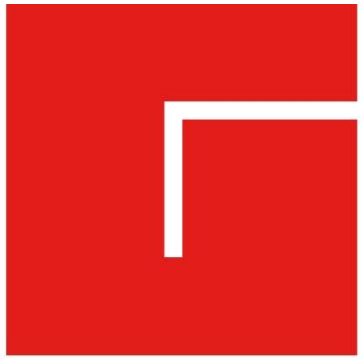
Assessing Risk

How Do We Decide What is Risky and How We Should Mitigate That Risk

Timothy Fawcett, CISSP, CISA, PCIP

Guernsey, founded in 1928 in Oklahoma City provides a wide range of engineering, architecture, and consulting services. Guernsey has provided consulting services to electric cooperatives since the rural electrification program was started in the 30's. Just within the last 20 years, Guernsey has enjoyed a broad range of consulting assignments with over 200 electric cooperatives. Security-related services encompassing both physical and cyber security have long been a component of our electric cooperative consulting engagements.

Guernsey Cyber Security Services



guernsey

REALIZE THE DIFFERENCE

guernsey

Virtual Information Security Officer

- **Guernsey fills the role of Chief Information Security Officer (CISO)**
  - Trusted Advisor
  - Regulations / Compliance
  - Policies and Procedures
  - Policy Enforcement
  - Best Practices

guernsey

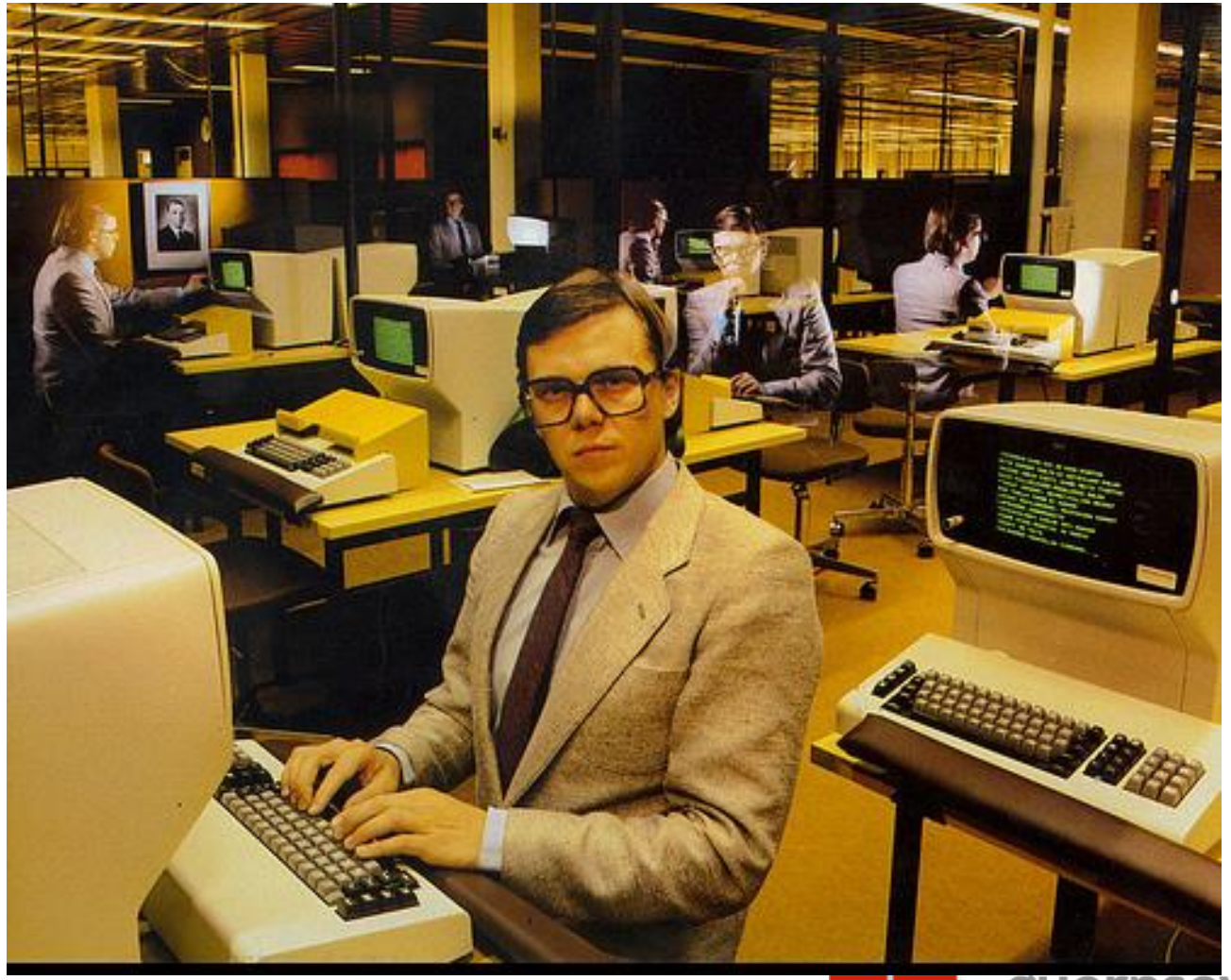
Audit and Testing

- Gap Analysis and Risk Assessment
- Web Application Security Reviews and
- Specific IT Audits and Testing
- Vulnerability and Configuration Reviews
- PCI, HIPAA, NERC-CIP

guernsey

Penetration Testing

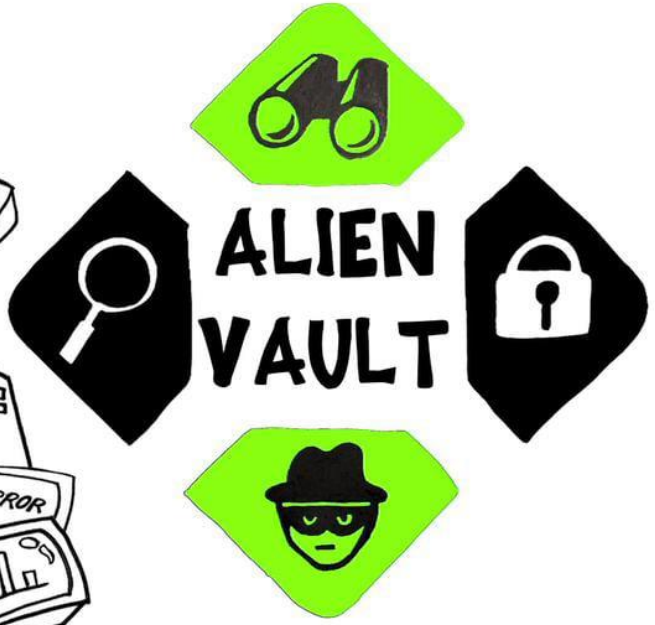
- Ethical Hacking
- External
- Internal
- Physical
- SCADA
- Radio
- Web Application



guernsey

Cyber Security Management Service

- Software at Client
- Remote Monitoring
- Managed Service
- Intrusion Detection
  - Host Based
  - Network Based
- Vulnerability Testing



guernsey

Incident Management

- When Incidents Do Occur:
  - Confirm That the Situation Has Been Addressed
  - Ensure Reporting Requirements Are Met
  - Evaluate Data Associated With Incident
  - Perform Root Cause Analysis
  - Perform Root Cause Analysis
  - Forensic Investigations
  - Independent Advisor

Training and Social Engineering

- User Awareness
- Phishing
- Physical Social Engineering
- Technical Training
- Recorded Media
- 25% DISCOUNT ON KNOWBE4

guernsey

Agenda

Defense in Depth – The Maginot Line

- **Did the French Understand the threats and properly mitigate risk?**

YMCA Aquatics Policy

- **Is the Y effectively managing risk?**
- **Is YMCA policy appropriate?**

Other Risks

- **Speeding**
- **Cold Boot Attack**
- **TSA**

What Factors Really Affect a Risk Evaluation

guernsey

Defense in Depth

Defense in depth (also known as **deep** or **elastic defense**) is a, buying time and military strategy that seeks to delay rather than prevent the advance of an attacker causing additional casualties by yielding space. Rather than defeating an attacker with a single, strong defensive line, defense in depth relies on the tendency of an attack to lose momentum over time or as it covers a larger area. A defender can thus yield lightly defended territory in an effort to stress an attacker's logistics or spread out a numerically superior attacking force. Once an attacker has lost momentum or is forced to spread out to pacify a large area, defensive counter-attacks can be mounted on the attacker's weak points, with the goal being to cause attrition or drive the attacker back to its original starting position.

guernsey

Maginot Line

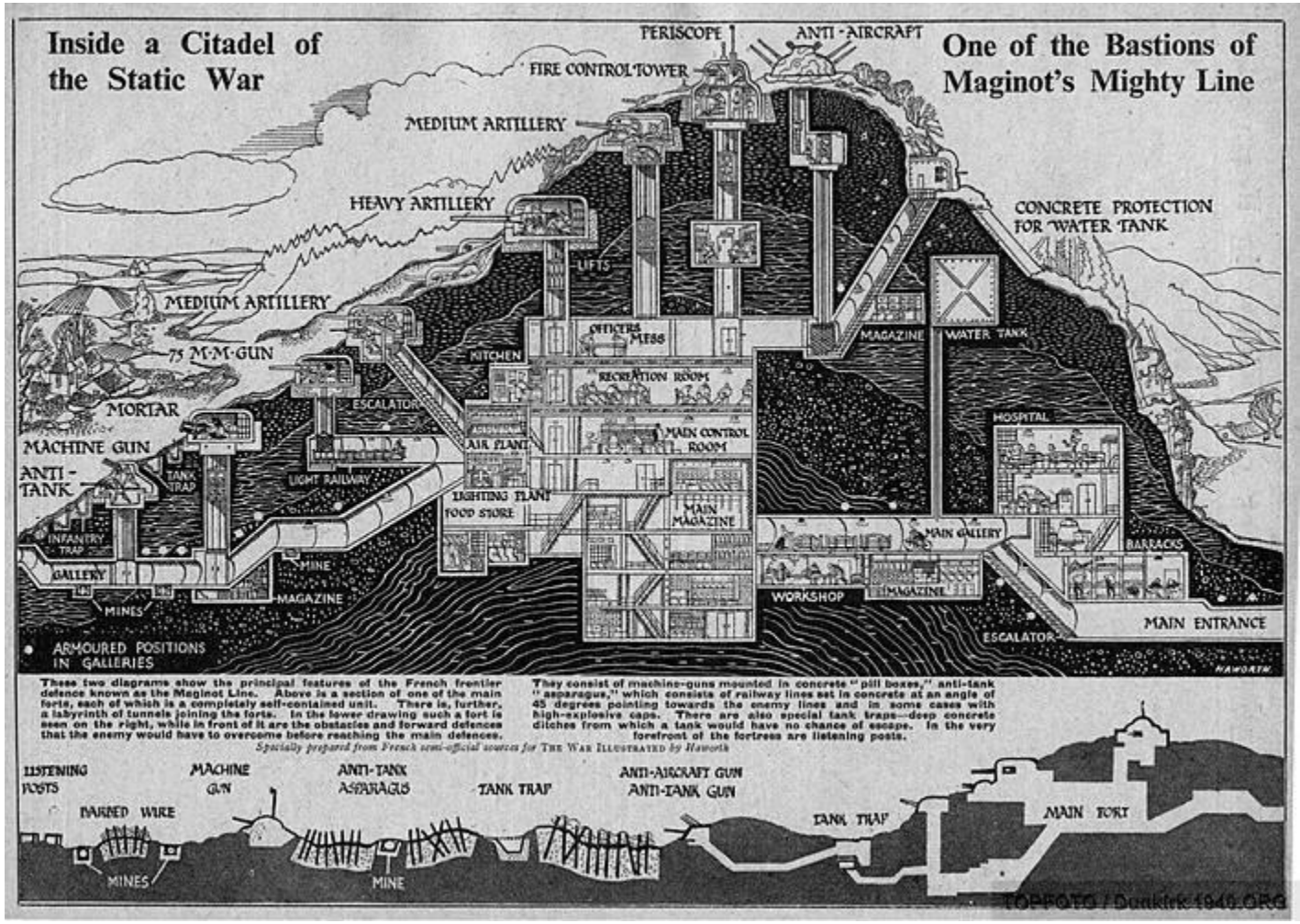
A line of concrete fortifications, obstacles, and weapon installations built by France in the 1930s to deter invasion by Germany and force them to move around the fortifications. Constructed on the French side of its borders with Italy, Switzerland, Germany, and Luxembourg, the line did not extend to 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

guernsey

The Maginot Line was built to fulfil several purposes:

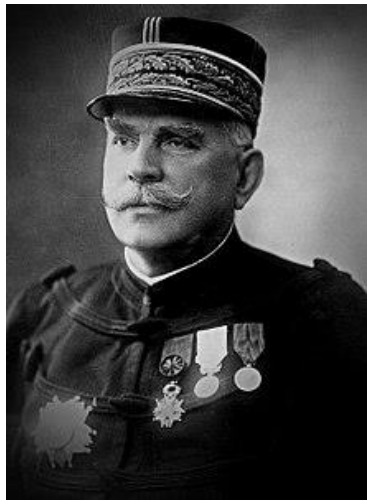
- To prevent a surprise German attack
- To deter a cross-border assault.
- To protect Alsace and Lorraine (returned to France in 1918) and their industrial basin
- To save manpower (France counted 39 million inhabitants, Germany 70 million)
- To cover the mobilization of the French Army (which took between two and three weeks)
- To push Germany into an effort to circumvent 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



guernsey

Divergent Opinions

Leaders such as Joffre, Reynaud, and 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 the long duration).



Joseph Joffre

Paul Reynaud

André Maginot

Paul Reynaud

Charles de Gaulle

The modernist view favored investment in armor and aircraft.

guernsey

From front to rear, (east to west) the line was composed of:

- Border Post line
- Outpost and Support Point line
- Principal line of resistance
- Infantry Casemates (Cloches)
- Petits 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

guernsey

Ouvrages

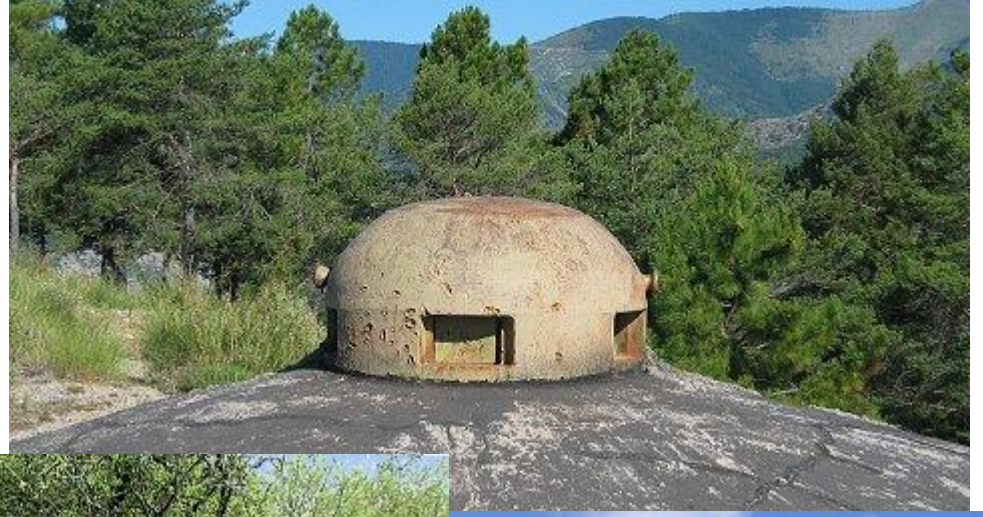
Casemate

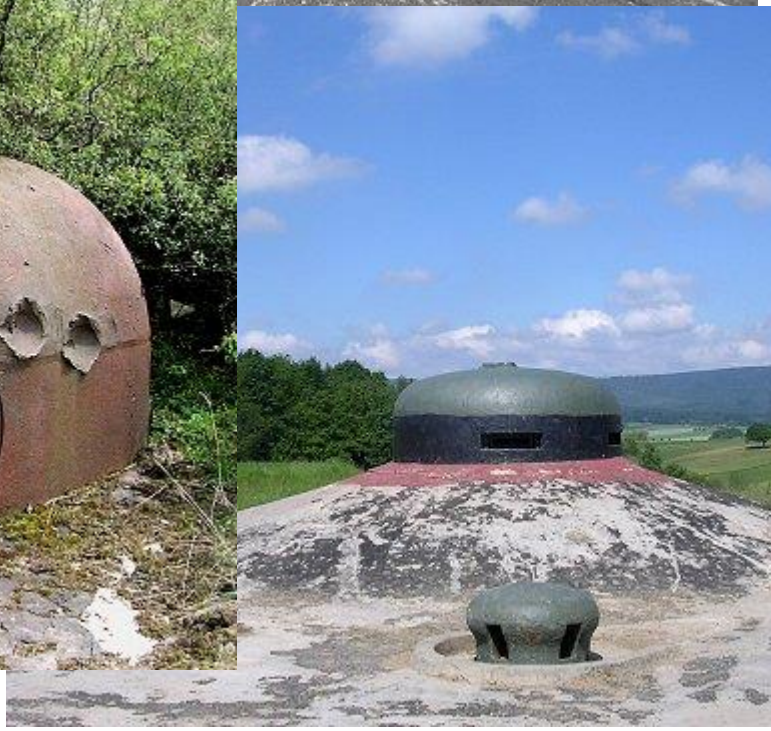
Blockhouse MOM (Main d'Oeuvre Militaire) de Richtolsheim

guernsey

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.





guernsey

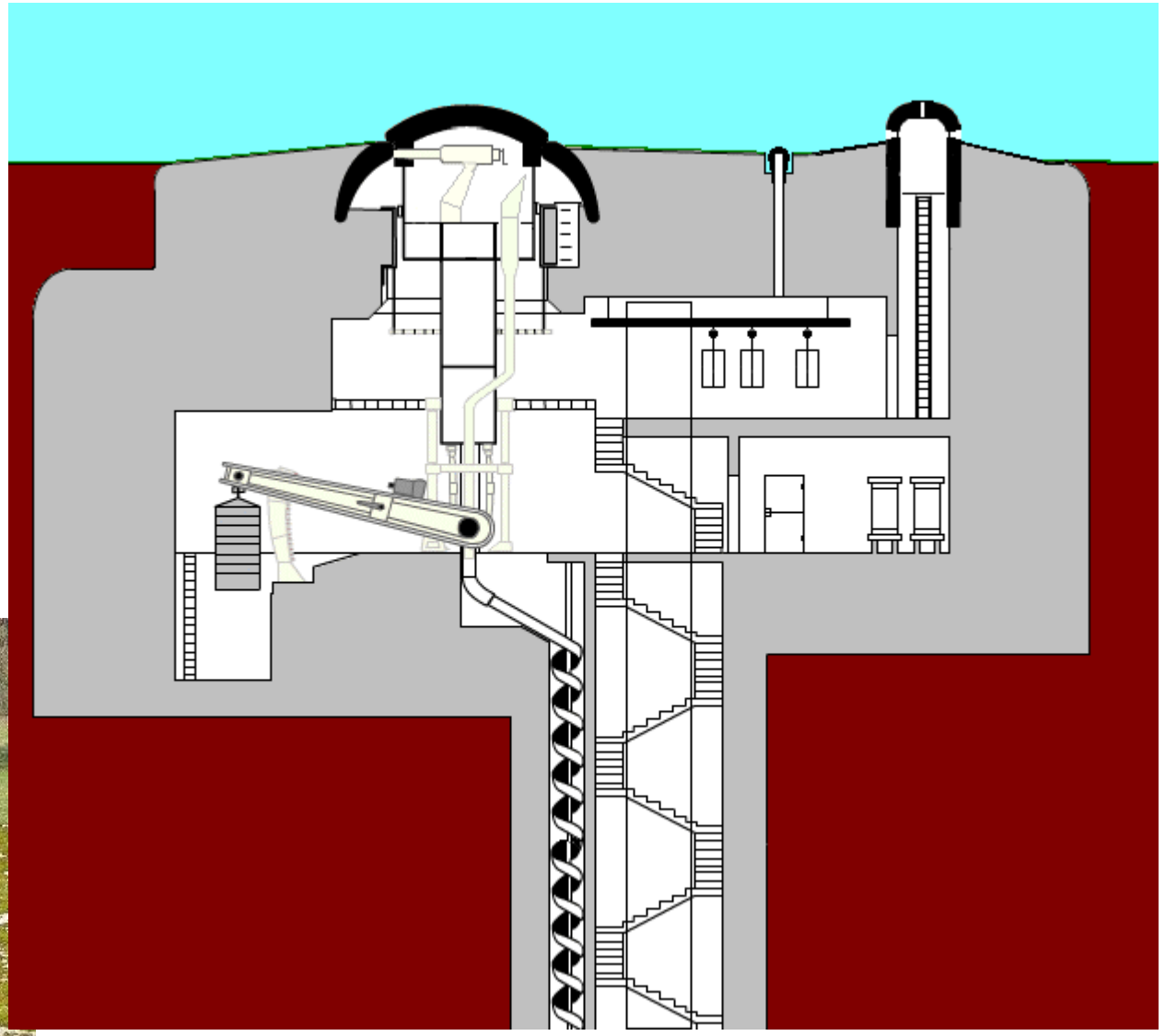
Other Defenses

81 mm (3.2 in) mortar

Anti-tank rails around casemate 9 of the Hochwald ditch

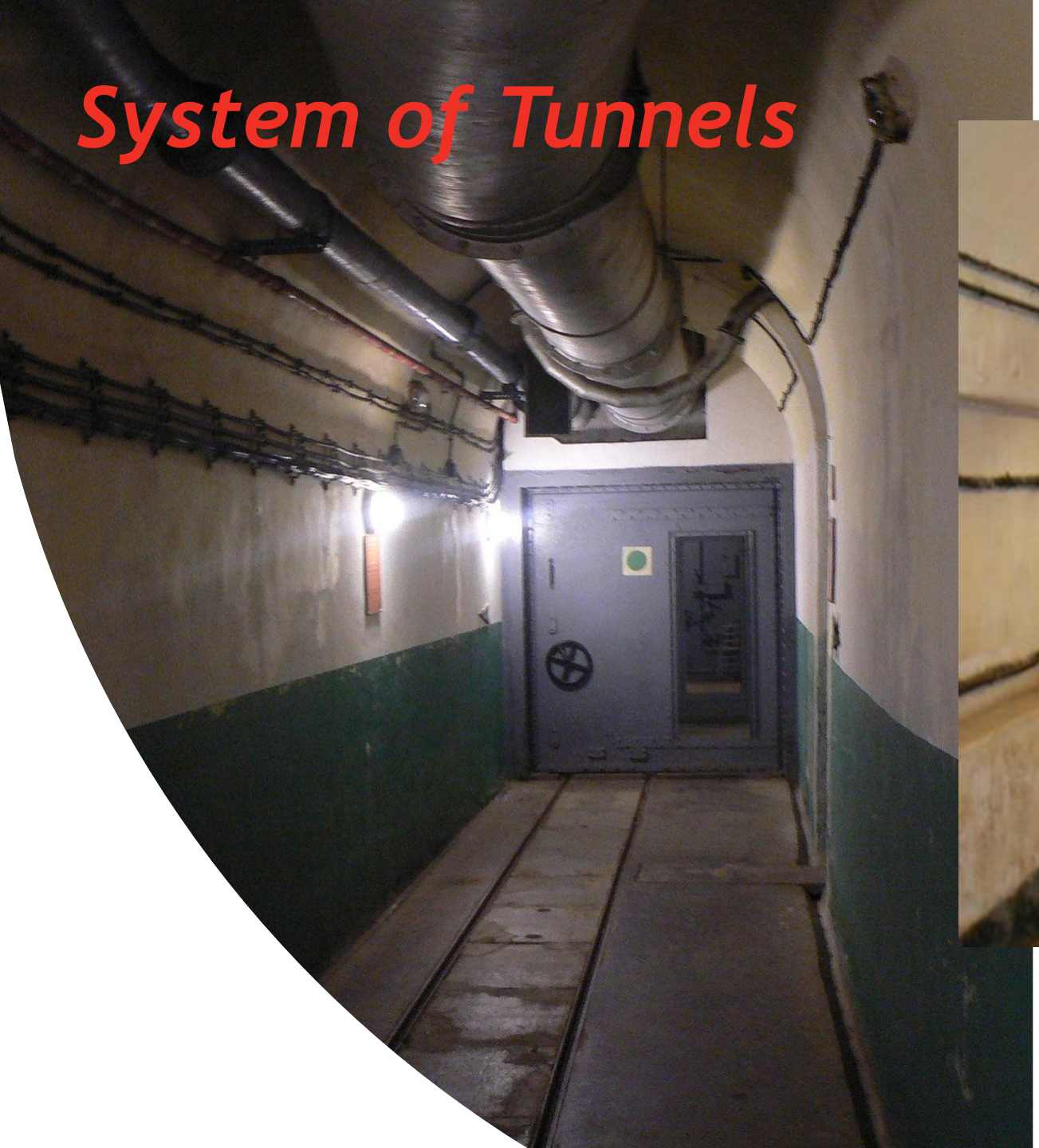
guernsey

Retractable Turrets



guernsey

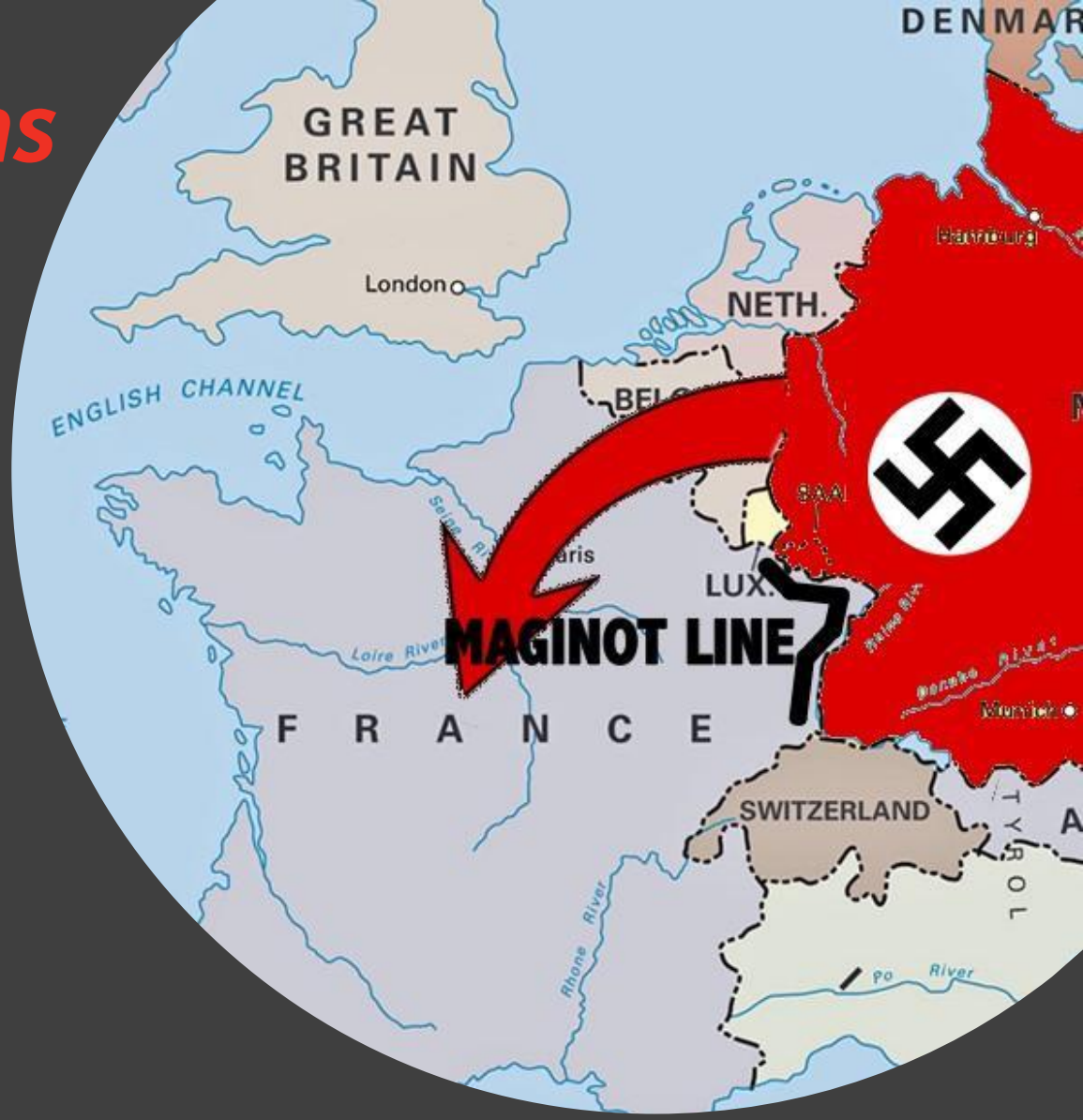
System of Tunnels



guernsey

Some of the Major Problems

- France expected Belgium to be an allies, expecting to fight the next war in Belgium, Belgium declared neutrality
- Line along Belgium border was much less well constructed, the area of the Arden forest was not developed believing that it would be to much of a natural barrier
- The French was fighting the last war and did not appreciate the advancement in tanks and aircraft
- Propaganda made to convince the Germans that the line was impenetrable mostly caused a sense of false security.



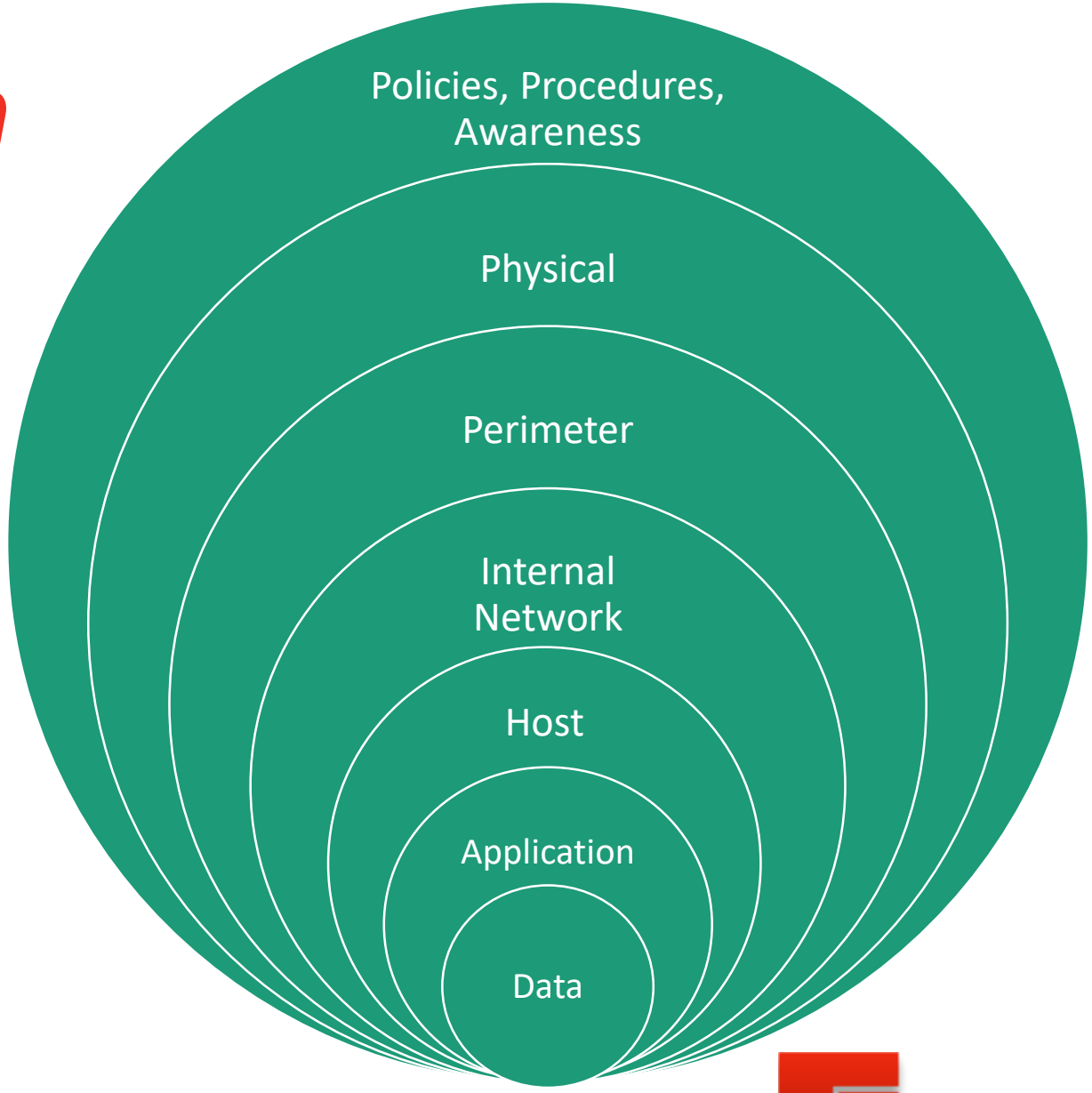
guernsey

Why the History Lesson? - A Metaphor for Expensive Efforts That Offer a False Sense of Security.

- These were built in the same period is the REA.
- The failure was not in the line but in the overall **risk management** strategy
- The Maginot line by some estimates cost **3 billion francs**
- Technology was used to **replace manpower**
- **Assumptions were made** about the environment, threats and methods of the enemy
- The line included **infrastructure and communication**
- The Germans brought the **ultimate zero day**, blitzkrieg.
- The plan for incident management was not adequate.
- The line for the most part worked as designed, the Germans just went around

guernsey

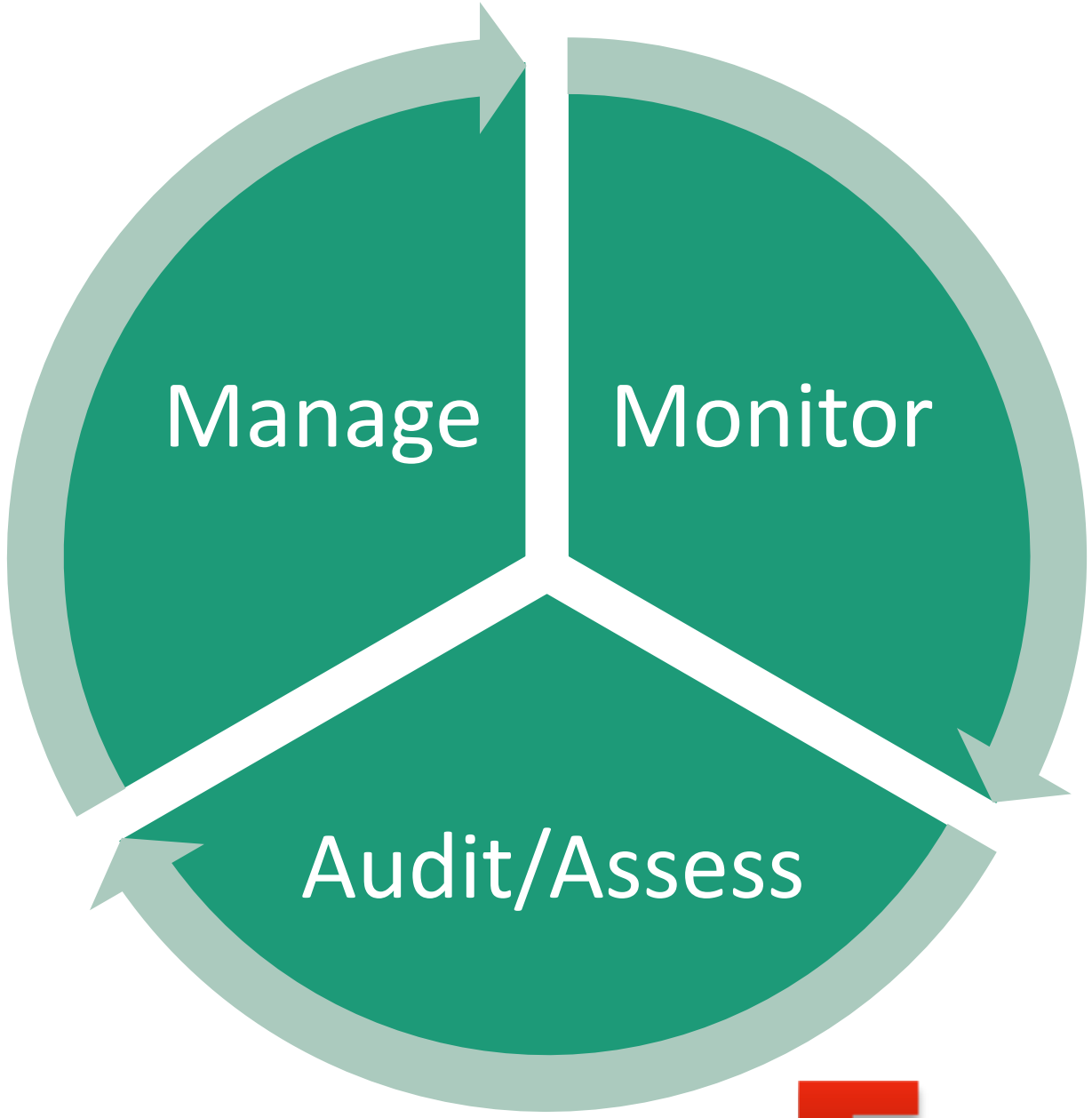
Defense in Depth as it relates to Cyber Security



guernsey

Lines of Defense

- Manage
  - Formal **Risk** Evaluation
  - Governance **Risk** and Controls
  - IT Operations Management
  - System Design
  - Training IT / Awareness
  - Formal **Risk** Acceptance
- Monitor
  - Threats, Vulnerabilities, **Risk**
  - Security Information and Event Management
  - Design and Configuration Monitoring
  - Social / Behavioral testing
  - Regular Management Review
  - Emerging **Risks**/Threats
  - Attack break penetration testing
- Audit/Assess
  - Internal Controls testing
  - Cyber Security Compliance
  - Investigation, forensics
  - Business Impact Analysis
  - Continuous auditing
  - Technical testing



guernsey

RISK - Likelihood and Impact

	Severity			
Likelihood	Catastrophic	Critical	Marginal	Negligible
Frequent	A	A	A	B
Probable	A	A	B	C
Occasional	A	B	C	C
Remote	B	C	C	D
Improbable	C	C	D	D
Incredible	C	D	D	D

WE MUST HAVE A REALISTIC AND HONEST EVALUATION OF RISK,
WHICH WE ARE HORRIBLE AT BY THE WAY.

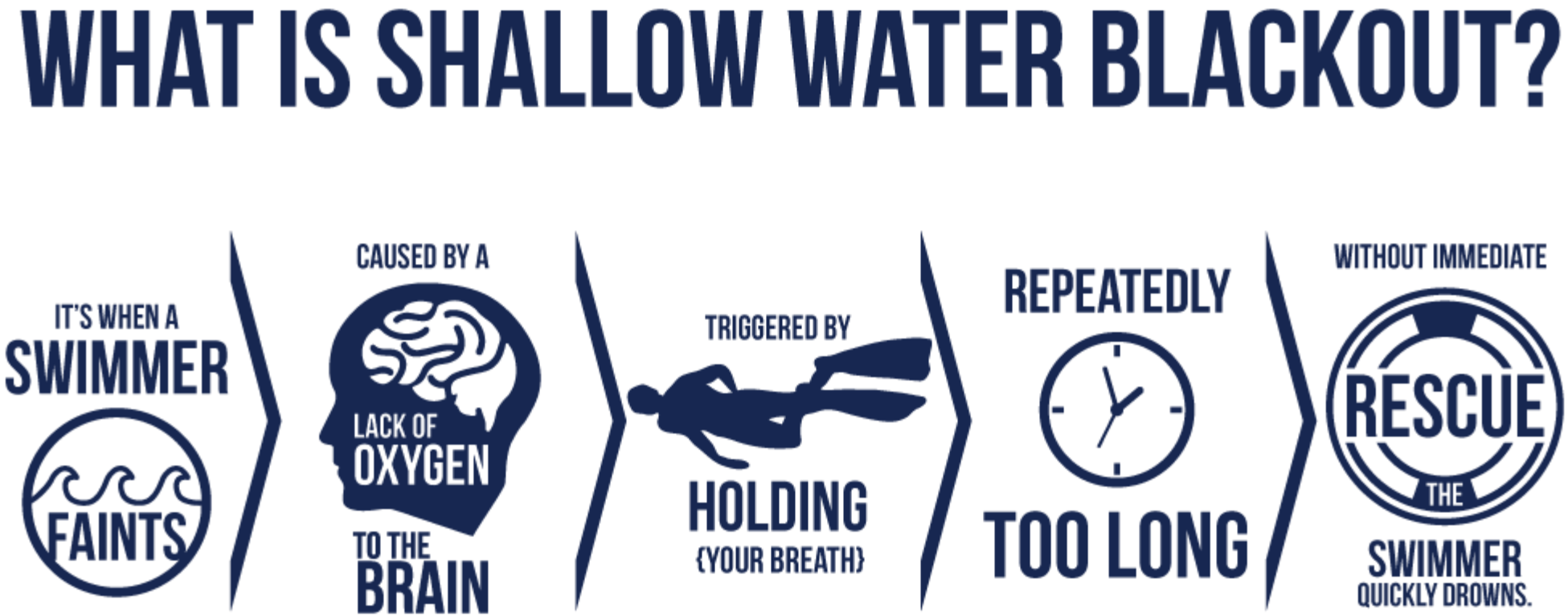
guernsey

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."

guernsey

Apparently This is a Thing



guernsey

Apparently This is a Thing

SHALLOW WATER
BLACKOUT PREVENTION

Our mission is to prevent senseless deaths from shallow water blackout through awareness and education. Besides preventing Shallow Water Blackout by awareness and education our goals are:

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

guernsey

Apparently This is a Thing

MAN DIES AT THE KEARN'S POOL WHILE PRACTICING UNDERWATER DRILLS

KEARNS, Utah (News4Utah) - A 39-year-old Taylorsville man died while swimming at the Kearns pool at 5624 Cougar Lane on Saturday morning.

Police say the man was practicing 'underwater drills' where holding your breath while under the water for a substantial amount of time is common...

15 YEAR OLD BOY LOST IN DIVING ACCIDENT

BOCA RATON INLET - As Tim Fernan and his team of divers from Palm Beach Reef Research searched for 15-year-old free diver Skyler Hunt on Saturday afternoon near the Boca Raton Inlet...

KATY TX LIFEGUARD DIES WHILE TRYING TO SWIM LENGTH OF POOL UNDERWATER

Witnesses said that at around 4 p.m. lifeguard Dustin Kruthaupt was swimming laps and at one point attempted to swim the length of the pool underwater.

DEEP WATER DIVER DIES AFTER TRYING FOR RECORD

LONG ISLAND, Bahamas — As Nicholas Mevoli lay on his back, floating in the azure sea, attempting to relax, his exhales were audible. The countdown had begun, and he prepared to dive into Dean's Blue Hole, hoping to reach 72 meters on a single inhalation, with no fins or supplemental oxygen. He began sipping the air, attempting to pack as much oxygen in his lungs as possible.

guernsey

Apparently This is a Thing

ER DI

NG
ER
tin Kr
swim

As
zu
di
ne
su

mpting to pack as much
ible.

guernsey

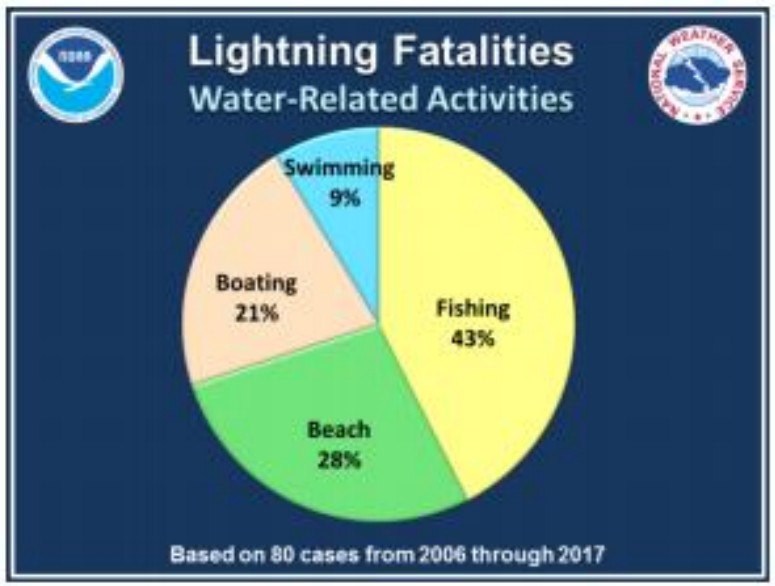
YMCA Closing Indoor Pools Due To Lightning

"A licensed electrician this must certify this through a inspection that results in a letter or certificate being sent to the YMCA stating that the pool is certified bonded and grounded. What do these things 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 evacuate the pool area to ensure safety."

guernsey

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 (**50**)

guernsey

Water-related Activities

Water-related activities include fishing, boating, swimming, or just relaxing at a beach or 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 included

camping (8%);

riding bikes, motorcycles and ATVs (7%);

social gatherings (6%);

hiking (4%);

walking (4%);

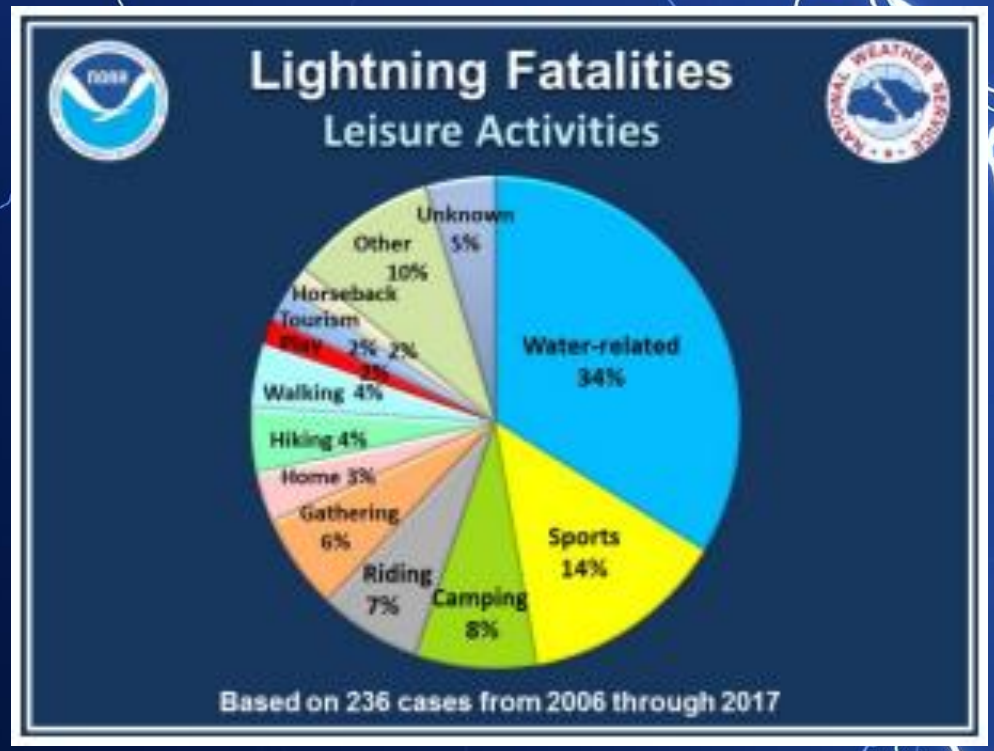
relaxing outside the home (3%);

tourism (2%);

children's play (2%);

horseback riding (2%);

and "other" (10%).

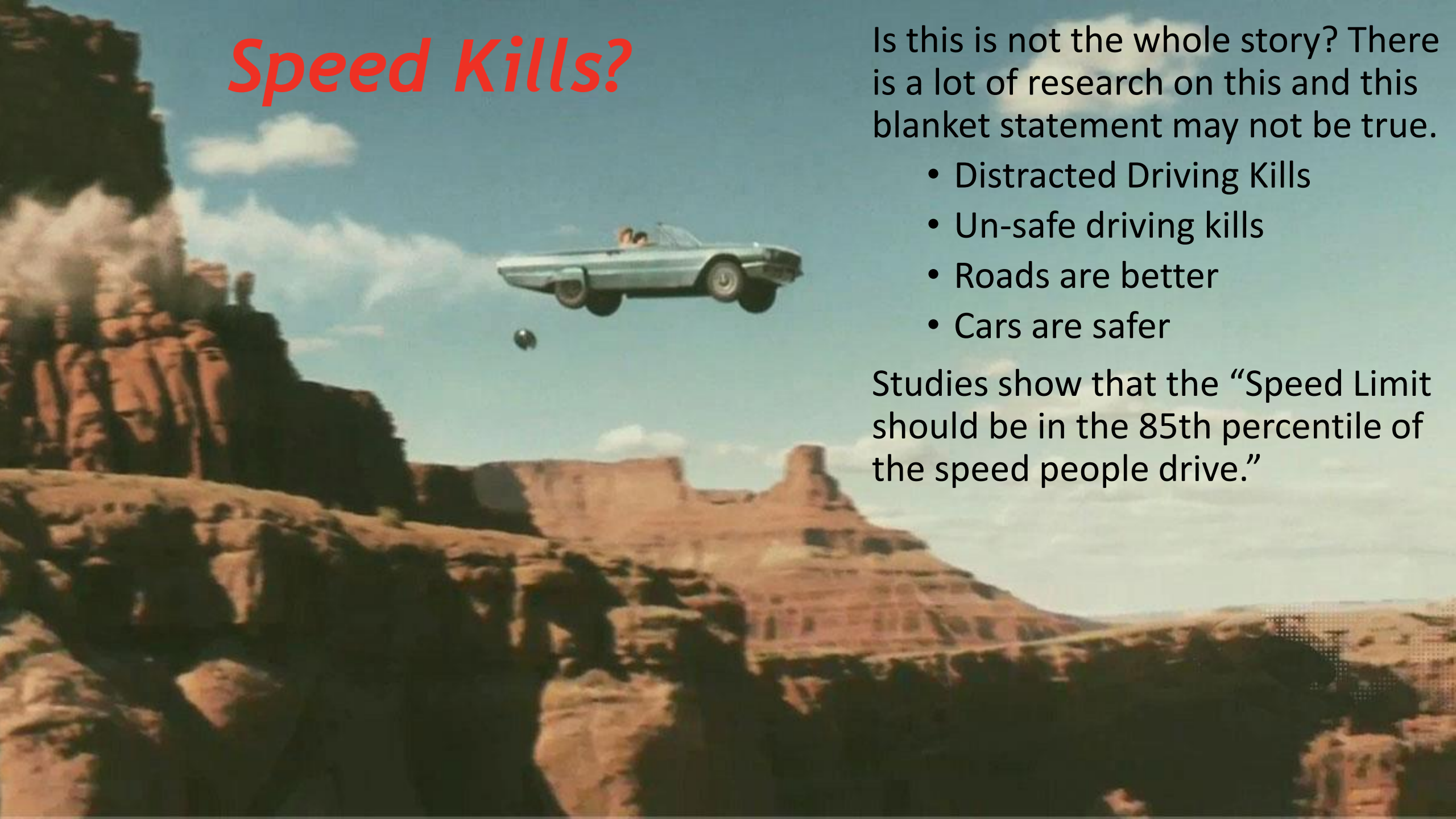


The "other" category included: hunting, building a tree house, building a cabin, taking a work break, picking berries, watching a car race, watching the storm, watching a fire, watching a swollen river, getting a book out of a vehicle, waiting in a parking lot, walking to a car from a local park, attending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

What Does Reddit Say?

guernsey

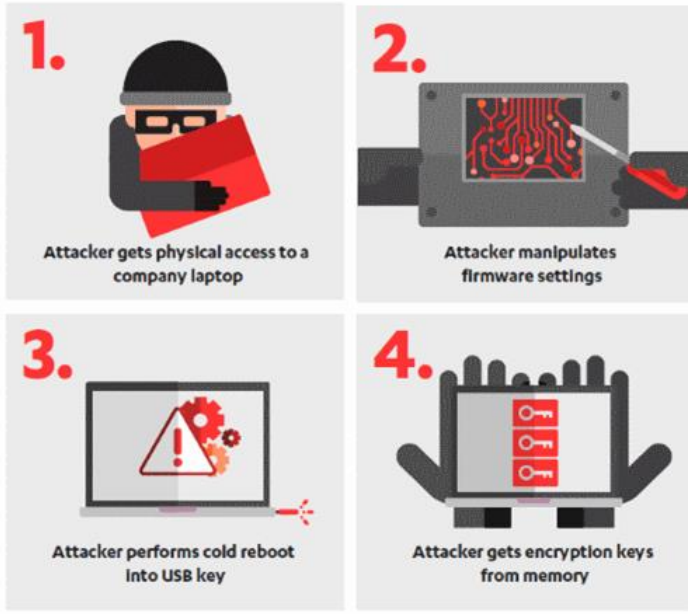
Speed Kills?



Is this is not the whole story? There is a lot of research on this and this blanket statement may not be true.

- Distracted Driving Kills
- Un-safe driving kills
- Roads are better
- Cars are safer

Studies show that the “Speed Limit should be in the 85th percentile of the speed people drive.”



Cold Boot Attack

A cold boot attack is a type of side channel attack in which an attacker with physical access to a computer is able to retrieve encryption keys from a running operating system after using a cold reboot to restart the machine. The attack relies on the data remanence property of RAM to retrieve memory contents that remain readable in the seconds to minutes after power has been removed. With certain memory modules, the time window for an attack can be extended to hours by cooling them with freeze spray. This form of attack has been known for over a decade.

guernsey

TSA - Checkpoint Security and Risk-Based Security

- There are more **than 900 advanced imaging technology machines** with privacy protecting software at airports nationwide
- In 2017, officers detected approximately 3,957 firearms at airport checkpoints, averaging 10 firearms per day
- TSA conducts over **12,000 assessments** a year to improve hands on training with transportation security officers
- Federal security directors conduct an additional **8,000 tests** a year to enhance officer performance
- TSA risk-based security is based on the understanding that the vast majority of people traveling pose little to no threat to aviation and applies an **intelligence-driven approach** focusing on higher-risk and unknown passengers. Through risk-based security:
  - There are over **350 TSA Pre✓® application centers** open nationwide
  - TSA Pre✓® is operating at approximately **200 airports**
  - More than **7 million passengers** each week experience expedited screening

guernsey

Factors That Affect Risk Evaluation

- Likelihood
- Impact

	Severity			
Likelihood	Catastrophic	Critical	Marginal	Negligible
Frequent	A	A	A	B
Probable	A	A	B	C
Occasional	A	B	C	C
Remote	B	C	C	D
Improbable	C	C	D	D
Incredible	C	D	D	D

guernsey

Factors That "REALLY" Affect Risk Evaluation

Money

- If you fly first class you are lower risk.
- 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 sells a product that protects against a specific risk may believe the risk is relatively greater.
- Speeding tickets are more about revenue than safety.
- Lack of adequate actuarial information for proper underwriting

guernsey

Factors That "REALLY" Affect Risk Evaluation

Emotion

- What about the kids?
- Better safe than sorry
- Loss of Life, even if only remotely possible
- This should never happen again.

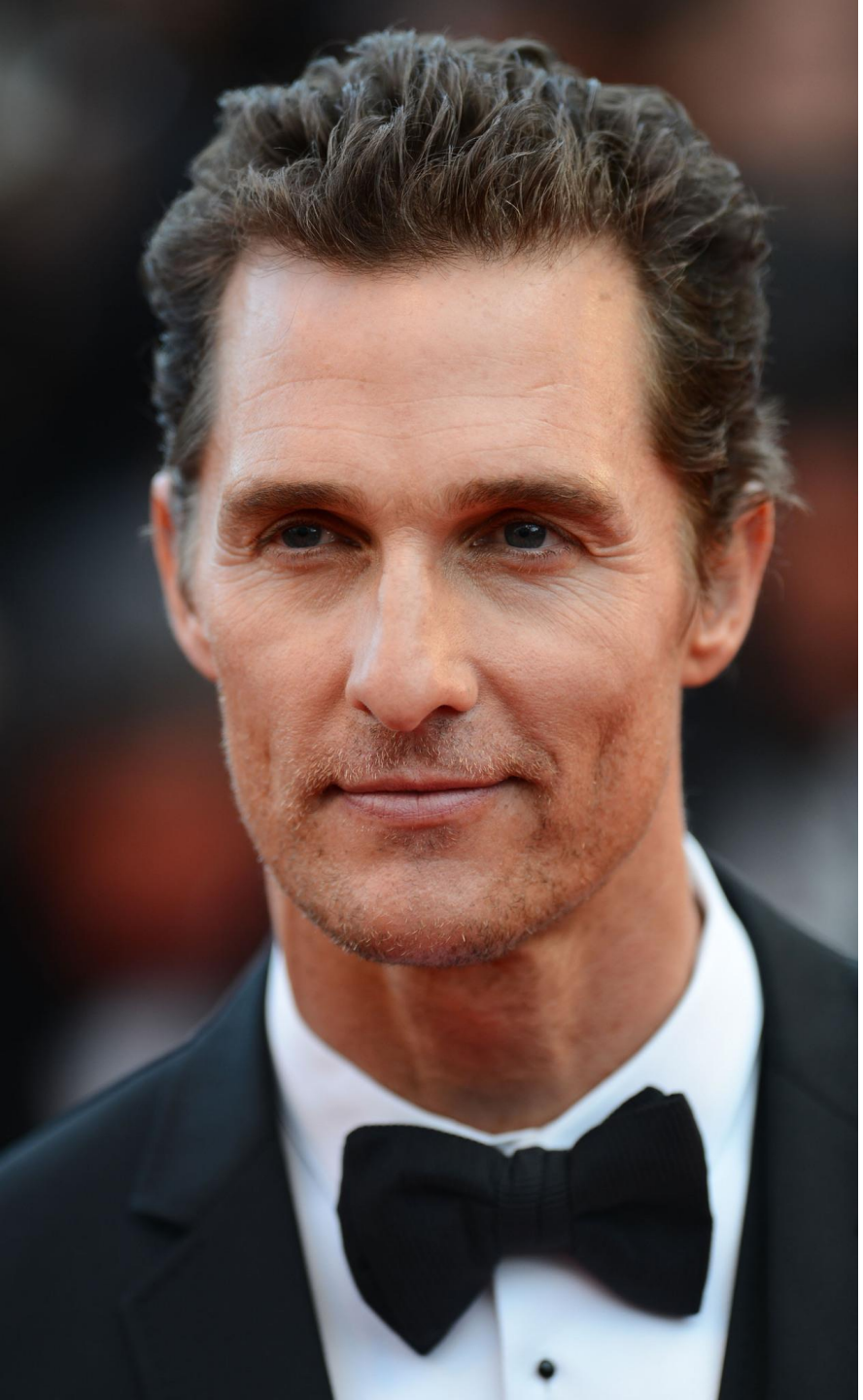
guernsey

Factors That "REALLY" Affect Risk Evaluation

Past Experience

- There was a time when any IT security professional knew what SETROPTS and RACF are.
- I used XYZ software at my last company, so I will use it here
- Not appreciating the specific circumstances of the current situation
- The French planned for WWI, because that is what the knew.

guernsey



Factors That "REALLY" Affect Risk Evaluation

Coolness

- Slick software
- Good reporting
- Shock and awe

guernsey

What Do Electric Cooperatives Do?

- Distribute Electricity
- Monitor Outages
- Dispatch - GIS
- Connect service
- Advanced Metering
- Billing
- Accepting Payments
- Run credit checks on new members
- Safety
- Community Outreach

guernsey

Agenda

Defense in Depth – The Maginot Line

- **Did the French Understand the threats and properly mitigate risk?**

YMCA Aquatics Policy

- **Is the Y effectively managing risk?**
- **Is YMCA policy appropriate?**

Other Risks

- **Speeding**
- **Cold Boot Attack**
- **TSA**

What Factors Really Affect a Risk Evaluation

guernsey

Tim Fawcett, CISSP, CISA, PCIP

Sr. Information Security Consultant
5555 North Grand Boulevard
Oklahoma City, OK 73112-5507
T: 405.416.8182
M: 918.808.0558
timothy.fawcett@guernsey.us
guernsey.us

guernsey