



# Why Humans Are So Bad at Assessing Risk?


Iowa Communications Alliance  
CyberCon V

May 14, 2020

 | guernsey


[www.guernsey.us](http://www.guernsey.us)

1



Tim Fawcett, CISSA, CISP, PCIP  
Director of Cyber Security Consulting

- 20 years of information assurance experience performing IT audits, risk assessments, and cyber threat and vulnerability analyses
- Consulted for scores of companies from start-ups to Fortune 500 companies
- Certified Information Security Professional, a Certified Information Systems Auditor, and a Payment Card Industry Professional

 | guernsey

[www.guernsey.us](http://www.guernsey.us)

2

- Guernsey was founded in 1928 in Cherokee, OK
  - Engineering, architecture, and consulting services
- Guernsey has been providing consulting services to rural electric cooperatives since the 1930s
- Guernsey continues to provide a wide range of engineering, architecture and consulting services to multiple markets, including healthcare, oil and gas, power and energy, sports and entertainment, tribal government, commercial, industrial, higher education, cooperative and municipal utilities, municipalities, federal government agencies, county and state governmental agencies, and international clients.

[www.guernsey.us](http://www.guernsey.us)

3

- Risk Assessment / Gap Analysis
- Incident Management
- Penetration Testing
- Investigation and Forensics
- Configuration Auditing
- Vulnerability Analysis
- Training and Awareness
- Regulatory Compliance

## CYBER SECURITY SERVICES

[www.guernsey.us](http://www.guernsey.us)

4

## AGENDA

- **The Maginot Line**
- **Other Examples of Risk Management Fails**
  - YMCA Underwater Breathing Policy
  - YMCA Pool Lightning Policy
  - Examples of Moral Panic
- **How “The Affect Heuristic” Impacts How People Perceive and Evaluate Risk**
- **What Does This Mean About Assessing Our Cybersecurity Risk?**

## The Maginot Line

- A line of concrete fortifications, obstacles, and weapon installations built by France in the 1930s to deter invasion by Germany and force them to move around the fortifications.
- Constructed on the French side of its borders with Italy, Switzerland, Germany, and Luxembourg, the line did not extend to the English Channel due to French strategy that envisioned a move into Belgium to counter a German assault.
- The main construction was largely completed by 1939, at an estimated cost of around 3 billion French francs



The view of the village of Lembach in Alsace (north-east), taken from the combat unit number 5 of the fortress ouvrage Four-à-Chaux

## Your Cyber Security Program

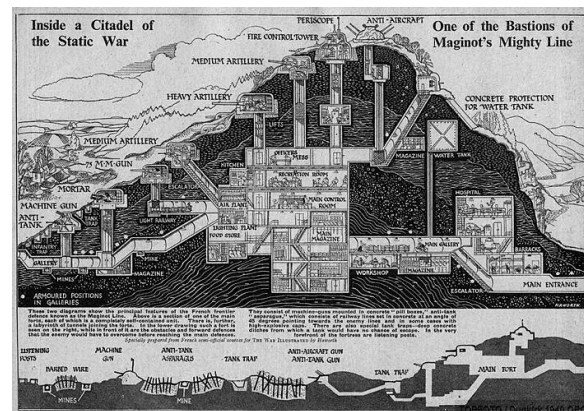
- A line of concrete fortifications, obstacles, and weapon installations built by France in the 1930s to deter invasion by Germany and force them to move around the fortifications.
- Constructed on the French side of its borders with Italy, Switzerland, Germany, and Luxembourg, the line did not extend to the English Channel due to French strategy that envisioned a move into Belgium to counter a German assault.
- The main construction was largely completed by 1939, at an estimated cost of around 3 billion French francs

- Cybersecurity is the protection of internet-connected systems, including hardware, software, and data, from cyberattacks.
- In a computing context, security comprises cybersecurity and physical security - both are used to protect against unauthorized access to data centers and other computerized systems.
- The goal of cybersecurity is to limit risk and protect IT assets from attackers with malicious intent.
- Information security, which is designed to maintain the confidentiality, integrity, and availability of data, is a subset of cybersecurity.
- The traditional approach focused resources on crucial system components and protected against the biggest known threats, which meant leaving components undefended and not protecting systems against less dangerous risks.

7

## The Maginot Line was built to fulfill several purposes:

- To prevent a surprise German attack
- To deter a cross-border assault.
- To protect Alsace and Lorraine and their industrial basin
- To save manpower (France counted 39 million inhabitants, Germany 70 million)
- To cover the mobilization of the French Army (which took between two and three weeks)
- To push Germany to circumvent France via Switzerland or Belgium, and allow France to fight the next war off of French soil to avoid a repeat of 1914-1918
- To be used as a basis for a counter-offensive



8



## Your cybersecurity program was built to fulfill several purposes:

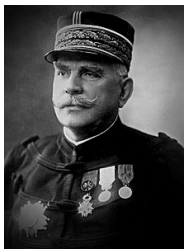
- To deter a cross-border assault.
  - To protect Alsace and Lorraine and their industrial basin
  - To save manpower (France counted 39 million inhabitants, Germany 70 million)
  - To cover the mobilization of the French Army (which took between two and three weeks)
  - To push Germany to circumvent France via Switzerland or Belgium, and allow France to fight the next war off of French soil to avoid a repeat of 1914-1918
  - To be used as a basis for a counter-offensive
- To prevent a cyber attack
  - To deter an attack from external and internal sources.
  - To protect computers and data from theft
  - To save manpower
  - To slow down an attack to allow security to address it
  - Designed around defense in depth.

9

## Divergent Opinions

Leaders such as Joseph Joffre, Paul Reynaud, and André Maginot had the perspective of WWI, which was a bloody stalemate of trench warfare and chemical weapons. This defensive strategy made assumptions that any future war would resemble the last and that they should prepare for *la guerre de longue durée* (the war of long duration).

The modernist view favored investment in armor and aircraft.



Joseph Joffre

Henri Philippe Pétain

André Maginot



Paul Reynaud



Charles de Gaulle

10

## Divergent Opinions

The correct approach to designing a cybersecurity program is also fraught with divergent opinions.

- CEO
- News media
- Security experts
- Salespeople
- Regulators
- Marketing
- Admin assistants
- Con-men
- Your teenager
- The yard guy

Everyone has an opinion!



CEO



News Media



Security Consultants



Account Manager



Regulators

11

## From front to rear, the Maginot Line was composed of:

- Border post line
- Outpost and support point line
- Principal line of resistance
- Infantry casemates (cloches)
- Petit ouvrages
- Gros ouvrages
- Observation posts
- Telephone network
- Infantry reserve shelters
- Flood zones
- Safety quarters
- Supply depots
- Ammunition dumps
- Narrow gauge railway system
- High-voltage transmission lines
- Heavy rail artillery

12

## From front to rear, the Cybersecurity Line is composed of:

- Edge router
- Firewall
- Intrusion detection system
- Web filter
- Email spam filter
- Intrusion prevention system
- SIEM
- Telephone network
- Endpoint software
- DMZ
- Awareness programs
- Back-ups
- Pen-testing
- Internal network infrastructure
- UPS and generators
- Incident response

13

## Ouvrages



Casemate



Blockhouse MOM (Main d'Oeuvre Militaire) de Richtolsheim

14

## Cloches

There are several kinds of armored cloches

The word "cloche" is a French term meaning *bell* due to its shape

All cloches were made in an alloy steel

Cloches are non-retractable turrets



15

## Other Defenses



81mm (3.2 inches) mortar

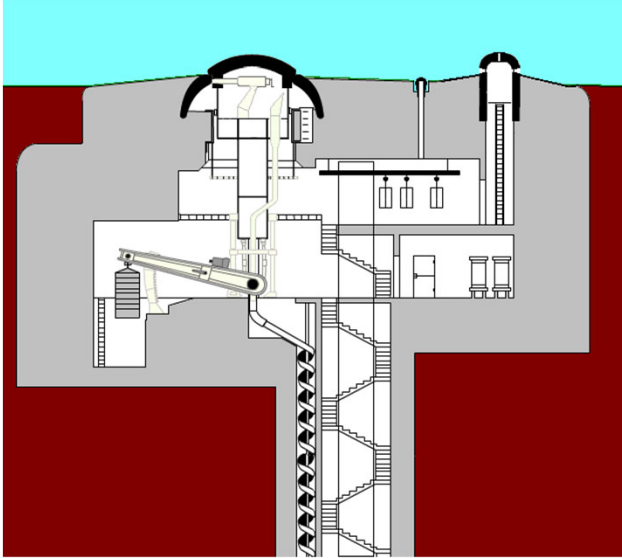


Anti-tank rails around Casemate 9 of the Hochwald Ditch

16



## Retractable Turrets



17

## System of Tunnels



18

## Some Major Problems

- France expected Belgium to be its ally; Belgium however, declared neutrality
- The line along the Belgium border was not well-constructed. The area of the Ardennes forest was not developed because it was believed it would act as a natural barrier
- The French fought the last war and did not appreciate the advancement in tanks and aircraft
- Propaganda created to convince the Germans that the Line was impenetrable mostly just caused a false sense of security



19

## AGENDA

- **The Maginot Line**
- **Other Examples of Risk Management Fails**
  - YMCA Underwater Breathing Policy
  - YMCA Pool Lightning Policy
  - Examples of Moral Panic
- **How “The Affect Heuristic” Impacts How People Perceive and Evaluate Risk**
- **What Does This Mean About Assessing Our Cybersecurity Risk?**

20

## YMCA Pool Guidelines – Breath-Holding



“For the safety of our swimmers, and to prevent shallow water blackout, any form of breath-holding practice is not allowed in YMCA pools. Swimmers may utilize correct rotary breathing during their swim activities. Any swimmer who violates this rule will be warned. A second violation will result in dismissal from the pool area.”

21

Apparently, this is a thing....

## WHAT IS SHALLOW WATER BLACKOUT?



22

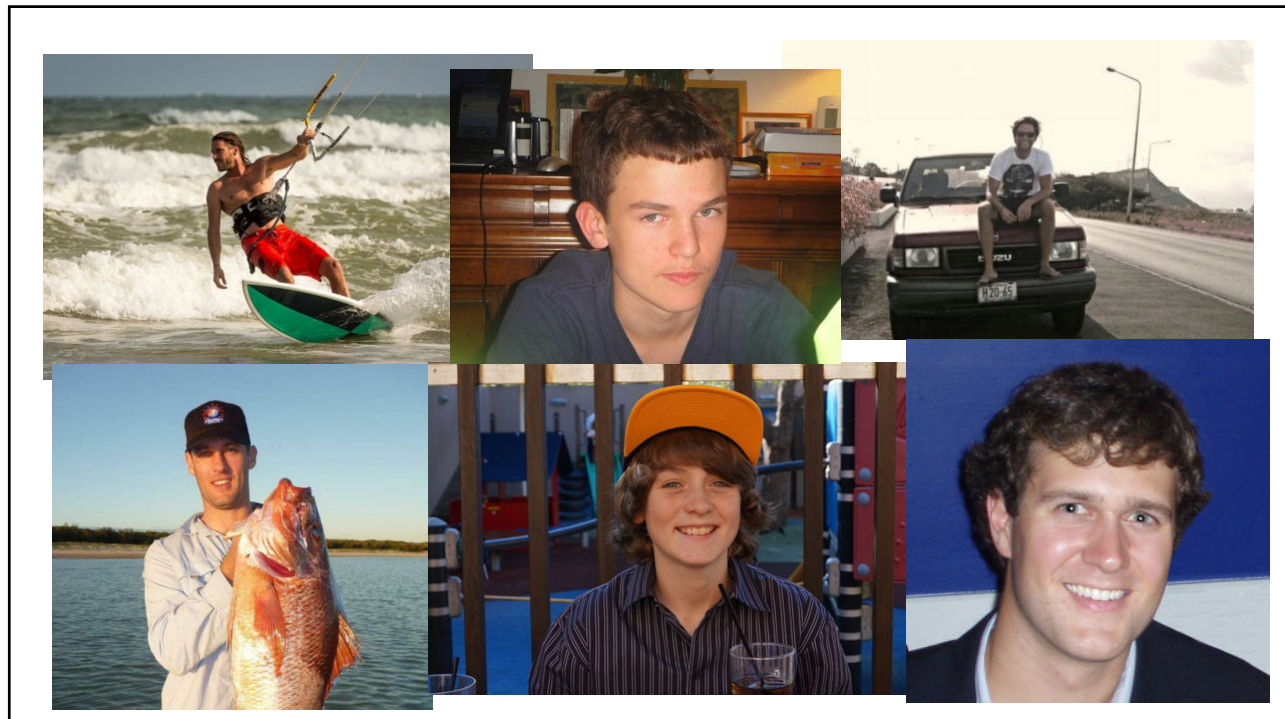
## Apparently, this is a thing....



Our mission is to prevent senseless deaths from shallow water blackout through awareness and education. Our goals are:

- To have warning labels of the dangers of prolonged breath-holding and the dangers of underwater blackouts on all spearfishing equipment, advocating safety courses in free-diving
- Ideally, to have spearfishing licensed separately from saltwater fishing, similar to a hunting license, which required a safety course
- To **ban** prolonged breath-holding from pools unless one is safety trained in **free-diving**
- For children to be raised with the knowledge that underwater breath-holding is dangerous and should not be encouraged

23



24



## AGENDA

- **The Maginot Line**
- **Other Examples of Risk Management Fails**
  - YMCA Underwater Breathing Policy
  - **YMCA Pool Lightning Policy**
  - Examples of Moral Panic
- **How “The Affect Heuristic” Impacts How People Perceive and Evaluate Risk**
- **What Does This Mean About Assessing Our Cybersecurity Risk?**



[www.guernsey.us](http://www.guernsey.us)

25

## YMCA Closing Indoor Pools Due to Lightning

“A licensed electrician must certify this through an inspection that results in a letter or certificate being sent to the YMCA stating that the pool is certified bonded and grounded.

What does this mean?

**Bonded** – all of the metal parts, motors, brackets, cable, and remote panels should be connected (bonded) together to provide a grid.

**Grounded** – This grid, along with any other machinery, should be grounded to allow the electric surge to escape the facility without disrupting any systems or injuring anyone.”

“The pool and shower areas should be evacuated until 30 minutes after the last evidence of lightning is present. While bonding and grounding may protect your participants, the YMCA should still evaluate the pool area to ensure safety.”

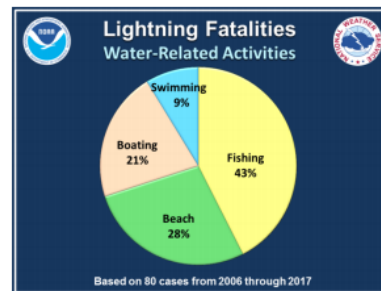


26

## Leisure activities are a killer...



- Of the 376 lightning deaths between 2006 and 2017, leisure activities were responsible for 236. Almost two-thirds (63%) of the deaths (149)
- Water-related activities contributed to 34% of leisure-related deaths (50)



27

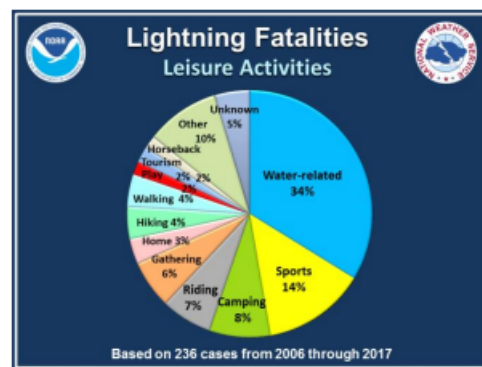
## Water-Related Activities

Water-related activities include fishing, boating, swimming, or just relaxing at the beach or a lake. Sports-related activities contributed another 14%.

Sports-related fatalities include soccer, golf, running, baseball, and football.

Other activities that contributed to the deaths in the leisure category include:

- Camping (8%)
- Riding bikes, motorcycles, and ATVs (7%)
- Social gatherings (6%)
- Hiking (4%)
- Walking (4%)
- Relaxing outside the home (3%)
- Tourism (2%)
- Children's play (2%)
- Horseback riding (2%)
- And "other" (10%)



The "other" category included: hunting, building a tree house, building a cabin, taking a work break, picking berries, watching a car race, watching a storm, watching a fire, watching a swollen river, getting a book out of a vehicle, waiting in a parking lot, walking to a car from a local park, attending a rock festival, searching for arrowheads, and getting better cell phone reception.

28

## What does Reddit say?



29

## AGENDA

- **The Maginot Line**
- **Other Examples of Risk Management Fails**
  - YMCA Underwater Breathing Policy
  - YMCA Pool Lightning Policy
  - **Examples of Moral Panic**
- **How “The Affect Heuristic” Impacts How People Perceive and Evaluate Risk**
- **What Does This Mean About Assessing Our Cybersecurity Risk?**

30

## Moral Panic

- A moral panic is a feeling of fear spread among many people that some evil threatens the wellbeing of society.
- The “process of arousing social concern over an issue. Usually the work of moral entrepreneurs and the mass media.”<sup>1</sup>
- According to Stanley Cohen<sup>2</sup>, there are five key stages in the construction of a moral panic:
  1. Someone, something or a group are defined as a threat to social norms or the community
  2. The threat is then depicted in a simple and recognizable symbol/form/words by the media
  3. The portrayal of the issue rouses public concern
  4. There is a response from authorities and policy makers
  5. The moral panic over the issue results in social changes within the community

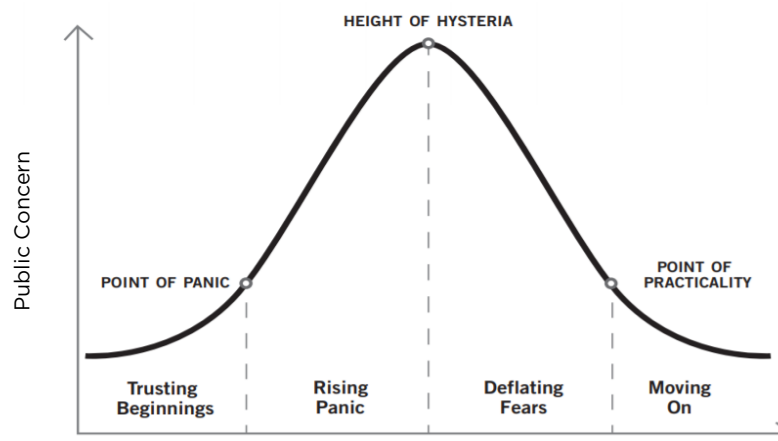
<sup>1</sup> Scott, John, ed. (2014), “M: Moral panic”, *A dictionary of sociology*, Oxford New York: Oxford University Press, p. 492.

<sup>2</sup> Cohen, Stanley (1973). *Folk Devils and Moral Panics: The Creation of the Mods and Rockers*. Paladin.

31

## Moral Panic

### The Panic Cycle



32



## Moral Panic

### Switchblades



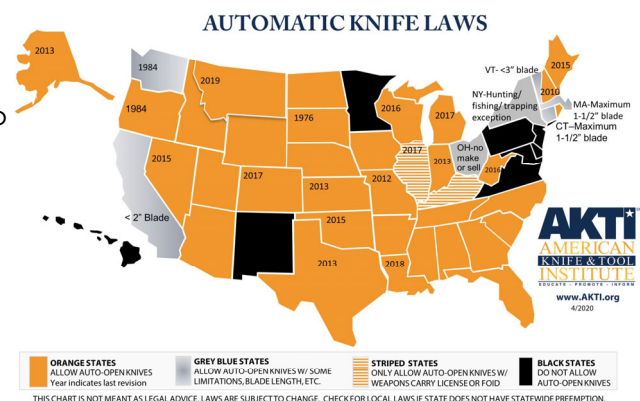
- In 1950, a woman's magazine - Women's Home Companion - published an article titled "The Toy That Kills" about automatic knives, or "switchblades." The article sparked significant controversy which was further fueled by the popular films Rebel Without a Cause, Crime in the Streets, and Westside Story.
- The switchblade became the symbol of youth violence and delinquency
- The public demanded the control of sales of such knives
- Federal and State laws restricting the transport or or criminalizing switchblade possession were adopted

33

## Moral Panic

### Switchblades

- Federal Switchblade Act of 1958
  - Regulated the manufacture had introduction of switchblades into interstate commerce.
  - Prohibits switchblades from being mailed through the U.S. Postal service.
- State Laws, many have been repealed in this century



34

## Moral Panic

### Halloween Candy Tampering

- The New York Times published an article that claimed “Those Halloween goodies that children collect this weekend on their rounds of ‘trick or treating’ may bring them more horror than happiness.”
- It provided examples of potential tamperings including “that plump red apple that junior gets from the kindly old woman down the clock may have a razor blade hidden inside.”
- There are no records that indicate a child has ever been killed by eating Halloween candy from a stranger.



35

## Moral Panic

- **Google Glass** - 7 out of 10 consumers said they would not use Google Glass, the now discontinued wearable, head-mounted device, because of privacy concerns. Unwarranted privacy concerns can slow adoption of beneficial new technologies.
- **The internment of Japanese Americans**- in the United States during World War II was the forced relocation and incarceration in concentration camps in the western interior of the country of about 120,000 people of Japanese ancestry.
- **Response to COVID-19** - In April, the unemployment rate increased by 10.3 percentage points to 14.7 percent.



36

## AGENDA

- **The Maginot Line**
- **Other Examples of Risk Management Fails**
  - YMCA Underwater Breathing Policy
  - YMCA Pool Lightning Policy
  - Examples of Moral Panic
- **How “The Affect Heuristic” Impacts How People Perceive and Evaluate Risk**
- **What Does This Mean About Assessing Our Cybersecurity Risk?**



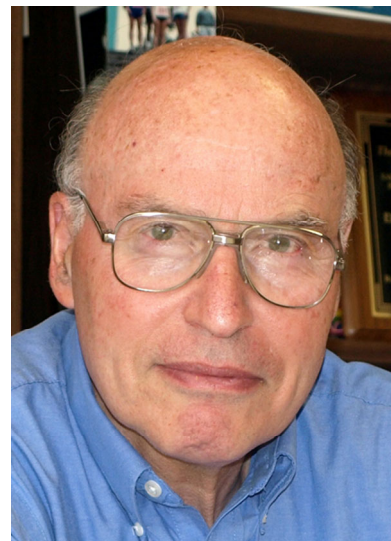
[www.guernsey.us](http://www.guernsey.us)

37

## How “The Affect Heuristic” Impacts How People Perceive and Evaluate Risk

Paul Slovic runs the Decision Research Institute in Oregon. He's spent his career studying how people judge risk. His research shows that people overestimate risk when a danger has a handful of qualities including:

- **Catastrophic potential:** Lots of people affected at once, rather than in small numbers over time
- **Familiarity:** A risk that isn't common knowledge
- **Understanding:** A sense that something isn't well understood by experts
- **Personal control:** a sense that danger is outside your control
- **Voluntariness:** Something can do harm even when you don't voluntarily put yourself in danger
- **Children:** Mention children and panic multiplies
- **Victim identity:** “One death is a tragedy; one million deaths is a statistic.” Joseph Stalin
- **Origin:** Man-made risks are viewed as more dangerous than natural disasters



38

## Factors That Affect Risk Evaluation

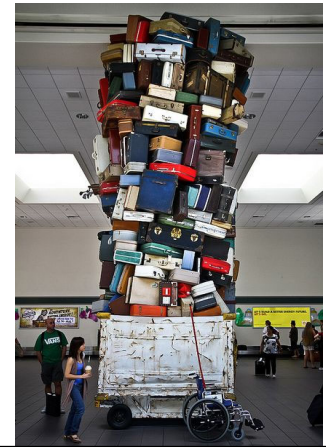


### Emotion

- What about the kids?
- We need to do SOMETHING
- Loss of life must be avoided, at all cost, even if only remotely possible
- This should never happen again

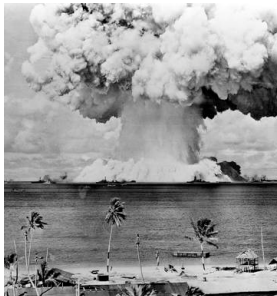
### Past Experience

- "I used XYZ software at my last company so I'll use it here"
- Not appreciating the specific circumstances of the current situation
- The French planned for WWI, because that is what they knew
- We have always done it this way
- Blindly following instructions



39

## Factors That Affect Risk Evaluation



### Unusual or Sensational Events or News

- Nuclear disasters
- Swine Flu/Ebola/COVID-19
- School shootings
- Plane crashes
- Terrorist attacks

### Bad Math

- Napoleon Bonaparte's height was recorded as 5 feet 2 inches. At the time of Napoleon's reign, the French and British had different systems of measurement that both used the same terms.
- If Napoleon was 5'2" in the French measurement system, he would have been 5'6" in the British system.
- This would indicate he was an average-sized man for his time.



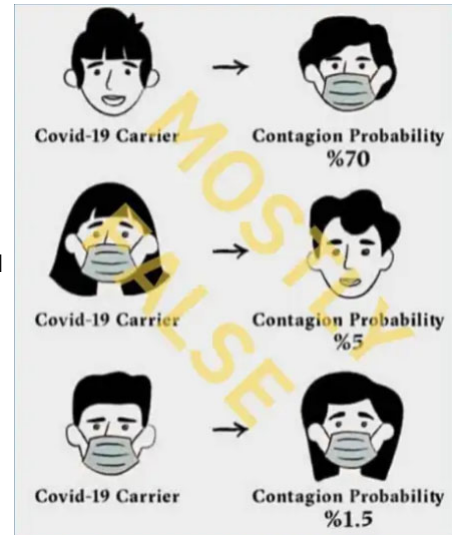
40



## Factors That Affect Risk Evaluation

### More Bad Math, and Numbers Having Too Much Power

- Snopes - The percentages displayed in this chart cannot be accurate because no scientific consensus exists on the efficacy of homemade masks in stopping the spread of COVID-19.
- Qualitative Data that was assigned a number and included in a calculation.
- If the weather model predicts snow in May, I am not putting my snow tires on the car.
- Often times claims are made with no consideration or understanding of the underlying data-set, assumptions or limitations.

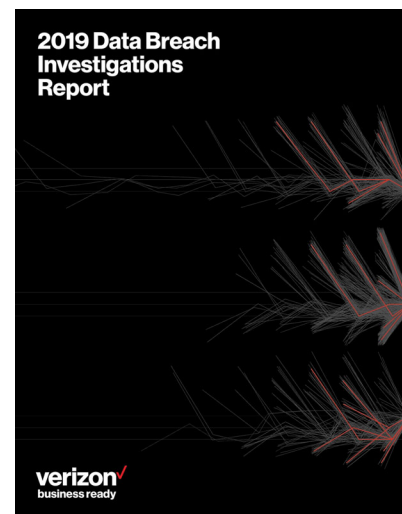


41

## Factors That Affect Risk Evaluation

### Even More ~~Bad~~ Not Fully Understood Math - Verizon DBIR

- Over a decade of analysis related to data breaches
- Quoted in nearly every presentation on cybersecurity
- Uses scientific approaches
- The data sets are larger than in the past
- Buried in Appendix B: "While we believe many of the findings presented in this report to be appropriate, generalization, bias, and methodological flaws undoubtedly exist. This is a great report, but when the information is quoted the underlying sampling, industries, company sizes, etc. are not well understood."



42

## Factors That Affect Risk Evaluation



Your momma  
was wrong!

### Stuff We Believe is True, But Isn't

- Hot water is required to wash hands well
- Picking up a baby bird will cause their mother to reject them
- Toilets flush counterclockwise in Australia

### Money

- Airlines charge for checked bags and make billions. This also requires those bags to be checked in screening lines, making us less safe and more inconvenienced.
- Someone who sells a product that protects against a specific risk may believe the risk is relatively greater.
- Lack of adequate actuarial information for proper underwriting



43

## AGENDA

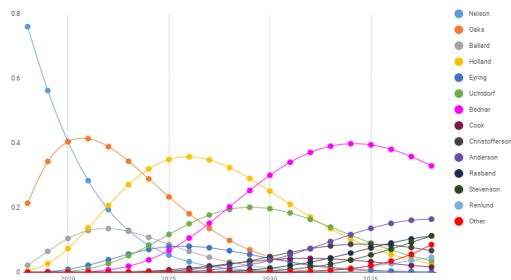
- **The Maginot Line**
- **Other Examples of Risk Management Fails**
  - YMCA Underwater Breathing Policy
  - YMCA Pool Lightning Policy
  - Examples of Moral Panic
- **How “The Affect Heuristic” Impacts How People Perceive and Evaluate Risk**
- **What Does This Mean About Assessing Our Cybersecurity Risk?**

44

## Risk – Likelihood and Impact

We must have a realistic and honest evaluation of risk which, as we just learned, we are horrible at doing

### Likelihood



### Impact

#### Customer Service and Goodwill Loss Ranges (Intangible)

Score	Effect
0	None
2	Minimal
4	Moderate
6	Moderately Heavy
8	Heavy
10	Severe

#### Cumulative Dollar Loss Ranges (Tangible)

Score	Loss Range
0	none
1	< \$1,000
2	≥ \$1,000 < \$5,000
3	≥ \$5,000 < \$10,000
4	≥ \$10,000 < \$25,000
5	≥ \$25,000 < \$50,000
6	≥ \$50,000 < \$100,000
7	≥ \$100,000 < \$150,000
8	≥ \$150,000 < \$250,000
9	≥ \$250,000 < \$500,000
10	≥ \$500,000

45

## What Does This Mean for Cybersecurity?

- We are poor at assessing risk
- We probably rely too heavily on technology
- We are deficient in areas that require human decisions
- We are probably overestimating the likelihood and impact of certain events
- We will never be 100% secure
- Risk will be different depending on the business
- A risk assessment must include an understanding of the business and information used by the business

46



# Why Humans Are So Bad at Assessing Risk?

Tim Fawcett, CISSP, CISA, PCIP  
Director of Cyber Security Consulting

Guernsey  
5555 N. Grand Blvd.  
Oklahoma City, OK 73112  
T: 405.416.8182  
M: 918.808.0558  
[timothy.fawcett@guernsey.us](mailto:timothy.fawcett@guernsey.us)  
[www.linkedin.com/in/timothy-fawcett](https://www.linkedin.com/in/timothy-fawcett)

 | guernsey

[www.guernsey.us](https://www.guernsey.us)