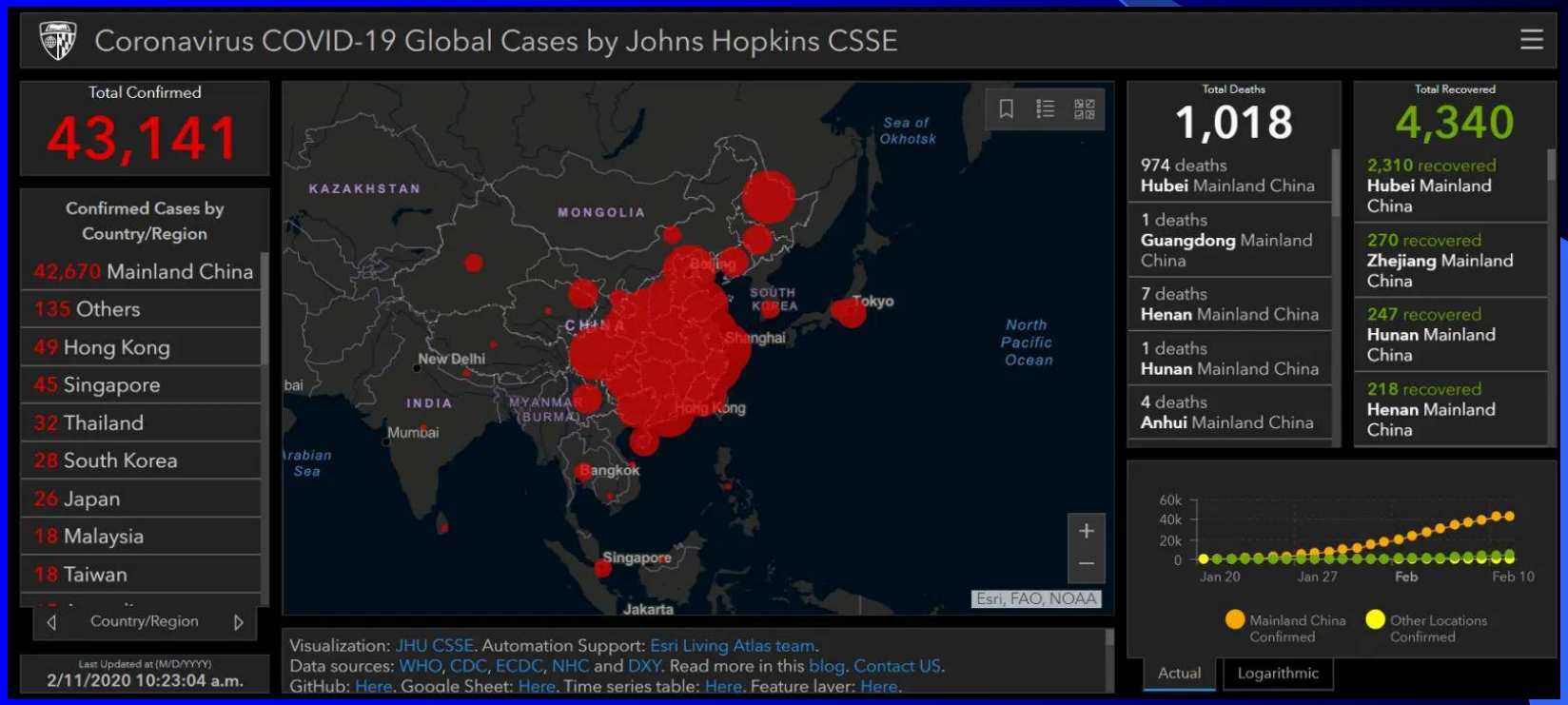
Ethan S. Burger, GULC '89 &
Cyber Intelligence Initiative Instructor,
The Institute of World Politics
eburger@iwp.edu

Cyber-Insurance and the Need for a New Model of the National Interest

Cyber and Future Technologies Society
Army-Navy Club, Washington, D.C. – March 9, 2020

It is Not for Mere Reasons of Happenstance that They Are Called “Computer Viruses”



UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

The Director

Preliminary Guidance to Agencies during Coronavirus Disease 2019 (COVID-19)

MEMORANDUM FOR:
HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

From: DALE CABANISS, DIRECTOR

Subject: Preliminary Guidance to Agencies during Coronavirus Disease 2019 (COVID-19)

On March 3, 2020, President Donald J. Trump announced the formation of the White House Coronavirus Task Force (the Task Force). The Task Force leads the Administration's efforts to monitor, contain, and mitigate the spread of the virus, while ensuring that the American people have the most accurate and up-to-date health and travel information.

At the direction of the Task Force, the U.S. Office of Personnel Management (OPM) provides the following preliminary guidance to the Heads of Executive departments and agencies to prepare the Federal workforce for the potential impacts of Coronavirus Disease 2019 (COVID-19). OPM coordinated this guidance with the National Security Council (NSC), Office of Management and Budget (OMB), Department of State (DoS), the Centers for Disease Control and Prevention (CDC), the Occupational Safety and Health Administration (OSHA), General Services Administration (GSA), Federal Emergency Management Agency (FEMA), and the Federal Protective Service (FPS). This preliminary guidance addresses Federal workforce posture, management of visitors to Federal facilities, and domestic and international travel by Federal employees.

Human Resources Flexibilities for Federal Employees

Over the past month, OPM has released CPM 2020-01 and CPM 2020-02 reminding agencies of the various human resources flexibilities available to assist agencies.

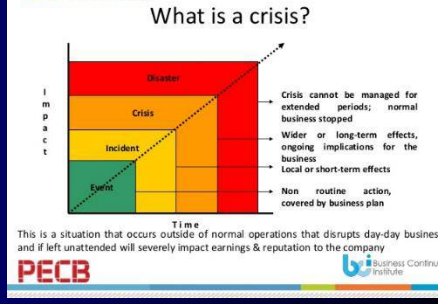
Telework and Federal Mission Resilience

To be prepared for COVID-19, departments and agencies must incorporate telework in their continuity of operations (COOP) plans. The Telework Enhancement Act of 2010 states that "each executive agency shall incorporate telework into the continuity of operations plan of that agency." See 5 U.S.C. § 6504(d) (1). If an agency COOP plan is in operation, that plan "shall supersede any telework policy." See 5 U.S.C. § 6504(d) (2). Therefore, agencies should immediately review their current COOP plans to ensure that telework has been fully incorporated and that as many employees as possible have been identified as telework employees in the plan, and are telework capable (or "telework ready").

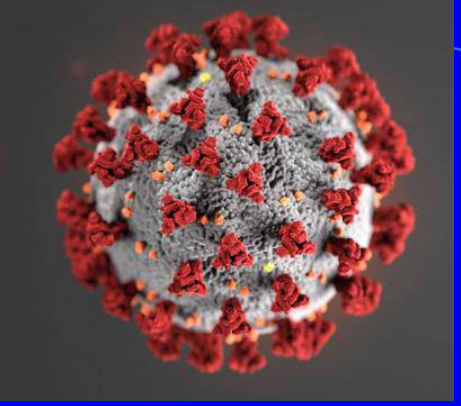
FEMA advises that departments and agencies continue to monitor and prepare for any circumstances that may hinder the performance of essential functions and continue to submit Continuity Status Reports (CSRs) in accordance with Federal Continuity Directive 1.

OPM and OMB plan to host periodic interagency calls concerning questions and issues that arise about relevant human resource issues. In the meantime, agency headquarters-level human resources offices may contact OPM at pay-leave-policy@opm.gov with questions about human resources flexibilities. Agency field offices should contact their appropriate headquarters-level agency human resources office. Individual employees should contact their agency human resources office.

Crisis Management



- Determine appropriate division of federal, state, and local responsibilities. Include relevant officials as part of the process.
- Find funding and allocate resources (including hospitals and skilled personnel) in accordance with applicable rules.
- Coordinate with allies and international organizations as appropriate.
- Determine and implement messaging plans for public.
- Maintaining order and distributing supplies with public and private organizations.
- Address evolving changes in circumstances.



Coronavirus Disease 2019 (COVID-19)
Situation Summary

Background -- CDC is responding to an outbreak of respiratory disease caused by a novel (new) coronavirus that was first detected in China and which has now been detected in almost 90 locations internationally, including in the United States. The virus has been named "SARS-CoV-2" and the disease it causes has been named "coronavirus disease 2019" (abbreviated "COVID-19").

Situation in U.S. In addition to CDC, many public health laboratories are now testing for the virus that causes COVID-19. View CDC's Public Health Laboratory Testing map.

With this increase in testing, now 19 states have reported cases of COVID-19 to CDC. View latest case counts, deaths, and a map of states with reported cases.

U.S. COVID-19 cases include:

- Imported cases in travelers
- Cases among close contacts of a known case
- Community-acquired cases where the source of the infection is unknown.

Uncertainty Reigns

At the time of writing, there are 105,558 confirmed cases of Covid-19, of which 58,354 have recovered, while 3,555 have died. One can follow the progress of the coronavirus as it moves around the world, in real time, thanks to a spell-binding "interactive web-based dashboard" hosted by Johns Hopkins University's Center for Systems Science and Engineering.

Since Jan. 22, the dashboard has shown the location and number of confirmed cases as they are reported, along with casualties and recoveries. Developed to "provide researchers, public health authorities and the general public with a user-friendly tool to track the outbreak as it unfolds," according to a university statement, it lays out the public health crisis in staggering detail.

With panic setting in all over the world, there's a strange sort of relief to be found in seeing the data right there, in black and white (and red, and green). Every new recovery is a moment to celebrate; the relatively flat rate of daily new cases may help make the anxiety a little easier to handle. It helps, too, that the map is intuitive to use and beautifully designed.

Query whether the emergency places any obligations on US persons (legal entities and individuals) to follow good hygiene practices. Should the failure to do so be punished as it puts others at risk?

Risk Assessment
(Cybersecurity is a Form of Risk Management)

Outbreaks of novel virus infections among people are always of public health concern. The risk to the general public from these outbreaks depends on characteristics of the virus, including how well it spreads between people; the severity of resulting illness; and the medical or other measures available to control the impact of the virus (for example, vaccines or medications that can treat the illness). That this disease has caused severe illness, including illness resulting in death is concerning, especially since it has also shown sustained person-to-person spread in several places. These factors meet two of the criteria of a pandemic. As community spread is detected in more and more countries, the world moves closer toward meeting the third criteria, worldwide spread of the new virus. It is important to note that current circumstances suggest it is likely that this virus will cause a pandemic. This is a rapidly evolving situation and CDC's risk assessment will be updated as needed.

Current risk assessment:

- For most people, the immediate risk of being exposed to the virus that causes COVID-19 is thought to be low. This virus is not currently widespread in the United States.
- People in places where ongoing community spread of the virus that causes COVID-19 has been reported are at elevated risk of exposure, with increase in risk dependent on the location.
- Healthcare workers caring for patients with COVID-19 are at elevated risk of exposure.
- Close contacts of persons with COVID-19 also are at elevated risk of exposure.
- Travelers returning from affected international location where community spread is occurring also are at elevated risk of exposure, with increase in risk dependent on the location.
- CDC has developed guidance to help in the risk assessment and management of people with potential exposures to COVID-19.

Highlights of CDC Response

CDC established a COVID-19 Incident Management System on January 7, 2020. On January 21, CDC activated its Emergency Operations Center to better provide ongoing support to the COVID-19 response.

The U.S. government has taken unprecedented steps with respect to **travel** in response to the growing public health threat posed by this new coronavirus: On February 2, the U.S. government suspended entry of foreign nationals who have been in China within the past 14 days.

- U.S. citizens, residents, and their immediate family members who have been in Hubei province and other parts of mainland China are allowed to enter the United States, but they are subject to health monitoring and possible quarantine for up to 14 days. On February 29, the U.S. government announced it was suspending entry of foreign nationals who have been in Iran within the past 14 days.

CDC has issued clinical guidance, including:

- On January 30, CDC published guidance for healthcare professionals on the clinical care of COVID-19 patients.
- On February 3, CDC posted guidance for assessing the potential risk for various exposures to COVID-19 and managing those people appropriately.
- On February 27, CDC updated its criteria to guide evaluation of persons under investigation for COVID-19.
- On February 28, CDC issued a Health Alert Network (HAN): Update and Interim Guidance on Outbreak of COVID-19.

CDC has deployed multidisciplinary teams to support state health departments case identification, contact tracing, clinical management, and public communications.

CDC has worked with the Department of State, supporting the safe return of Americans who have been stranded as a result of the ongoing outbreaks of COVID-19 and related travel restrictions. CDC has worked to assess the health of passengers as they return to the United States and provided continued daily monitoring of people who are quarantined.

An important part of CDC's role during a public health emergency is to develop a test for the pathogen and equip state and local public health labs with testing capacity. After distribution of a CDC RT-PCR test to diagnose COVID-19 to state and local public health labs started, performance issues were identified related to a problem in the manufacturing of one of the reagents. Laboratories were not able to verify the test performance.

CDC worked on two potential resolutions to this problem.

- CDC developed a new protocol that uses two of the three components of the original CDC test kit to detect the virus that causes COVID-19 after establishing that the third component, which was the problem with the original test, can be excluded from testing without affecting accuracy. CDC is working with FDA to amend the existing Emergency Use Authorization (EUA) for the test, but in the meantime, FDA granted discretionary authority for the use of the original test kits.
  - Public health laboratories can use the original CDC test kit to test for the virus that causes COVID-19 using the new protocol.
- Further, newly manufactured kits have been provided to the International Reagent Resource external icon for distribution to state and local public health labs.

Combined with other reagents that CDC has procured, there are enough testing kits to test more than 75,000 people.

In addition, CDC has two laboratories conducting testing for the virus that causes COVID-19. CDC can test approximately 350 specimens per day.

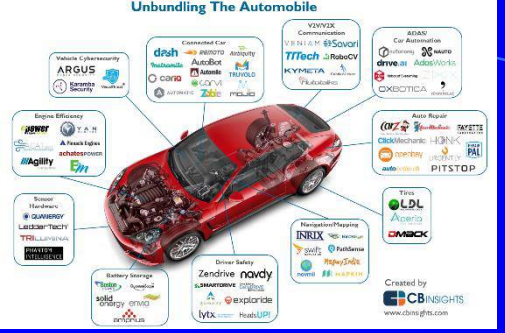
Commercial labs are working to develop their own tests that hopefully will be available soon. This will allow a greater number of tests to happen close to where potential cases are.

CDC has grown the COVID-19 virus in cell culture, which is necessary for further studies, including for additional genetic characterization. The cell-grown virus was sent to NIH's BEI Resources Repository external icon for use by the broad scientific community.

Should Organizations Be Required to Practice Good Cyber-Hygiene as the Failure to Do so Poses a Threat to Others?

Cybersecurity hygiene is a set of practices for managing the most common and pervasive cybersecurity risks faced by organizations today.

1. Identify and prioritize key organizational services, products, and their supporting assets.
2. Identify, prioritize, and respond to risks to the organization's key services and products.
3. Establish an incident response plan.
4. Conduct cybersecurity education and awareness activities.
5. Establish network security and monitoring.
6. Control access based on least privilege and maintain the user access accounts.
7. Manage technology changes and use standardized secure configurations.
8. Implement controls to protect and recover data.
9. Prevent and monitor malware exposures.
10. Manage cyber risks associated with suppliers and external dependencies.
11. Perform cyber threat and vulnerability monitoring and remediation.



Corporate Nationality in a Globalized World

Where was it established?

Where is its headquarters located?

Where are its shares listed?

Consider the location of its:

-- Subsidiaries, Branches, and Business activity.

-- Employees.

-- Sales.

-- Supply chain (contractual relationships).

To what extent should Governments consider corporations as their “responsibility” in light of the above factors? What steps should Governments consider to “defend” their corporations?

North Korea's Attack on SONY. A dangerous precedent. What how should the US Respond?

Model for a Public/Private Partnership for Cyber-Security?

In 2013, President Obama signed Executive Order 13636, which first mandated the National Institute of Standards and Technology (NIST) to develop an approach to combat cybersecurity risks against critical infrastructure. One year later, NIST issued its "Framework for Improving Critical Infrastructure Cybersecurity," which has been widely used by government and private sector organizations.

Other NIST efforts include:

- National Cybersecurity Centers for Excellence
- National Initiative for Cybersecurity Education (NICE)
- Privacy Framework

Query whether there should be a "cybersecurity" national guard? Should there be a licensing scheme of cybersecurity specialists?

Regulation in Lieu of a Cyber: Public/Private Partnership?

- **Robert Knake of the Council on Foreign Relations** has called for the president, and Congress to act swiftly to bring the true state of corporate cybersecurity in the US out into the light. In addition to the expansion of public awareness campaigns, the SEC should require disclosures of intellectual property thefts, allowing markets to determine their impact, and incentivizing better security.
- In fact, the SEC has suggested that more comprehensive cybersecurity information be disclosed on filers' Forms 8-K, 10-Q, and 10-K. 'Material' remediation efforts made by companies to address breaches and the current status of any law enforcement actions or regulatory investigations should be disclosed. New York State has its own requirements in this area. **There is considerable resistance to such mandates in the corporate world.**
- If such measures were adopted the "market" for cyber-insurance might evolve since the extent of the economic consequences of cyber-attacks to the private sector would be more widely appreciated.

Preliminary Observation With Respect to Many Cyber-Insurance Issues: Be Skeptical

- Surveys of management personnel and IT specialists on cybersecurity, particularly those relating to cost issues, often produce data of limited value. The use of collective nouns, inconsistent terms; and imprecise data can produce methodological problems for cybersecurity modeling and research.
- The prevalence of unsubstantiated data within an echo-chamber such as "60 percent of small and mid-size businesses go bankrupt within six months of a cyberattack," attributed to HSB Vice President Eric Cernak (but what is the rate for those not attacked?).
- According to the National Association of Insurance Commissioners, "cyber risk remains difficult for insurance underwriters to quantify due in large part to a lack of actuarial data. Insurers compensate by relying on qualitative assessments of an applicant's risk management procedures and risk culture. As a result, policies for cyber risk are more customized than other risk insurers take on, and, therefore, more costly. The type of business operation will dictate the type and cost of cyber liability coverage."

Council of Economic Advisors, "The Malicious Cost of Cyber Attacks on the US Economy," (2016)

Malicious cyber activity cost the U.S. economy between $57 billion and $109 billion in 2016. Such activity is directed at private and public entities manifests as denial of service attacks, data and property destruction, business disruption (sometimes for the purpose of collecting ransoms) and theft of proprietary data, intellectual property, and sensitive financial and strategic information.

Damages from cyberattacks and cyber theft may spill over from the initial target to economically linked firms, thereby magnifying the damage to the economy. Firms share common cyber vulnerabilities, causing cyber threats to be correlated across firms. The limited understanding of these common vulnerabilities impedes the development of the cyber insurance market.

Cybersecurity is a common good; lax cybersecurity imposes negative externalities on other economic entities and on private citizens. Failure to account for these negative externalities results in underinvestment in cybersecurity by the private sector relative to the socially optimal level of investment. Cyberattacks against critical infrastructure sectors could be highly damaging to the U.S. economy and national security.

Scarce data and insufficient information sharing impede cybersecurity efforts and slow down the development of the cyber insurance market.

Cyber-Insurance & Moral Hazards

Moral Hazard is the concept that parties to a contract have incentives to alter their behavior when their risk or bad-decision making is born by others.

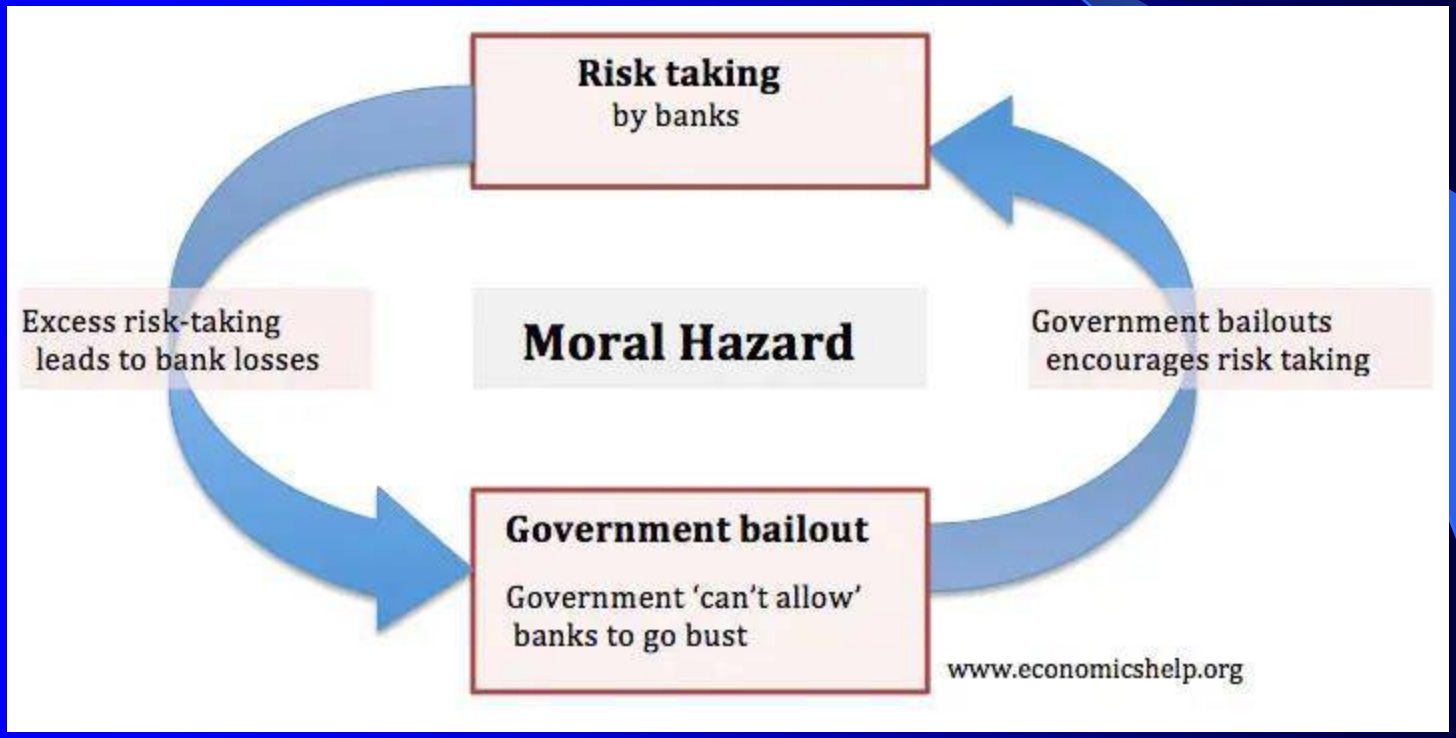
How Moral Hazards applies to cyber-insurance policies:

- Comprehensive insurance policies decrease the incentive for the insureds to defend their assets (data).
- Governments promising to bail out either the insureds or insurance companies (& reinsurers) can encourage the latter actors to take greater risks.

Ergo insureds (& potential insureds) will either self-insure or purchase policies with low face-values. If the insurance (reinsurance) policy issuers believe they will receive a bailout from the Government, they will seek to maximize their profits by placing caps on the number of policies and the value of such policies up to a certain value.

Will the "front-end" sales model for insurance sales make cyber-insurance a PR action for boards or a product not suitable for many companies? Is cyber-insurance subsidizing other insurance products?

Does the Same Dynamic Apply to Cyber-Insurance?



The State of Cyber-Insurance

- The "immature" cyber insurance market fails to supply products that a majority of private organizations deem to be worth buying. This situation is unlikely to change in the foreseeable future.
- Even those organizations that procure cyber-insurance are likely to 'discover' that their policies provide insufficient coverage (e.g., face-values are too low) or inadequate cover (e.g., too many exclusions and reasons for denying claims), forcing these 'insureds' to absorb the costs of cyber-attacks on their own. This situation will often result in litigation coverage issues.
- Many cyber insurance providers and their reinsurers seem to lack sufficient financial assets to cover multiple extreme cyber events, the consequences of which will be felt throughout the insurance industry and the national economy.

∴ *As a result, extreme harm from cyber-attack campaigns against particular geographic areas, the national infrastructure, and particular sectors (e.g., financial, energy), locales (e.g., city clusters), relationships (e.g., users of one cloud provider) will have a cascading effect likely to damage supply chains and consumer confidence, ultimately the magnitude of harm will create crises triggering governmental intervention. Politicians inevitably will feel pressure to intervene.*

Although Officially Agnostic, the Department of Homeland Security Seems To Promote Cyber-Insurance

Cybersecurity insurance is designed to mitigate losses from a variety of cyber incidents, including data breaches, business interruption, and network damage. A robust cyber-insurance market could reduce the number of successful cyber attacks by:

(i) promoting the adoption of preventative measures (good cyber-hygiene in return for more coverage; and

(ii) encouraging the implementation of best practices by basing premiums on an insured's level of self-protection (good cyber-hygiene).

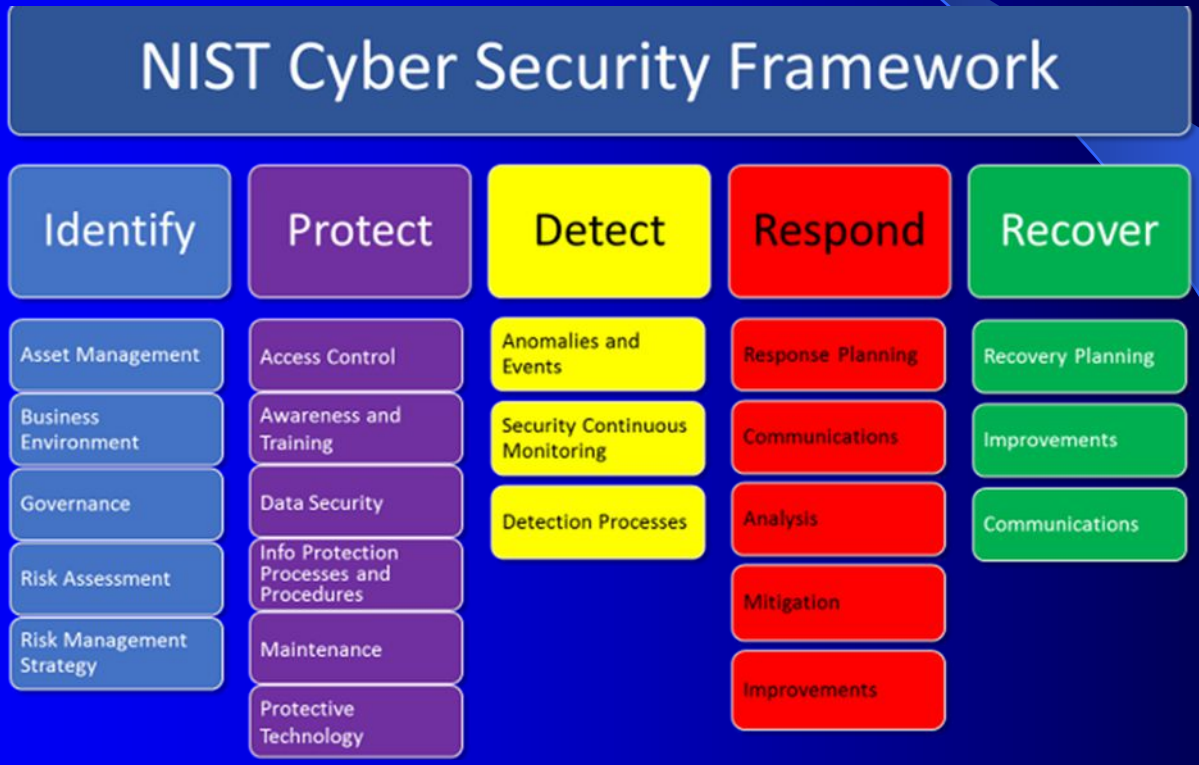
Since "cyber" is a cross-border phenomenon, is it appropriate for cyber-insurance is regulated by state governments? Should cyber-insurance policies meet some federal standard?

The **Cybersecurity Information Sharing Act of 2015**

- This Act was designed to "improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes".
- The law allows the sharing of Internet traffic information between the U.S. government (e.g. law enforcement) and technology and manufacturing companies, without antitrust risk. The bill was introduced in the U.S. Senate in 2014, and passed in the Senate in 2015.
- Opponents question Cybersecurity and Infrastructure Security Agency's value, believing it will move responsibility from private businesses to the government, thereby increasing vulnerability of personal private information, as well as dispersing personal private information to appropriate federal and state government bodies.

Can Organizations Achieve Meaningful Cybersecurity'?

What metrics to use? Individual organizations? Systemic approach? Cyber Maginot Line?



Full Disclosure:
My Views Have Been Strongly Influenced by:

- Lloyd's/Cyence, *Counting the cost: Cyber exposure decoded," Emerging Risks Report 2017 Technology*, July 2017 (the Lloyd's Study);
- Martin Ering & Jan Hendrick Wirfs, *Cyber Insurance: Too Big to Insure, Institute of Insurance Economics*, University St. Gallen, 2016, (the 'IIE Study'); and
- Sasha Romanosky, et al., *Content Analysis of Cyber Insurance Policies: How do carriers write policies and price cyber risk*, Rand White Paper (Draft), 2017 (the 'Rand Study').

Lloyd's Study on Insurance Industry's Cyber Risk

- Lloyd's of London issued a study suggesting that a global cyber-attack could cause harm greater than $53 billion (on average), and possibly as high as $121 billion.
- The larger of these sums exceeds the damage caused by any natural disaster in the U.S. since 1980 – excluding Harvey ($125 Billion), Katrina ($105 billion), Maria ($90 Billion), California Fires, and Sandy ($70 billion).
- According to Munich Re, in 2017, total insured losses from natural disasters $135 Billion with total losses of $330 Billion (the highest ever was $354 Billion in 2011).

IIE Study's Key Findings

'Cyber risks of daily life' are usually insurable (e.g. data privacy risks). Nonetheless, organizations generally under-insure in cybersecurity. 'Questionnaire only' applications are unlikely to result in suitable cyber-insurance policies. Both organizations and the public benefit if the organizations go through the underwriting process. Completing an insurance application is an educational exercise, forcing one to think about cybersecurity, develop written cybersecurity policies, practices, and procedures), discuss cyber issues, inventory assets, preparing plans, etc. Sometimes insureds are afraid of the consequences of making an insurance claim.

'Extreme Scenarios' (e.g., a breakdown of the critical infrastructure) are difficult to insure, given the lack of good actuarial data, cumulative risk, and other problems of insurability. These scenarios are extremely likely to materialize in the next ten years.

Hence, a two-tier approach might be appropriate:

(i) improve insurability for 'cyber risks of daily life'' and engage in industry-wide cooperation; and

(ii) address 'extreme scenarios' to the extent possible (e.g. look towards government programs and sector initiatives).

Why is the Cyber-Insurance Market Not 'Mature'?

- Insufficient actuarial data to support meaningful underwriting (unlike automobile, home-owner, and maritime insurance). Lack of trust between insurance companies and potential insureds. Are the applications complete and candid? If they are not, insureds will have difficulty collected on claims.
- Insurance companies are eager to write cyber-insurance policies to cash in on a new market, albeit with an insufficient understanding of their potential financial exposure due to cumulative risk. As a consequence, there are incentives for insurance companies to find reasons for denying coverage.
- Cyber-insurance policies lack standard (and tested) language. Cyber-insurance is not a commodity since it is crafted for the insureds, whose profiles vary considerably. Litigation outcomes are unpredictable.
- Key development: Allianz will provide discounted cyber security insurance coverage to customers that use certain Apple devices and Cisco security products. Aon will perform security consulting.

Consider the Implications of Wanna Cry & [Not]Petya Cyber-Attacks (2017)

- These viruses were propagated without human intervention, but they are **not regarded as very sophisticated**. Estimated to have caused harm in the low billions of dollars, almost all of which will not be covered by insurance.
- Whereas **Wanna Cry** ransomware was designed for financial gain, **NotPetya** seems to have been politically driven (**attributed by UK and US to Rus**sia(– seeking to maximize harm. Initial attacks against Ukrainian state bodies, it spread to DLA Piper (a U.S. firm), FedEx (U.S. delivery service company), MAERSK (Danish-based shipping company), Merck (U.S, pharmaceutical company), Rosneft (Russian oil company), and many others.
- **Good cyber-hygiene practices could have prevented infection.** Only a minority of the victims carried stand-alone cyber insurance. But the common exclusions for failing to install patches, nation-state attackers, or otherwise failing to follow good cybersecurity practices are likely to prevent recoveries from insurers.

Cost of a Data Breach Report (IBM/Ponemon 2019)

- For the 2019 Cost of a Data Breach Report (the "Study"), IBM recruited 507 organizations that have experienced a breach in the last year and interviewed more than 3,211 individuals who are knowledgeable about data breach incidents in these organizations. The first data points IBM collected from these organizations were the number of customer records lost or stolen in the breach and what percentage of their customer base was lost following the data breach.
- In the course its interviews, IBM also asked questions to determine what the organization spent on activities detecting the breach and the immediate response to the data breach, such as forensics and investigations, and those conducted in the aftermath of discovery, such as the notification of victims and legal fees. Other issues studied that influence the cost are the root causes of the data breach and the time to detect and contain the incident (the data breach lifecycle).

NOTE: THE IBM STUDY IS DISCUSSED IN THE APPENDIX.

The Average Total Cost of Data Breach in the US in 2019 was $8.19 million

In the United States, the average cost of a data breach increased from $7.91 million in 2018 to $8.19 million in 2019 which is the highest cost globally when compared to other regions. Globally, the average cost of a data breach has increased to $3.92 million.

The Council of Insurance Agents & Brokers (The Council), Cyber Survey Fall 2018's Key Findings

Market Trends

32% of respondents' clients purchased at least some form of cyber coverage 33% of respondents' clients purchased at least some form of cyber coverage

32% of those clients who purchased cyber insurance, 32% were first-time buyers

34% of respondents' clients increased their coverage within the past six months

67% of those with cyber insurance have standalone policies

Pricing Trends

$2.8 M was the typical cyber insurance policy limit

87% of respondents said premium prices either stayed the same or decreased over the last six months

Underwriting

65% of respondents did not see any tightening of carrier underwriting practices in the last six months

23% of respondents believed there was not adequate clarity as to what is included and excluded in a cyber policy

79% of respondents noted that capacity in the market is either plentiful or increasing

Cybersecurity/Cyber Risk

85% of respondents' firms have a strategic approach to marketing and educating clients about cyber risks

37% of respondents' clients have an information security program in place focused on prevention, detection, containment and response

Principal Properties of Cyber Risks

- Cyber-losses results in both short-tail and long-tail losses.
- There are 1st and 3rd Party (i.e., property and liability) losses.
- Cyber losses are not independent events (correlations between cyber risk).
- Cyber insurance market has a small number of providers (≈ 60) and as percentage of portfolio value .
- Human beings are the weakest link (victims of social engineering & negligence)
- Uncertainty about data (modeling approaches untested actuarial standards).
- Risk of change (historical data is not necessarily a good indicator of the future).
- Extreme events are difficult to estimate (low frequency, high severity occurrence).
- Insurance coverage limited (high deductibles are common).

Some Common Cyber Insurance Policy Exclusions

- Data taken from paper and similar records.
- Employee privacy claims for released data.
- Fraud, intentional, and illegal misconduct committed by insured.
- Lack of cyber-hygiene (failure to encrypt data or install software updates and security patches).
- Mechanical/electronic failure and other acts of God.
- Mobile electronic devices (computers, cell phones, etc.).
- **Nation-states, organized criminal groups, and terrorists (and persons acting on their behalf). Attribution issues will arise, but how is the final coverage decision reached? It will be a costly, inexact process.**
- Patent, software, copyright infringement.
- Prior notice (knowledge, suspicions).
- Secondary liability for personal injury & property damage.
- Vicarious liability for data breaches by third-party vendors.

Disquieting Questions About Cyber-Insurance

- If the global value of cyber-insurance premiums written is estimated at $3.5bn, but the global cost of cyber-crime exceeds $450bn annually (see Aon chief warns that insurance industry is losing its relevance, FT, 4/25/2018) can the ‘cyber-insurance market’ be viable? Can these numbers be trusted?
- When the cyber-insurance policy is in force, how can insurers be confident that the insureds’ cybersecurity ‘baseline’ are being observed?
- Rather than a cyber 9/11 or Pearl Harbor, is the interconnected of the economy and the Internet of Things likely to cause a collapse in consumer and business confidence.

Expanded Role for NIST?

In 2013, President Obama signed Executive Order 13636, which first mandated the National Institute of Standards and Technology (NIST) to develop an approach to combat cybersecurity risks against critical infrastructure. One year later, NIST issued its "Framework for Improving Critical Infrastructure Cybersecurity," which has been widely used by government and private sector organizations.

Other NIST efforts include:

- National Cybersecurity Centers for Excellence
- National Initiative for Cybersecurity Education (NICE)
- Privacy Framework

Query whether there should be a "cybersecurity" national guard? Should there be a licensing scheme of cybersecurity specialists?

What's a Government to Do?

The Federal Government (alone or with National Association Insurance Commissioners) can:

Promote through incentives the use of standardized insurance policy provisions and language to promote underwriting standards to strengthen the cyber-insurance market;

Create cyber-insurance policy pools (to date Congress has rejected giving small business tax incentives to buy cyber insurance; and

Establish either federal flood or terrorism-like programs (but Flood Insurance Program is insolvent).

Two Obstacles:

- Lack of political consensus of relevant roles and responsibilities of government (note Flood Insurance Program has a huge deficit).
- Given problems with the Affordable Care Act, is it realistic to expect the government to take on role of national cyber hygienist?

Appendix

The Convention on Cybercrime

An European Union-led effort, the Convention aims principally at:

- Harmonizing the domestic criminal substantive law elements of offences and connected provisions in the area of cyber-crime;
- Providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offenses as well as other offenses committed by means of a computer system or evidence in relation to which is in electronic form; and
- Setting up a fast and effective regime of international cooperation.

In the absence of a desire to observe implement mutual legal assistance treaties (when they exist) and political will, the Convention has not proven to achieve the goals for which many had hoped. Note that China, Iran, North Korea and Russia are not signatories.

IBM Study Findings (1of 3)

- Lost business was the biggest contributor to data breach costs.
- Data breach costs impacted organizations for years.
- The lifecycle of a data breach was longer than previously believed (i.e. long-dwell times and delayed attacks following initial attacks).
- Malicious attacks were the most common and most expensive root cause of breaches.

IBM Study Findings (2 of 3)

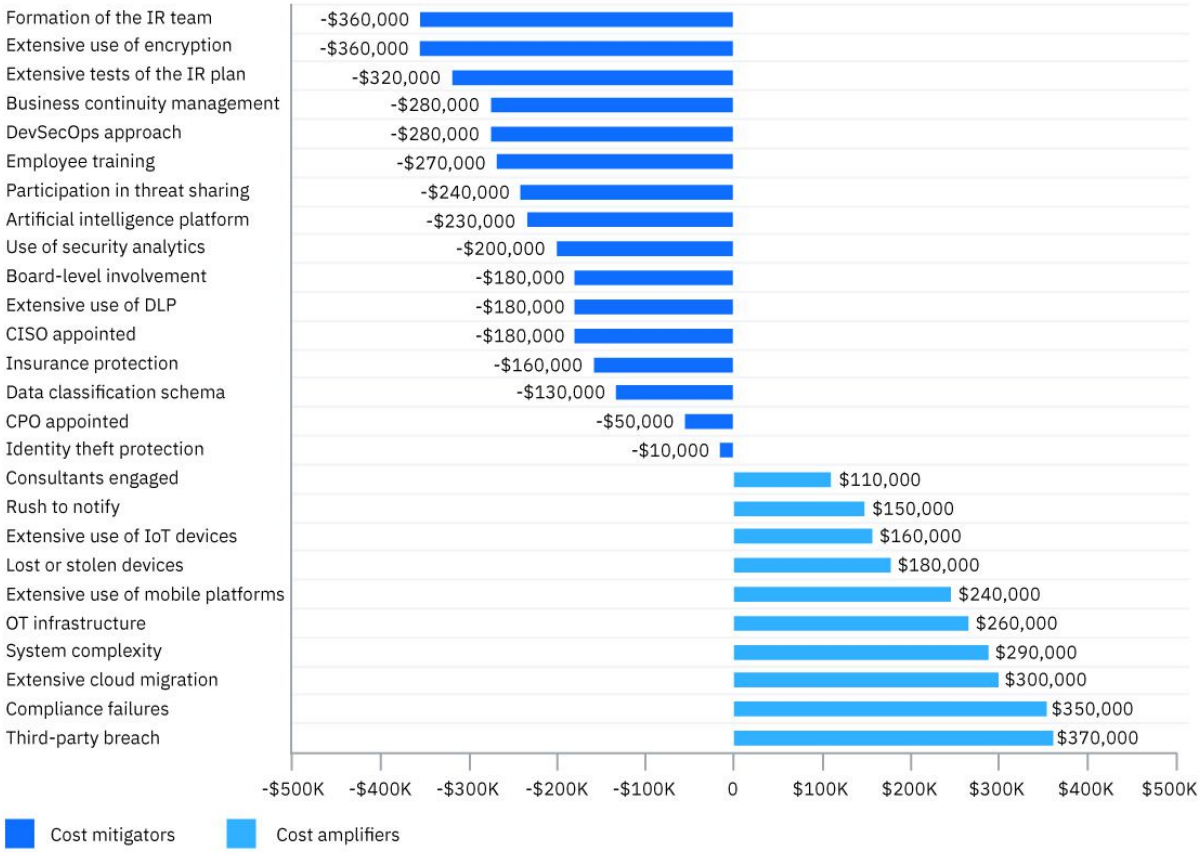
- Breaches from system glitches and human error still cost millions. Beware of the insider threat acting alone or as part of a larger operation.
- Small businesses face disproportionately greater percentage costs relative to larger organizations.
- Cloud migration, IT complexity, and third-party breaches were cost amplifiers.
- Encryption, business continuity management, DevSecOps and threat intelligence sharing were cost mitigators.

IBM Study Findings (3 of 3)

- Companies studied that had an incident response team and extensive testing of their response plans saved over $1.2 million (low figurer).
- Automation of security reduced costs.
- Region and industry impacted total costs.
- The odds of experiencing a data breach have increased in recent years.

How factors increase or decrease the total cost of a data breach

Difference from average total cost of US $3.92 million



Lost Business Was the Biggest Contributor to Data Breach Costs (IBM)

- The loss of customer trust had serious financial consequences for the companies studied, and lost business was the largest of four major cost categories that contributed to the total cost of a data breach.
- The average cost of lost business for organizations in the 2019 study was $1.42 million, which represents 36% of the total average cost of $3.92 million. The study found that breaches caused abnormal customer turnover of 3.9% in 2019.
- Whereas organizations that lost less than one percent of their customers due to a data breach experienced an average total cost of $2.8 million, organizations with customer turnover of 4% or more averaged a total cost of $5.7 million – 45% greater than the average total cost of a data breach.

Data Breach Costs Impact Organizations Over Time (IBM)

- About one-third of data breach costs occurred more than one year after a data breach incident in the 86 companies IBM were able to study over multiple years.
- While an average of 67% of breach costs came in the first year, 22% accrued in the second year after a breach, and 11% of costs occurred more than two years after a breach. **The long-tail costs** of a breach were higher in the second and third years for organizations in highly regulated environments, such as the healthcare and finance industries. Consider the implication of the sales mode for cyber-insurance policies.
- Organizations in a high-data protection regulatory environment saw 53% of breach costs in the first year, 32% in the second year and 16% more than two years after a breach.

Life Cycle of a Data Breach Was Longer (IBM)

- The time between when a data breach incident occurred and when the breach was finally contained (also known as the breach lifecycle) grew noticeably between 2018 and 2019.
- The average time to identify a breach ("**dwell time**") in 2019 was 206 days and the average time to contain a breach was 73 days, for a total of 279 days. This represents a 4.9% increase over the 2018 breach lifecycle of 266 days. However, the faster a data breach can be identified and contained, the lower the costs.
- Breaches with a lifecycle less than 200 days were on average $1.22 million less costly than breaches with a lifecycle of more than 200 days ($3.34 million vs. $4.56 million respectively), a difference of 37%.

Malicious Attacks Were the Most Common and Most Costly Types of Attacks (IBM)

- The study found that data breaches originating from a malicious cyber attack were not only the most common of the breaches studied, but also the most expensive.
- Since 2014, the share of breaches caused by malicious attacks surged by 21%, growing from 42% of breaches in 2014 to 51% of breaches in 2019. It took substantially longer to identify and contain a breach in the case of a malicious attack: a combined 314 days, for a breach lifecycle that was 12.5% longer than the average breach lifecycle of 279 days.
- This finding helps explain why breaches caused by a malicious attack were 27% more costly than breaches caused by human error ($4.45 million vs. $3.5 million) and 37% more costly than a breach caused by system glitches ($4.45 million vs $3.24 million).

Costs from System Breaches and Human Error are Still Higher (IBM)

- While malicious breaches were most common, inadvertent breaches from human error and system glitches were still the root cause for nearly half (49%) of the data breaches studied in the report.
- Human error as a root cause of a breach includes "inadvertent insiders" who may be compromised by phishing attacks or have their devices infected or lost/stolen. These were responsible for about one-quarter of breaches.
- System glitches, or inadvertent failures that could not be tied to a human action, accounted for another quarter of breaches. While less expensive than malicious attacks, system glitches and human error breaches are still costly, with an average loss of $3.24 million and $3.5 million respectively.

Small Organizations Find the Costs due to Cyber-Attacks are Proportionally High (IBM)

- We found significant variation in total data breach costs by organizational size. The total cost for the largest organizations (more than 25,000 employees) averaged $5.11 million, which is $204 per employee.
- Smaller organizations with between 500 and 1,000 employees had an average cost of $2.65 million, or $3,533 per employee. Thus, smaller organizations have higher costs relative to their size than larger organizations, which can hamper their ability to recover financially from the incident.

Cloud migration, IT complexity, and Third-Party Breaches Were Cost Amplifiers (IBM)

- Out of 26 factors we studied contributing to the cost of a data breach, the five that contributed the most cost were third-party involvement, compliance failures, extensive cloud migration, system complexity, and operational technology (OT).
- If a third party caused the data breach, the cost increased by more than $370,000, for an adjusted average total cost of $4.29 million. Organizations undergoing a major cloud migration at the time of the breach saw a cost increase of $300,000, for an adjusted average cost of $4.22 million.
- System complexity increased the cost of a breach by $290,000, for an average cost of $4.21 million.

Encryption, Business Continuity Management, DevSecOps and Threat Intelligence Sharing Were Cost Mitigators (IBM)

- Among the 26 cost factors we studied, there was a diverse set of cost mitigators that either helped reduce costs preventatively or in the aftermath of a breach.
- Extensive use of encryption, data loss prevention, threat intelligence sharing and integrating security into the software development process (DevSecOps) were all associated with lower-than-average data breach costs.
- Among these, encryption had the greatest impact, reducing breach costs by an average of $360,000. Business continuity management in the aftermath of a breach reduced the total cost of a data breach by an average of $280,000.

Companies Studied That Had An Incident Response Team and Extensive Testing of Their Response Plans Saved Over $1.2 Million (IBM)

- An organization's ability to respond effectively after a data breach was strengthened by the presence of an incident response (IR) team that follows an incident response plan. In this year's research, IBM found that organizations with an incident response team amplified their cost-savings by also conducting extensive testing of their IR plan, such that the combined effect of the IR team and IR plan testing produced a greater cost savings than any single security process.

- Those organizations who conducted extensive testing of an IR plan had an average total cost of a breach that was $1.23 million less than those that neither had an incident response team or tested their incident response plan ($3.51 million vs. $4.74 million). Testing the incident response plan, through exercises such as tabletop exercises or simulations of the plan in an environment such as a cyber range, helped teams respond faster and potentially contain the breach sooner.

Automation of Security Reduces Costs (IBM)

- Organizations that had deployed automated security solutions that reduce the need for direct human intervention – including the use of security solutions with artificial intelligence, machine learning, analytics, and automated incident response orchestration – saw significantly lower costs after experiencing a data breach.
- Organizations that had not deployed security automation experienced breach costs that were 95% higher than breaches at organizations with fully-deployed automation ($5.16 million average total cost of a breach without automation vs. $2.65 million for fully-deployed automation). Breach costs at organizations without automation deployed were far costlier in 2019 than in 2018, going up from an average of $4.43 million in 2018 to $5.16 million in 2019, an increase of more than 16%.
- Breaches at organizations with fully deployed automation decreased in cost from 2018 to 2019. Those breaches decreased in cost by 8%, from an average of $2.88 million in 2018 to $2.65 million in 2019.

Region and Industry Impacted Total Costs (IBM)

- Continuing a multi-year trend, data breaches in the U.S. were vastly more expensive than those in other nations, with an average total cost of $8.19 million (more than double the global average). The U.S. average total cost has increased 130% over the 14 years of the study, up from $3.54 million in 2006.
- Organizations in the Middle East reported the highest average number of breached records (38,800 per incident, compared to global average of around 25,500)
- For the ninth year in a row, healthcare organizations had the highest costs associated with data breaches at $6.45 million – over 60% more than the global average of all industries.

The Odds of Experiencing a Data Incident Has Increased (IBM)

- The percentage chance of experiencing a data breach within two years was 29.6% in 2019, an increase from 27.9% in 2018. In 2014, organizations had a 22.6% chance of experiencing a breach within two years.
- In the span of six years, the likelihood of experiencing a breach within two years grew by 7 percentage points (700 basis points), representing a 31% increase in the odds of experiencing a breach within two years.
- In other words, organizations in the 2019 study were nearly one-third more likely to experience a breach within two years than they were in 2014.

Victims of Cyber Attacks by Breach (Verizon Report 2019)

43% -- Small Businesses

16% -- Public Utilities

15% --Healthcare Organizations

10% -- Financial Institutions

Tactics Used by Attacker (Verizon Report 2019)

52% -- Hacking

33% -- Accomplish through Social Engineering

28% -- Malware

21% -- Employee Errors

15% -- Misuse by Authorized Users

4% -- Involved Physical Actions

Who's Behind the Breach (Verizon Report 2019)

69% -- Outsiders

34% -- Insiders

39% -- Organized Crime Group

23% -- Nation-State

5% -- Multiple Parties

2% -- Business Partners

Other Commonalities (Verizon Report 2019)

71% -- Financially Motivated

56% -- Took Months or Longer to Discover

32% -- Involved Phishing

29% -- Involved Stolen Credentials

25% -- Motivated by the gain of strategic advantage (espionage)

CONTACT ME WITH ANY FOLLOW-UP QUESTIONS

ETHAN S. BURGER

eburger@iwp.edu or 917-291-3362.