enforcement Network issued an advisory on cyber-crime as well as guidelines for how and when to report suspicious activity. According to a recent report by Verizon, which involved 67 organisations in the private and public sectors, 48% of data breach incidents among banks in 2015 involved compromised web applications, prompting many financial institutions to require two-step verification procedures, and a host of other protective measures.

While cyber-attacks can pose a nuisance for countries with cyber defense capability, for businesses without it, cyber-attacks can pose an existential threat, not just operationally, but in terms of reputation risk, so they must create a sturdy defense. A large variety of insurance carriers now provide cyber-risk insurance, which can provide meaningful protection. But businesses must go further than to take out insurance. Business continuity plans must be carefully crafted, and an implementation plan must be both realistic and executable. Employees must be trained what not to do (for example, click on the wrong email link), as well as what to do in the event of an attack. And crisis management programmes should be put into place in advance of actually needing to do so, so as to be able to respond in a meaningful fashion.

Apart from heightening awareness to cyber-attacks, a number of actions should also be taken so as to avoid the gaze of regulatory and legal action that can occur after an attack has occurred. To the extent possible, avoid collecting or retaining unnecessary personal information of customers. Restrict access to sensitive information to a small pool of employees. Deploy best practice methods to store and transmit sensitive information, and be sure to require that third party partners and service providers do the same. If there is a data breach, be sure to carefully weigh the key messages you wish to convey to your customers, partners and employees.

RISK MATTERS | SUMMER 2017

Featured Analysis

Don't make matters worse by sending the wrong message to the marketplace.

Conclusion
Governments around the world have plans in place to deal with the consequences of natural disasters, yet none have disaster relief plans for a downed power grid. Clearly, this must change. Local and state governments must work together with their national counterparts to produce and quickly implement plans to address future attacks. The same may certainly be said of the need for businesses to put cyber-risk on the front burner, and stop presuming it is someone else's problem. Doing so will take as much will and determination as successfully tackling any other risk that poses a potentially existential threat to a firm.

professionalism.cfauk.org/rise-cyber-attacks-protect/

HOW U.S. COMPANIES CAN PLAY A ROLE IN LATIN AMERICA'S GROWING CYBER ECONOMY | PUBLISHED 03.23.2017

Written by Miguel Tavera
Originally published on International Policy Digest

The transformation of Latin America's economy towards knowledge and technology dependence begs American businesses to engage more in the region than ever before. The "pink tide" of economic orthodoxy and integration in Latin America has led to an unprecedented boom in innovation and entrepreneurship. More importantly, these orthodox economic policies have lifted millions of people out of poverty and into the middle class.

Critical to the success of these policies is a technological revolution which places consumers and businesses at the forefront of progress and prosperity. Despite the hesitancy by the current U.S administration towards investment in Latin America, the U.S private sector must lead the charge in the hemisphere's changing economy. Failure to do so can result in missed economic opportunities and geopolitical concessions to America's competitors.

Across the globe, the "Uberization" of economies is empowering people and small businesses to create growth using little more than their mobile phones. Mobilizing underutilized capital in the region has created tremendous growth opportunities in the Latin American cyber economy, the most important of which is people. According to the Inter-American Development Bank (IDB), only 43.5% of Mexicans are internet users and only 30.7% of Mexican households have access to the internet. However, this number is rapidly growing.

The increasing number of connected consumers in Latin America presents a unique opportunity for small and medium sized companies to sell direct to consumers. Retail sales through online sales channels, for instance, are expected to grow to $85 billion in the next two years. Given these trends, large U.S companies such as Walmart and Amazon are already seizing the opportunity to expand and invest in their online sales. Incredibly, the growth in Latin America's e-commerce industry is occurring while more than half of the region's largest economies still don't have access to the internet.

This is particularly true in the area of cash transfers, where peer to peer technology is changing the way people send and receive money. The success of programs such as M-Pesa in Kenya has opened the door for similar technologies that promote financial inclusion and economic growth.

In Ecuador, for instance, the government launched a peer to peer money transfer platform and bill payment system using prepaid mobile phone accounts. The application of similar technologies has an immense impact on unbanked and underbanked communities, giving purchasing power back to the middle class.

Despite the growth of e-commerce and technology platforms, regulatory standards and legislation have not caught up. Political uncertainty and a lack of cyber and e-commerce standards create a high-risk environment for local and foreign companies. This is yet another opportunity for U.S firms to create a more favorable investment environment in the region. While these sorts of risks have traditionally been a repellant for investment in otherwise lucrative and burgeoning markets, companies must see risk as an opportunity. Comprehensive financial instruments which safeguard investment such as political risk insurance and standalone cyber liability insurance can become instruments for growth in the region, as opposed to a cost. Moreover, U.S firms have the opportunity to introduce cyber governance and education opportunities to reduce risk, increase revenues, and shape policy.

The failure of businesses to engage in the future of Latin America's economy will effectively cede market share to America's competitors. China's continued investment in Latin America presents a geopolitical and economic threat to the United States given the Chinese government's traditionally "lax" views on cyber accountability. In Brazil, Chinese telecom giant Huawei reportedly owns 40% of the telecommunication equipment market and has made significant investments in Mexico. It is undoubtedly in the best interest of American companies and American national security to invest and shape the future of commerce in the Western hemisphere.

intpolicydigest.org/2017/03/23/how-u-s-companies-can-play-a-role-in-latin-america-s-growing-cyber-economy/

RC Answers

There has been so much talk of changing the healthcare law recently. How can I make sure my company is on top of these changes?

HAVE A QUESTION FOR OUR EXPERTS?

Send your inquiries to info@riskcooperative.com and your question and answer may be published in a future edition of Risk Matters.

Potential changes that may be forthcoming to the Affordable Care Act and overall health care system in the U.S. are top of mind for many individuals and business owners.

Business owners in the U.S. have a duty and an obligation to ensure that our citizens and our employees have adequate health insurance protection in the unfortunate event that something were to happen to them. With the changes that are forthcoming, it's likely that prices are going to increase. These changes will be particularly harmful to small businesses, which account for 90% of U.S. employment.

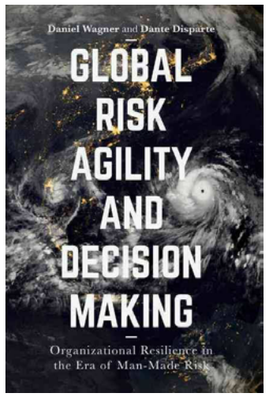
In order to stay ahead of these changes, while controlling rising costs, firms should: 1) Work with their benefits advisors and insurance brokers well in advance of their policy renewals. 2) Structure plan design around equitable cost sharing models between the employer and employee. 3) Increase the number of complimentary benefits, such as wellness programs, that are low cost, high impact ways of driving employee engagement. 4) Always be candid with their employees about the challenges in the healthcare market and the firm's commitment to share the burden in a fair manner.

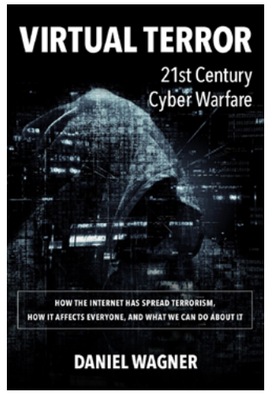
Announcements

In this issue, we highlight two recently published books authored by experts at Risk Cooperative.

GLOBAL RISK AGILITY AND DECISION MAKING

The agile risk manager must be part sociologist, anthropologist, psychologist, and quant. Daniel Wagner and Dante Disparte bring the concept of risk agility to life through a series of case studies that cut across industries, countries and the public and private sectors. In *Global Risk Agility and Decision Making*, Wagner and Disparte, make a compelling case for the need to bring traditional approaches to risk management and decision making into the twenty-first century. The rich, real-world examples underscore how once mighty organizations can be brought to their knees by a failure to do the right thing. The reader is offered deep insights into specific risk domains that are shaping our world, including terrorism, cyber risk, climate change, and economic resource nationalism, as well as a frame of reference from which to think about risk management and decision making in our increasingly complicated world.





VIRTUAL TERROR: 21ST CENTURY CYBER WARFARE

In this extremely timely, important, and compelling book, Daniel Wagner redefines what terrorism has become in the 21st century. Anyone who logs on to the Internet can become a victim of Virtual Terrorism; anyone seeking to do harm to others online can be a virtual terrorist. That is the era we live in now —someone sitting behind a laptop half a world away can interfere with, invade, or take over your life, business, or government.

Virtual terrorists can strike at any time, invisibly and silently. You may never know they are even there, and they may plant malware on your computer that steals your information for years without being discovered. Wagner takes us on a comprehensive tour of the Virtual Terrorism landscape — from cybercrime and bioterrorism to drones and artificial intelligence — to reveal the chilling reality that confronts us all. After reading this book, you may not ever want to log on to your smartphone or the Internet again. The book is a clarion call for individuals, businesses, and governments to rise up against virtual terrorists, for if we fail to do so now, the battle may soon be lost.

Risk Cooperative

LIFE & HEALTH | PROPERTY & CASUALTY | COMPREHENSIVE BENEFITS | SPECIALTY INSURANCE

Risk Cooperative is a specialized strategy, risk and capital management firm founded around the question, what would you do in a world without risk? Risk Cooperative is a licensed brokerage across the full spectrum of risk and insurance solutions.

www.riskcooperative.com