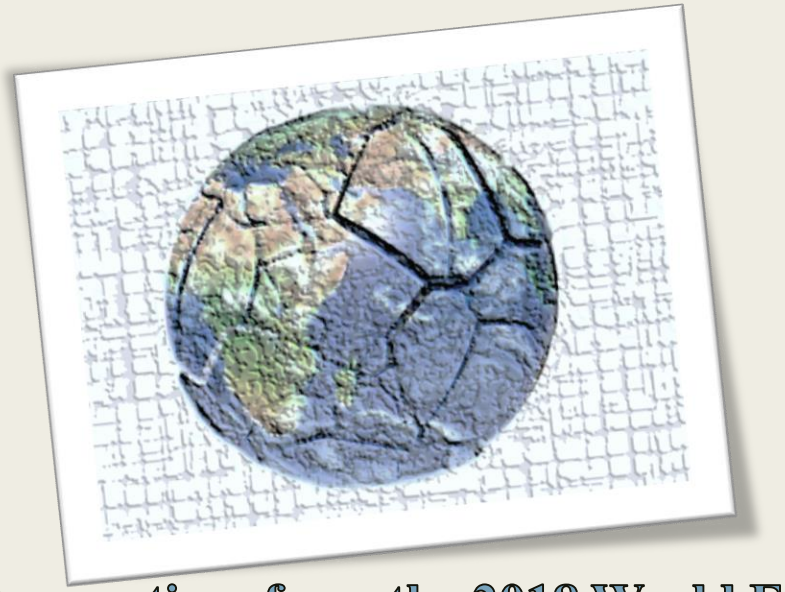
ENVIRONMENTAL AND TECHNOLOGICAL RISKS | CREATING A SHARED FUTURE IN A FRACTURED WORLD



Perspectives from the 2018 World Economic Forum Global Risks Report, Hurricane Harvey and the Maersk Cyberattack

Texas Southern University

Maritime Transportation Management and Security

James R Bryant, MSIA

April 18, 2018

Agenda

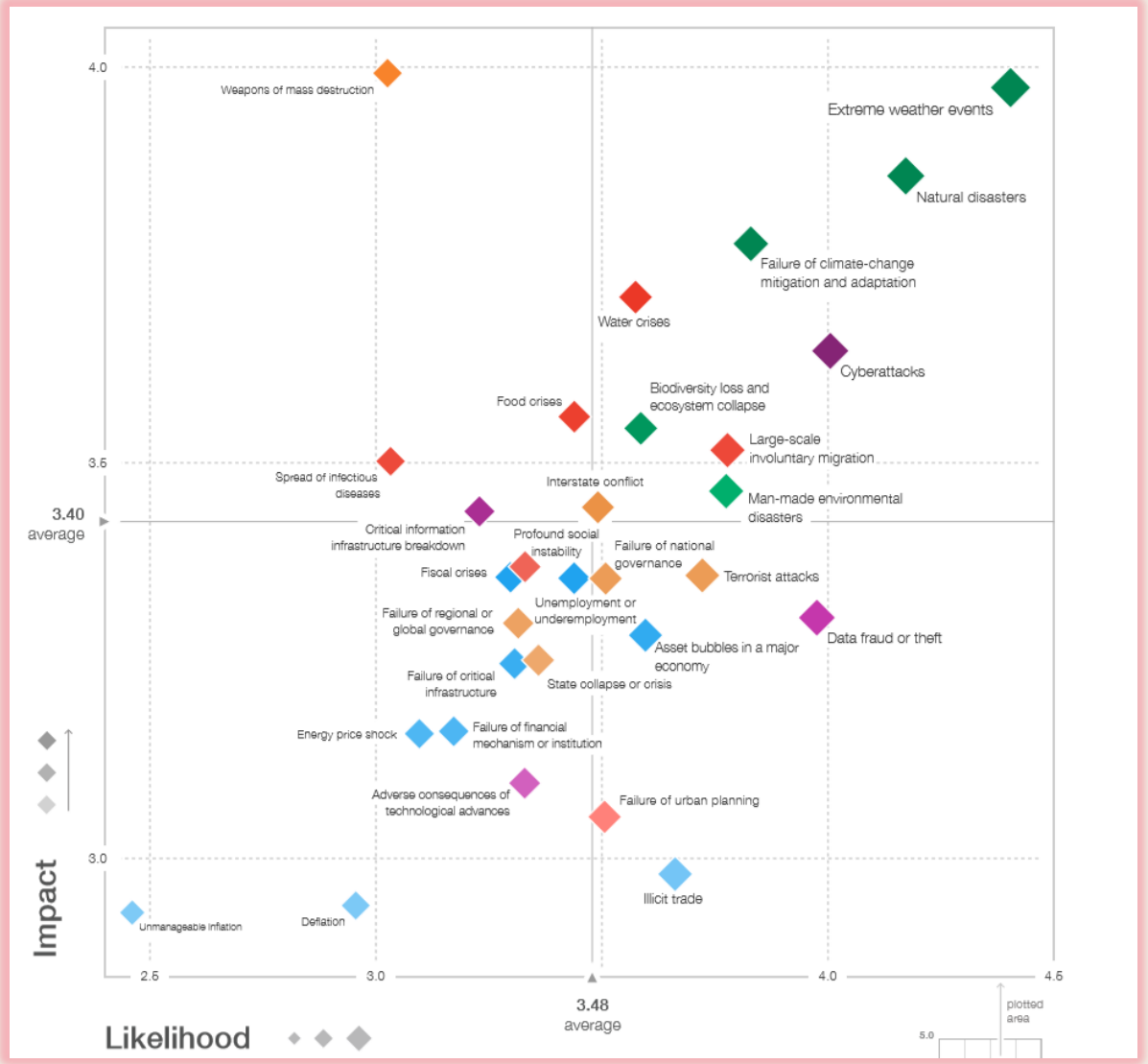
- *World Economic Forum Overview*
  - *The Global Risks Report and Perceptions Survey*
    - *Environmental Risks*
      - *Hurricane Harvey*
      - *Climate Events*
    - *Technological Risks*
      - *Maersk Cyberattack Case Study*
        - *Petya/NotPetya 101*
      - *Risk Management Framework*
    - *Lessons Learned*
- *Creating a Shared Future in a Fractured World*

The **World Economic Forum** is an independent international organization committed to improving the state of the world by engaging business, political, academic and other leaders of society to shape global, regional and industry agendas.
www.weforum.org

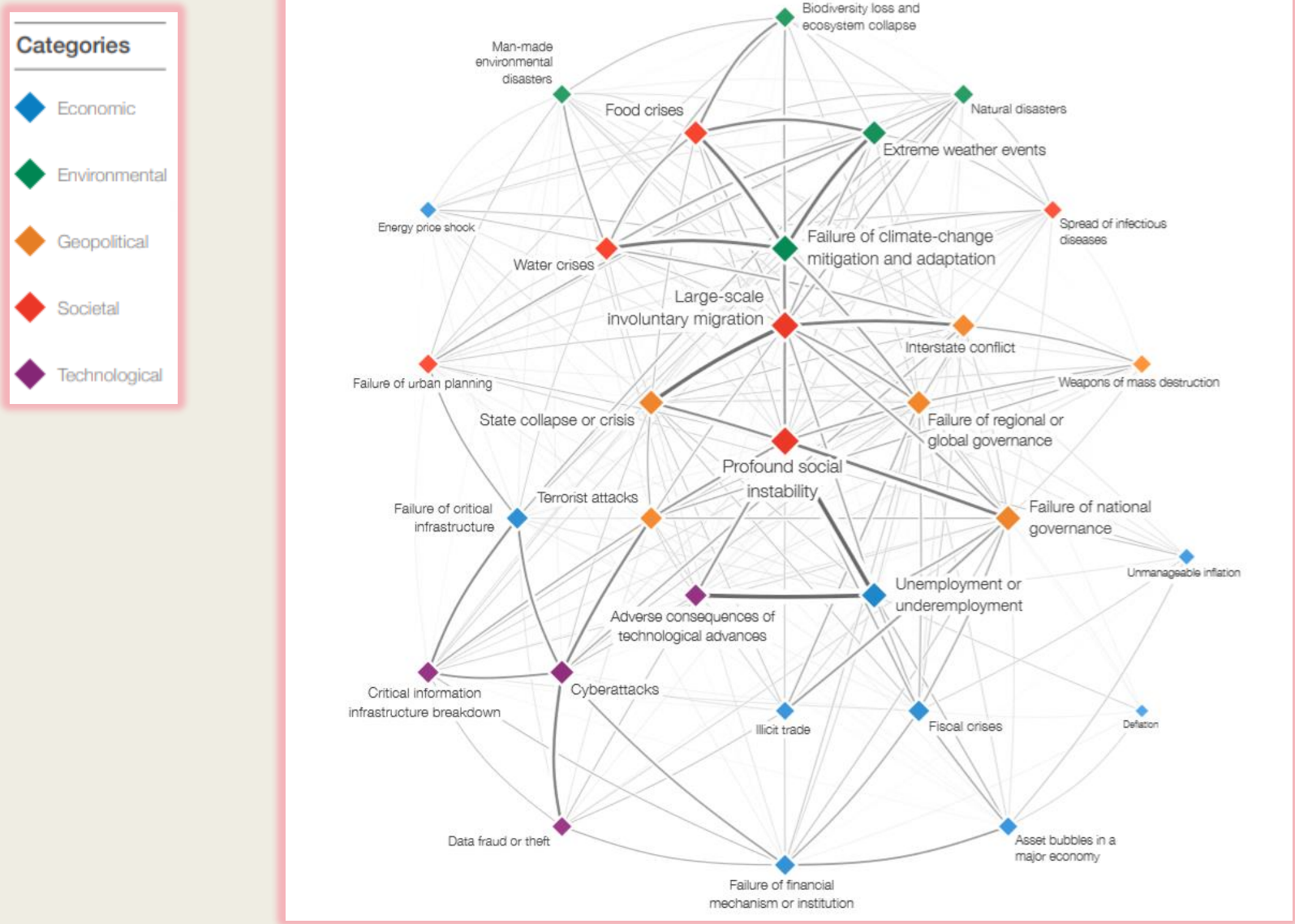
www.weforum.org/reports/the-global-risks-report-2018

The global risks landscape captures the challenges we face

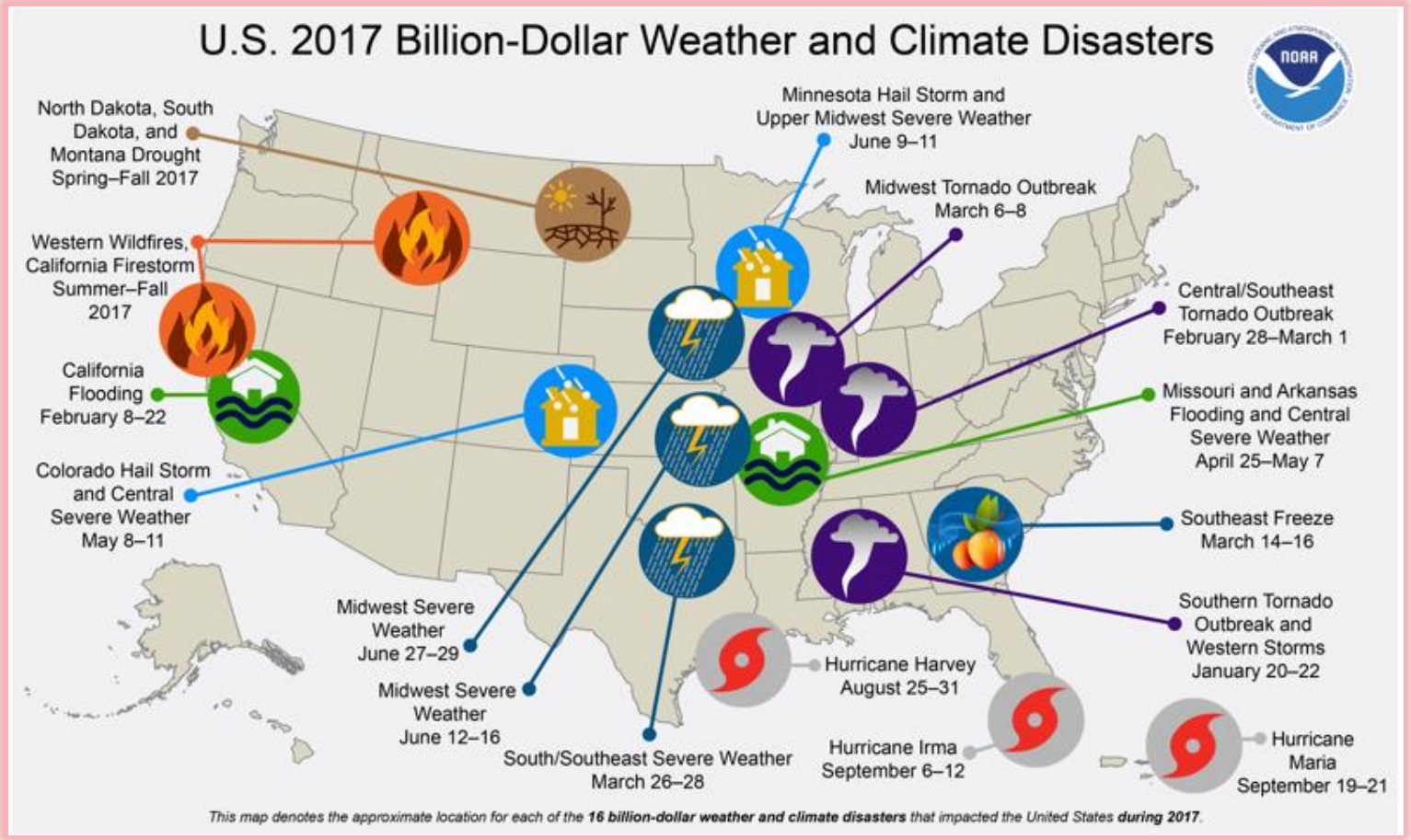
https://www.youtube.com/watch?v=shb98NRhfqE



Global risks interconnections exacerbate the situation



Environmental risks can be devastating



More notable than the high frequency of these events was the cumulative cost, which **exceeded $300 billion in 2017** — a new U.S. annual record. The cumulative damage of these 16 U.S. events during 2017 is $309.4 billion (CPI-adjusted to present), which shattered the previous U.S. annual record cost of $219.2 billion (also CPI-adjusted) that occurred in 2005 from the impacts of Hurricanes Dennis, Katrina, Rita and Wilma.

....Disruptive and controversial

Chron | Local | US & World | Sports | Business | Entertainment | Life | Jobs | Cars | Real Estate

152677 items matched your search for hurricane harvey

Section | Type | Sort By: Date | Relevance

Heroes of Hurricane Harvey

April 12, 2018

Heroes of Hurricane Harvey | Houston Chronicle | Chron.com Get the latest news and information on Hurricane Harvey. news/houston-weather/hurricaneharvey/heroes

Hurricane Harvey

February 15, 2018

Hurricane Harvey | Houston Chronicle | Chron.com Get the latest news and information on Hurricane Harvey. news/houston-weather/hurricaneharvey

Could this product have saved your car from Hurricane Harvey?

April 13, 2018 | *Fernando Alfonso III*

: The story behind the viral Hurricane Harvey movie poster, and its redesign As a way to fund his idea, Dela Fuerte went on the Philippines' "The Final Pitch," which is similar to "Shark Tank" in the U.S. ...

Houston home sales tumble for first time since Hurricane Harvey

April 11, 2018 | *Nancy Sarnoff*

Nancy Sarnoff Houses are taking longer to sell and sales across the region fell last month for the first time since Hurricane Harvey, a new housing report shows. ... RELATED: Development tactic questioned in ...

From HoustonChronicle.com

Get All Digital Access to Houston's top stories and in-depth investigative journalism

Hurricane Harvey: A closer look at Houston's biblical floods

March 22, 2018

Hurricane Harvey: A closer look at Houston's biblical floods Dive deep into our coverage of the city's worst flooding storm, exclusively on HoustonChronicle.com. ... Hurricane Harvey was Houston's reckoning ...

Damaged and defiant: Hurricane Harvey

February 5, 2018

Houston holds strong in the wake of devastation left by Hurricane Harvey. Toggle navigation Project home Deeper Dive 51 Inches Lost in Cypress Creek Gun Hunters of Harvey A home lost, but not hope Special ...

Houston's proposed floodplain development rules would have spared thousands during Harvey, city says

By Mike Morris Updated 5:29 pm, Tuesday, March 13, 2018

6

Photo: David J. Phillip, STF

Climate change made Harvey's 51 inches of rain 3 times more likely, scientists say

By Alex Stuckey Updated 1:27 pm, Wednesday, December 13, 2017

29

Shell joins Exxon in the climate change spotlight

By Jordan Blum | April 13, 2018

12

Cyberattacks are perceived as the global risk of highest concern to business leaders in advanced economies

https://www.marsh.com/content/dam/marsh/Documents/PDF/US-en/Marsh%20Microsoft%20Global%20Cyber%20Risk%20Perception%20Survey%20February%202015.pdf

Maersk Cyberattack Case Study

- A.P. Moller-Maersk handles one out of seven containers shipped globally and operates in 121 countries, serving 343 ports
- Maersk was hit by the NotPetya virus. The cyber assault cost $250-$300 million and required 10 days to recover fully. Russia was blamed
- Due to the attack in June 2017, Maersk's entire global IT infrastructure had to be shut down. 4,000 new servers, 45,000 new PCs, and 2,500 applications had to be reinstalled in the short period. A remarkable feat
- While down, Maersk operated manually and kept up with 80% of their typical workload
- Post mortem, Maersk's Chairman said they had "basically average" cyber security management; however, the attack was a "wake-up call"

Petya/NotPetya 101

On June 27, 2017, a ransomware variant titled Petya/NotPetya was reported to be spreading across Europe. Since then, it has spread to at least 65 countries. This new variant exercises unique methods of both infection and propagation. Read on to learn more.

1. **Trusted software updates were used by Petya/NotPetya to initially infiltrate devices** – A legitimate software updater process (EzVit.exe) from M.E.Doc, a Ukrainian company offering tax software, is believed to have been the victim of software update hijacking which was responsible for the initial infections of Petya/NotPetya. These compromised updates were trusted by computers running the relevant software. Therefore, the hidden malicious code was able to slip past most defenses when EzVit.exe was downloaded and executed.

2. **Petya/NotPetya exhibits worm-like behavior –** After obtaining the current user credentials of infected machines via either the command line, the CredEnumerateW Windows API, or through two executables embedded within Perfc.dat, Petya/NotPetya attempts to spread laterally to other devices on the local network. Petya/NotPetya utilizes PsExec or WMI, and the obtained user credentials or token to install its wiper-ware on targeted devices. If these devices have not yet applied the Microsoft MS17-010 patch, Petya/NotPetya will utilize the EnternalBlue or EternalRomance exploit (depending on the user's operating system) to compromise the systems.

3. **Petya/NotPetya's encryption was not designed to be reversed –** If administrative access was obtained, Petya/NotPetya will overwrite the master boot record (MBR) code. During this process, it schedules a task to reboot the machine and then attempts to encrypt the master file table (MFT). Once the computer has been rebooted, the MFT is removed, preventing the computer from normally booting, even if decryption keys could be received.

For more information, please visit:

New ransomware, old techniques: Petya adds worm capabilities

New Ransomware Variant "Nyetya" Compromises Systems Worldwide

Petya, dead but still dancing

Best practices moving forward for Petya/NotPetya et al.

Patching ≠ Security	**Just because a patch is available *does not* mean it has been deployed.** Many organizations run a few patching cycles behind. Conduct an inventory of current operating systems and immediately patch vulnerable endpoints. Stay up to date with your patching efforts, and ensure other vulnerability management practices (e.g. hardening, virtual patching, system isolation) are in place where appropriate
Leverage Threat Intelligence	**Take a proactive approach to vulnerability identification.** Leverage third-party open-source vendor websites and mailing lists to actively search for new indicators of compromise and CVEs. Schedule regular scans and prioritize your patching efforts
Back Up Your Data	**Get in the habit of periodically backing up all sensitive data.** Whether through cloud-based solutions or offline devices, sensitive data must be frequently backed up and stored in a secure manner
Assess Port Security	**Assess port security and exposure of internet-facing services** related to affected RDP and SMB services. Standard ports include 139 and 445. Consider disabling unused legacy protocol such as SMBv1
Plan For The Worst	**Formalize incident response procedures.** Create detailed runbooks that actively address all mitigation and operational procedures in the event that an endpoint is infected. Actively distribute runbooks and collaborate internally so that all security members are aware of the required steps and procedures
Block Indicators	**Information alone is not actionable.** A successful security program contextualizes threat data, aligns intelligence with business objectives, and then builds processes to satisfy those objectives. Actively block indicators and act on gathered intelligence

Important risk management terms and definitions

Risk	An uncertain event or set of events which, should it occur, will have an effect on the achievement of objectives. A risk consists of a combination of the probability of a perceived threat or opportunity occurring and the magnitude of its impact on objectives (M_o_R, 2007).
Threat	An event that can create a negative outcome (e.g. hostile cyber/physical attacks, human errors).
Vulnerability	A weakness that can be taken advantage of in a system (e.g. weakness in hardware, software, business processes).
Risk Management	The systematic application of principles, approaches, and processes to the tasks of identifying and assessing risks, and then planning and implementing risk responses. This provides a disciplined environment for proactive decision-making (M_o_R, 2007).
Risk Category	Distinct from a risk event, a scenario is an abstract profile of risk. It represents a common group of risks. For example, you can group certain types of risks under the risk category of IT Operations Risks.
Risk Event	A specific occurrence of an event that falls under a particular risk category. For example, a phishing attack is a risk event that falls under the risk category of IT Security Risks.
Risk Appetite	An organization's attitude towards risk taking, which determines the amount of risk that it considers acceptable. Risk appetite also refers to an organization's willingness to take on certain levels of exposure to risk, which is influenced by the organization's capacity to financially bear risk.
Enterprise Risk Management	(ERM) – A strategic business discipline that supports the achievement of an organization's objectives by addressing the full spectrum of organizational risks and managing the combined impact of those risks as an interrelated risk portfolio (RIMS 2015)[1].

The FARM acronym defines the risk management lifecycle

Developed by Info Tech Research Group (ITRG) and based on the National Institute of Standards and Technology (NIST) framework
https://www.infotech.com

F Frame

Determine the organizational risk tolerance

Establish the context for risk-based business decisions:

- How do we define risk?
- What is the organizational culture toward risk acceptance / avoidance?
- What types of business impact could we tolerate, and how often?
- What are our strategic business priorities?

A Assess

Develop and implement threat and risk assessments

Develop a formal process for assessing risk that is relevant for the business and will identify:

- Threats and vulnerability exposure
- The impact / harm that would occur if a threat were exploited
- The likelihood that the impact will occur

R Respond

Implement formal processes for risk approval / rejection

Implement a consistent and formal process to respond to security risks and security assessment results:

- Determine whether risk is tolerable or not
- Determine the appropriate course of action
- Implement the appropriate risk response (accept / reject / additional mitigations)

M Monitor

Continuously monitor and manage the organizational risk profile

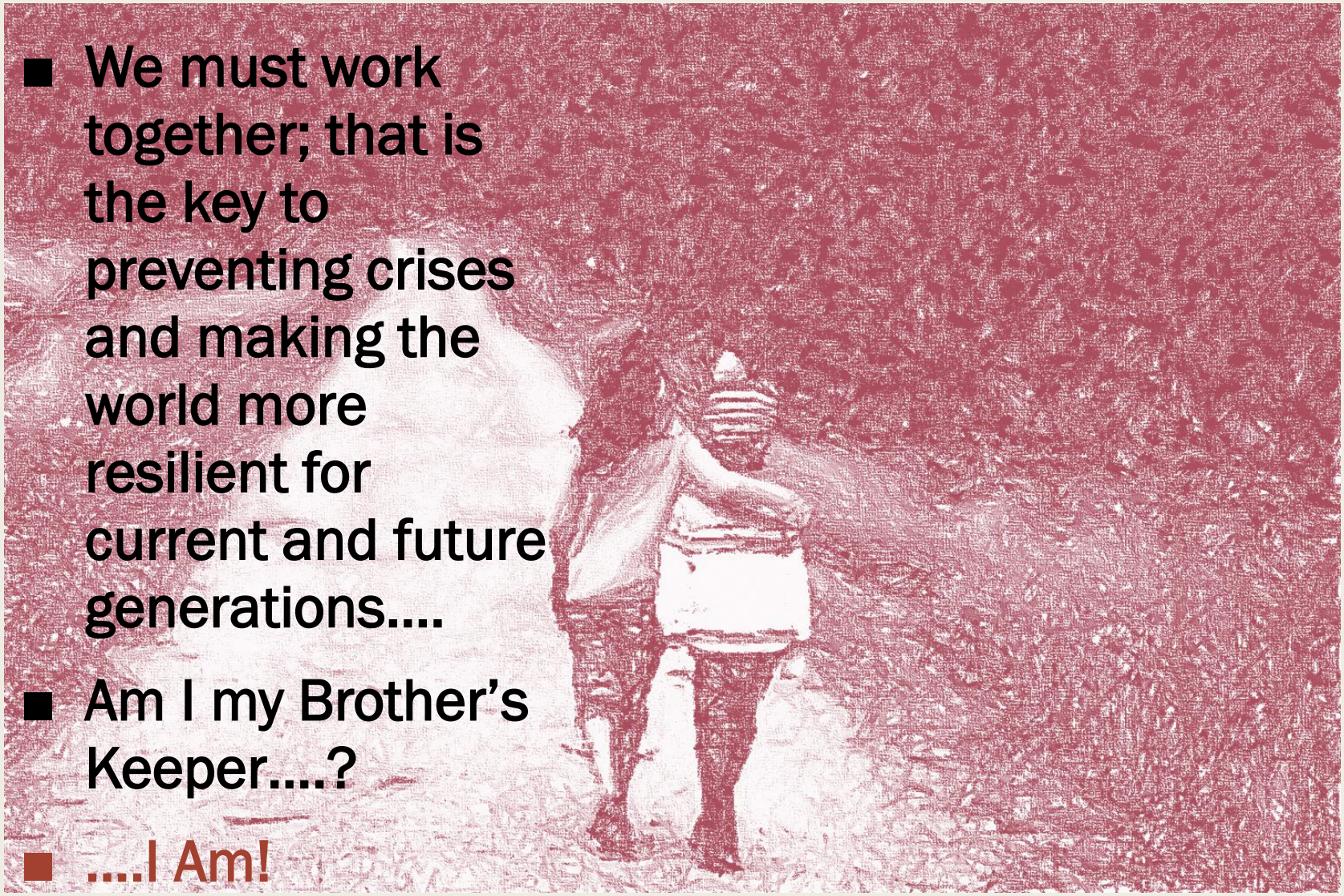
Address how the organization plans to:

- Verify that the planned risk responses have been implemented
- Manage ongoing effectiveness of security controls in mitigating risk
- Monitor and manage the overall risk profile of the organization

Lessons learned from the World Economic Forum, Hurricane Harvey, Maersk Cyberattack and beyond

- We have become adept at understanding how to mitigate risks that can be isolated and managed with risk management approaches including FARM. These approaches are essential and necessary at the senior organizational level and below
- Macro level environmental, cyber and other risks are much more complex and complicated, so we are much less competent when it comes to dealing with them in the interconnected systems that underpin our world. Standard Risk Management approaches alone have some limitations
- There are signs of strain in many of these systems; we experienced this first hand with Hurricane Harvey
- Humanity cannot successfully deal with the multiplicity of challenges we face either sequentially or in isolation. Just as global risks are increasingly complex, systemic and cascading, so our responses must be increasingly interconnected across the numerous global systems that make up our world
- Trends towards nation-state unilateralism may make it more difficult to sustain the long-term, multilateral responses that are required to counter some of these global risks such as global warming
- Multistakeholder dialogue remains the keystone of the strategies that will enable us to build a better world

Creating a shared future in a fractured world



- We must work together; that is the key to preventing crises and making the world more resilient for current and future generations….
- Am I my Brother's Keeper….?
- ….I Am!