
13TH ANNUAL LEADERSHIP EVENT
CYBER SECURITY
cybersecuritysummit.org SUMMIT
RESILIENCE
UNLOCKED
TITLE SPONSOR
Island
#cybersecuritysummit #css13

Adapting to the Unpredictable

A Look at Human Resilience and Cyber Resilience

* These views are my own, not representative of Google

AKASH VERMA

TPM, Continuous Assurance Engineering,
Google

- Over a decade of experience in Cybersecurity across BigTech, FinTech, and MedTech Space
- Across 1st, 2nd, and 3rd Line of Defense
- FL Gator 🐊 | BE in Telecomm and MS in Info Sys
- Certs: CISSP, CISM, CRISC, CISA, GCIH, GCSA, PMP, and many more...

“Resilience” What and How?

- Comes from Latin ‘Resilire’
  - To Rebound, or
  - To Spring Back

- First came into existence in 1807 in Material Science World

- By the 20th Century it was heavily utilized in Psychology field
  - Individual’s ability to recover from adversity, trauma or stress

- By the 21st Century the word entered the realm of Cyber

> “Resilience is when you address uncertainty with flexibility.”

“Resilience” Mission

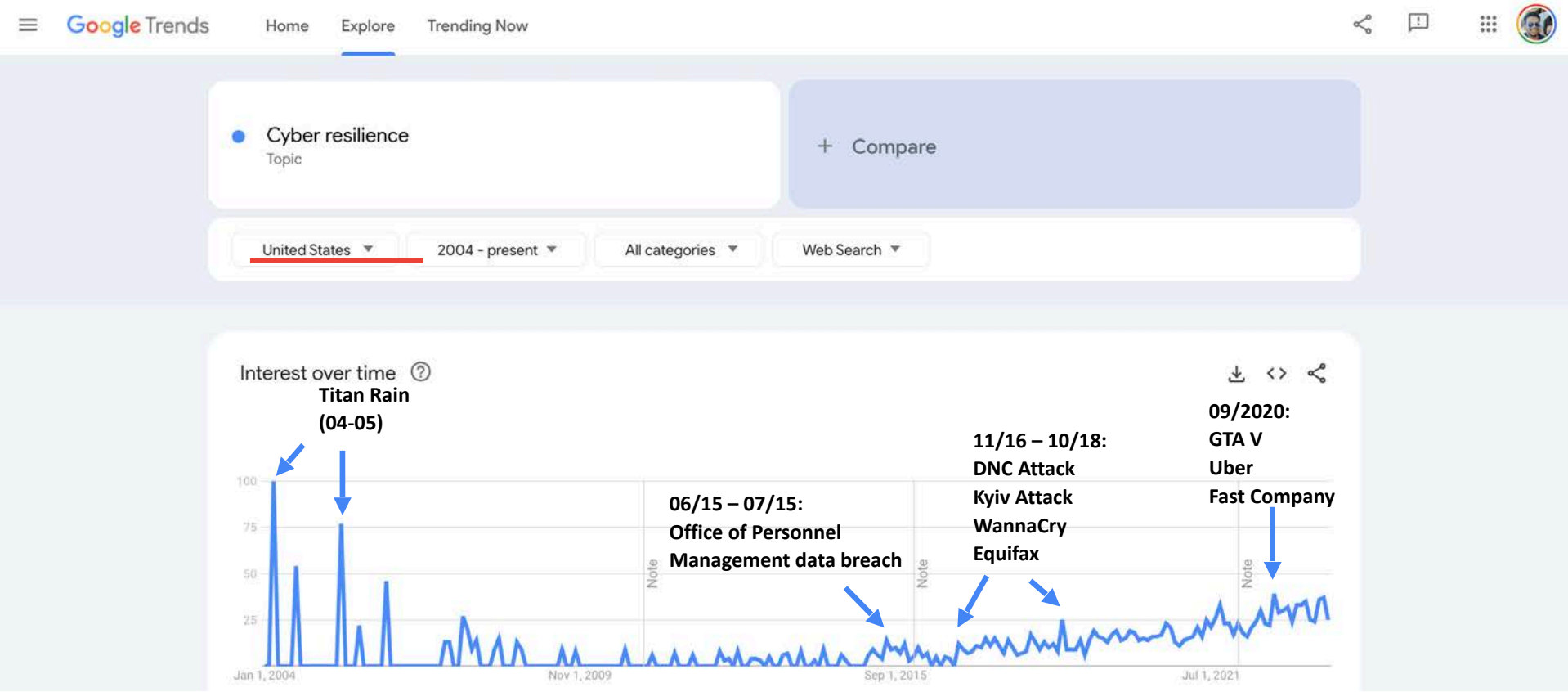
There is only one ultimate goal of Cyber Resiliency, and that is “Rapid Recovery”

But Why???

- IBM conducts an annual research on cyber breach quantification called as 'Cost of Data Breach Report 2023'
- N= 550 organizations that were hit by a data breach
- Key Stats:
  - The global average cost of a data breach in 2023 was USD 4.45 million, a 15% increase over 3 years.
  - $2.66 million — Average cost savings associated with an incident response team and regularly tested IR plan
  - 51% of organizations are planning to increase security investments as a result of a breach, including, but not limited to:
    - Incident response (IR) planning and testing,
    - Employee training, and
    - Threat detection and response tools.

Source: https://www.ibm.com/reports/data-breach

Cyber Resilience: Unique History

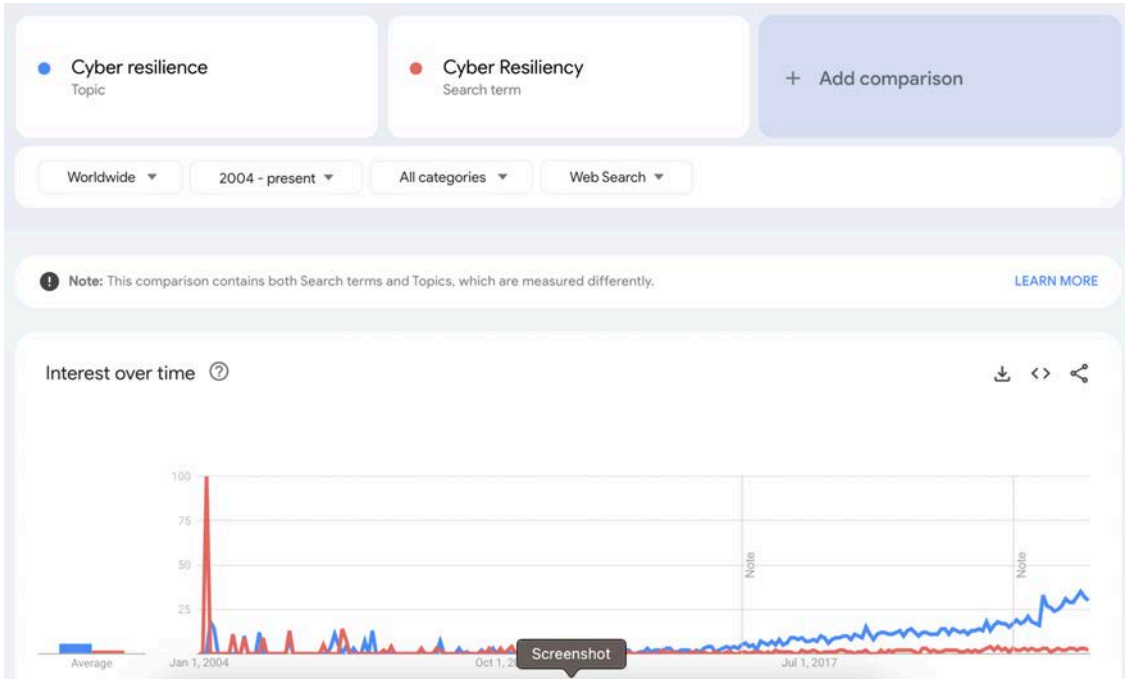


Cyber Resilience: Unique History

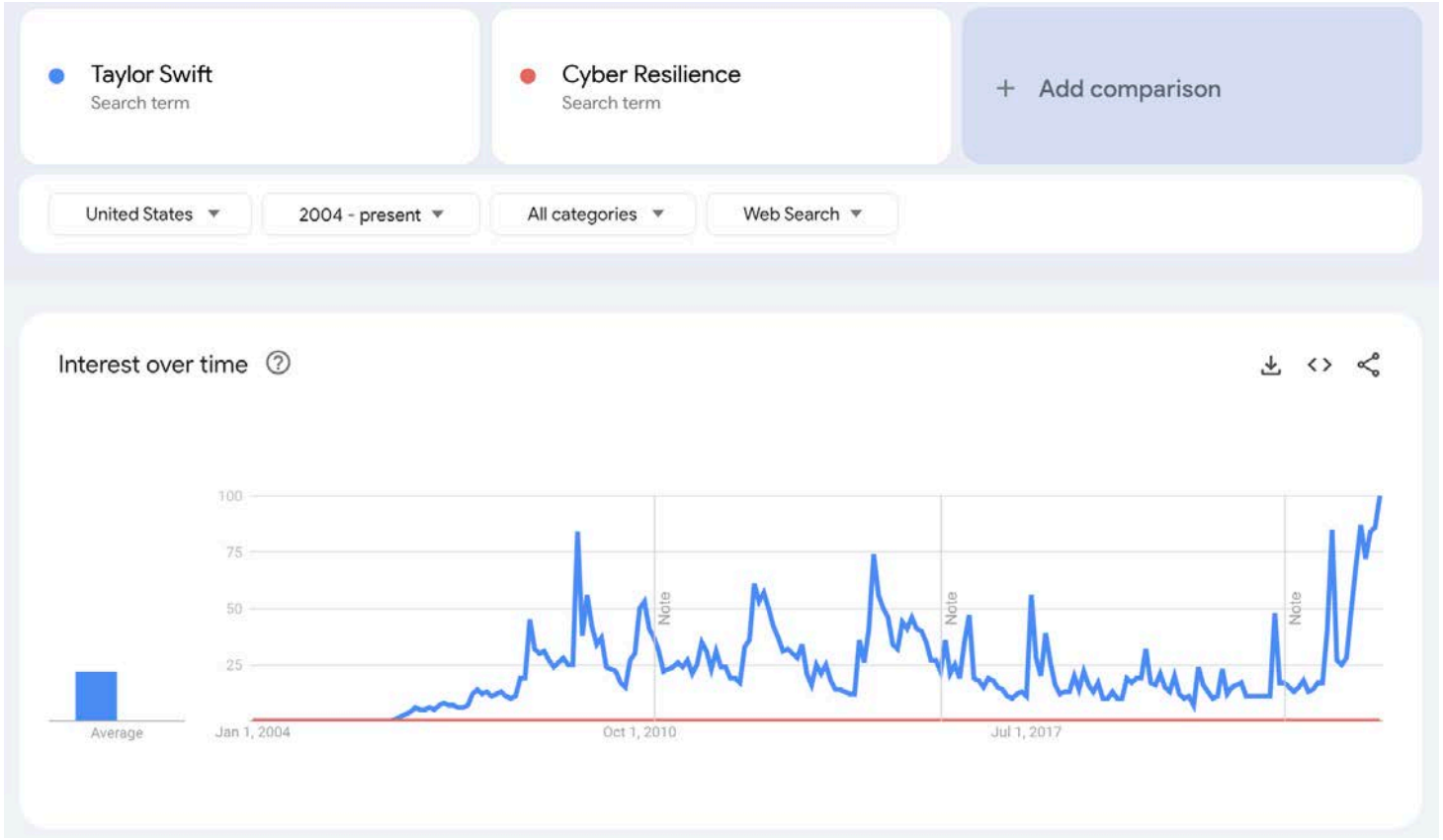
- Cyber Resiliency is supposed to be Proactive rather than Reactive

- The up-word search trends highlights that Cyber Resilience becomes an interesting topic after a cyber attack

- However, in most organization Cyber Resiliency still takes a Reactive approach than a Proactive Strategy



Cyber Resilience vs Taylor Swift



Resilience: A Comparative Analysis

Human Resilience and Cyber Resilience	
Similarities	**Difference**
+ Adaptable	- Innate Vs Designed
+ Learning from Past Experience	- Predictability
+ Continuous Improvement	- Scope of Impact
+ Systemic Perspective	- Recovery Time

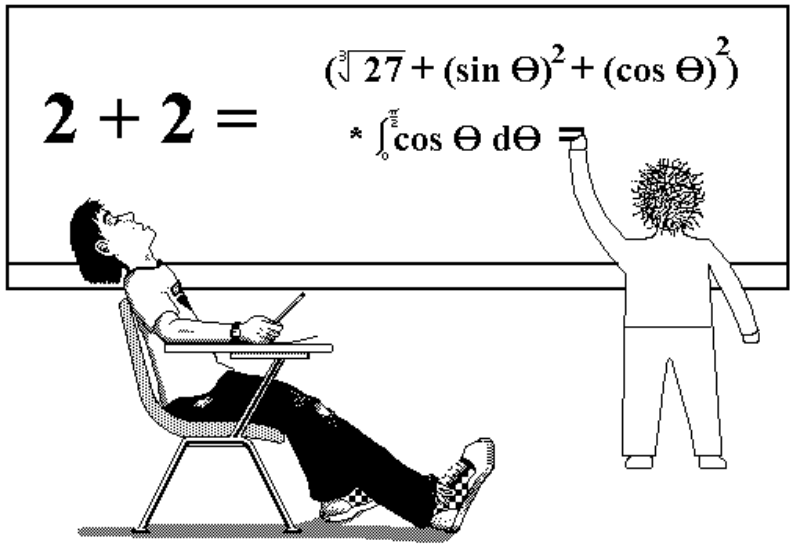
Resilience: A Comparative Analysis

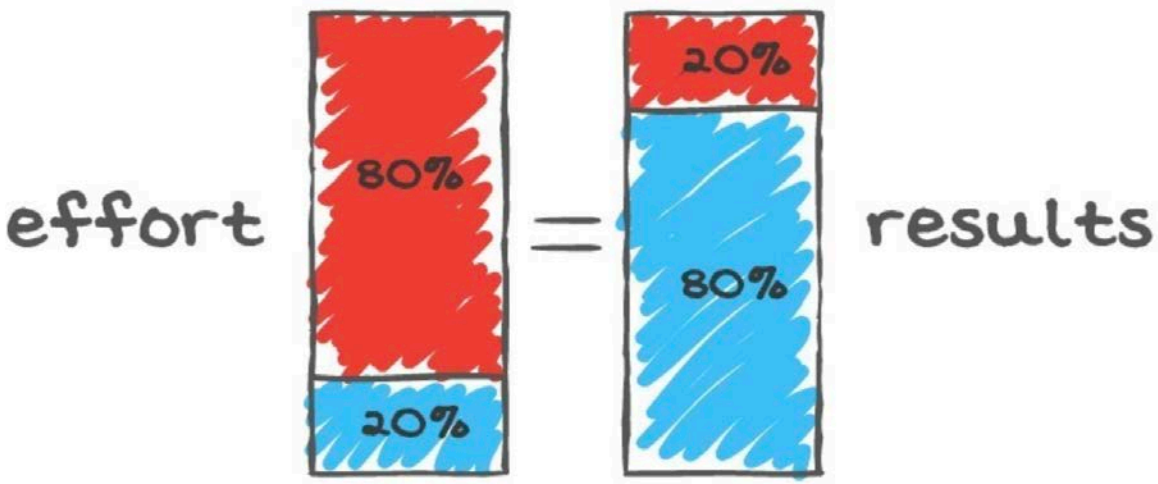
Human Resilience		Cyber Resilience	
Pre-Sick	**Post Sick**	**Pre-Boom**	**Post-Boom**
Get Multivitamins	Rest and Sleep	Access Control	Incident Response
Exercise	Medication	Threat Intelligence	Forensic Analysis
Stay Hydrated	Therapy	IR Simulations	Communications
Avoid Fatty Foods	Family Support	Effective T&A	External Support

Outsmarting Bytes with Bits!

"If you can't explain it simply, you don't understand it well enough." ~ Albert Einstein

KISS Principle	Pareto Principle





Outsmarting Bytes with Bits!

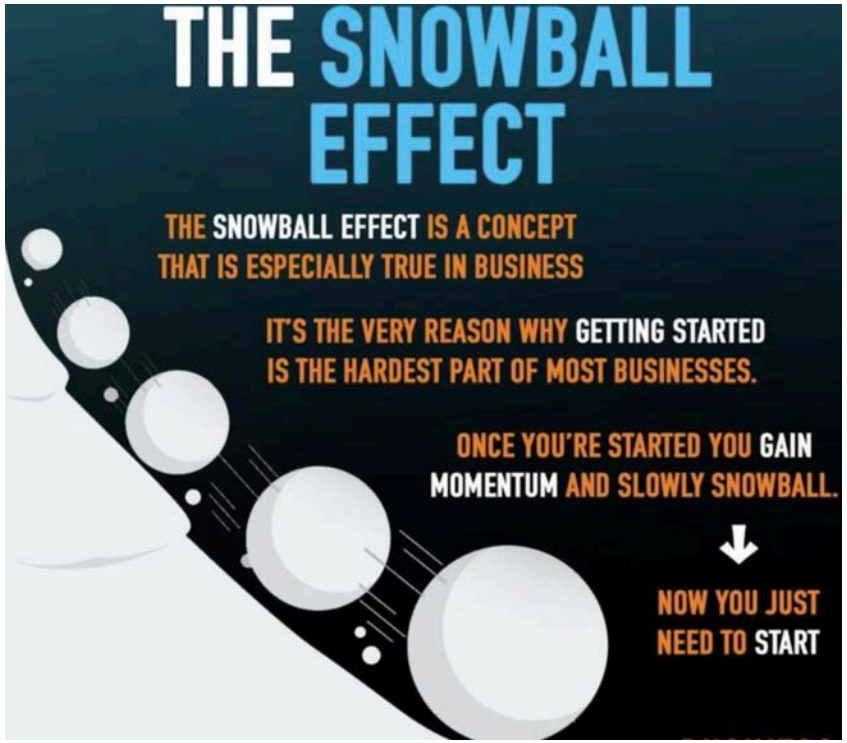
- Cyber Resiliency exercises are still not a requirement in majority of regulations across globe

- Bad Thing: Many organizations have Compliance-driven mind-set
    - No obligations to do a resiliency review

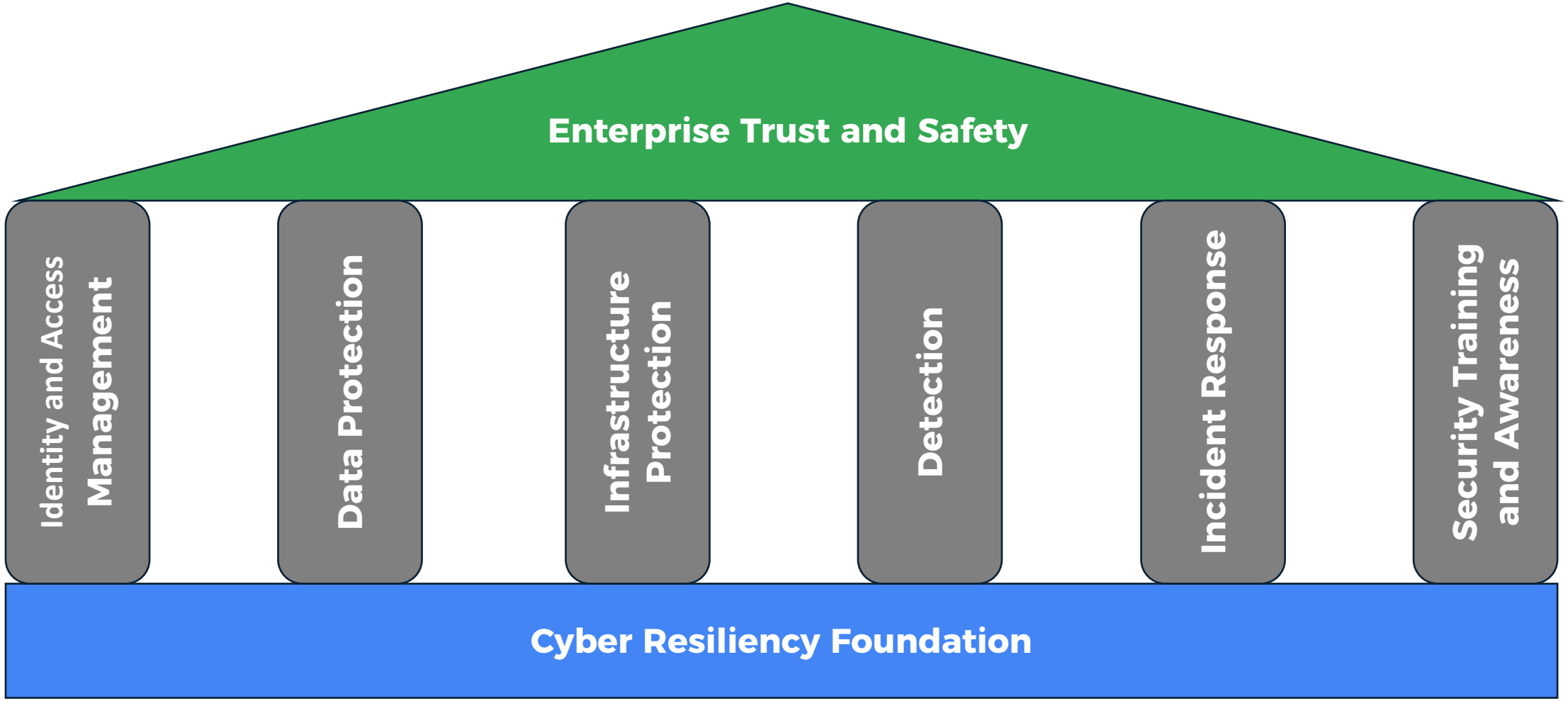
- Good Thing: Cyber Resiliency exercises can be self-driven/ self-assessment, and can be conducted by either 1st, 2nd or 3rd line of defense

Ready to boot up the Resilience?

- So where can we get started?
    - The various domains in InfoSec world is vast and cumbersome
- If we look into NIST as an example:
    - 800-53 has 20 Control Families
    - CSF has 23 Categories
- If we look into Cyber Resiliency Review from CISA as an example:
    - CRR has 10 domains



The Cyber Six-Pack: Flex Those InfoSec Muscles



The Cyber Six-Pack: Flex Those InfoSec Muscles

- Think about the 6 domains from holistic perspective, i.e., both 1st and 3rd Party lens (aka Same Rule for Everyone and Everything!)
- Think about these domains in centralized fashion (as much as possible)
- For each domain, keep the following 5 Ws framework as baseline for Resiliency Review:

1. WHO: Who are all important stakeholders for that particular domain? Have they been identified, documented, and formally signed-off? Signed-off RACI for each domain

2. WHAT & WHY: Is the Governance (Policies, Standards, Procedures, Guidelines, Playbooks and/or controls) created, approved, and socialized?

3. WHEN & WHERE: When are the actions performed (Frequency) and Where is it being performed (Pinpoint People, Process and Technology)? →→→→→→ [Includes Software and Inventory Assets]

4. HOW: How is the domain running? Test of Design and Test of Operating Effectiveness

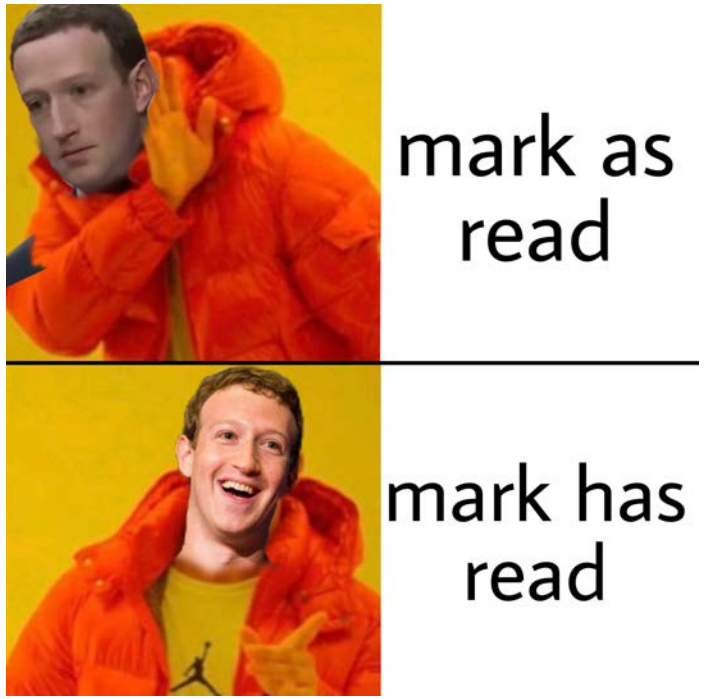
Identity and Access: The Welcome Mat for Ransomware?

- Everything starts at IAM. Effective Identity and Access Management (IAM) is the cornerstone of ransomware resilience.
  - First Line of Defense
  - Detection and Alerting
  - Limit Ransomware Reach
  - User Behavior Analytics
- Strong IAM program means Right People should have Right Access at Right Time to your Data, Systems, Assets, Infra or other technologies
- Sample Metric:
  1. XX% of PAGs have Just-In-Time Access (Right Access at Right Time)
     a. PAGs W/ JIT% =[$\frac{\sum_{i=1}^{n} w(i) \times JIT(i)}{Total\ Number\ of\ PAGs}$] x 100
     - n is the total number of PAGs in your dataset.
     - $w(i)$ represents the weight assigned to each PAG.
     - $JIT(i)$ represents the Just-In-Time Access value for each PAG.

Multi-Factor Authentication | Principle of Least Privilege | User Behavior Analytics | Secure Lifecycle of Identities | Access Rotation & Audits | Just-In-Time Access

Guard your Bytes, Because Hackers are always Biting!

- Encrypt a Byte, shield it from Ransomware Plight
  - Rapid Recovery
  - Financial Savings
  - Data Availability
  - Avoidance of Secondary Attack
- Strong Data Protection program ensure the data is secure even if the infrastructure is compromised
- Sample Metric:
  - XX% of successful data backups and restorations out of all attempts made.
    a. Calculation (for backups): (Number of Successful Backups / Total Backup Attempts) x 100



Periodic Backup w/ Air Gapping

Data Flow Threat Modeling

Secure Key & Cert Management

Keep Direct Data Access Away

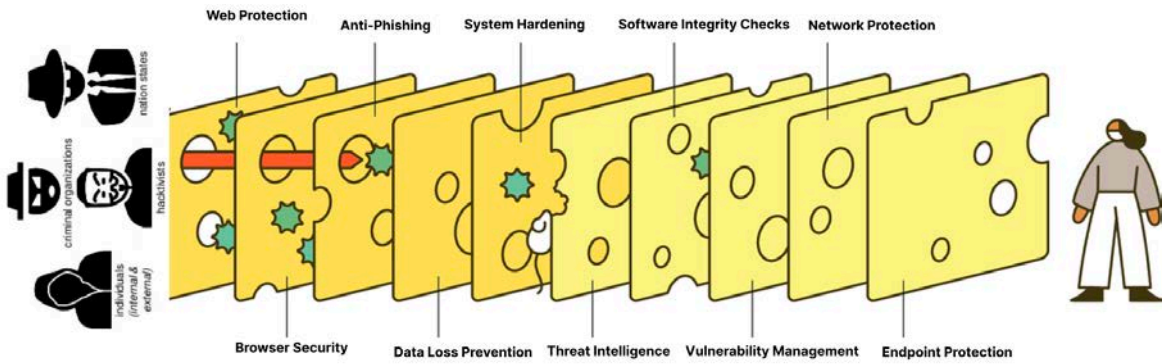
Auto. Data Encryption

Establish Decoy Data

Building a Cyber Igloo: Cold as Ice, Strong as Stone!

- Cold as Ice (Think Layered Defense): Just as an igloo's layers insulate from the cold, our layered defense strategy insulates from ransomware threats
- Strong as Stone (Think Hardening and Testing Everything): Just as igloo's structure cannot drift from baseline, so can't our infrastructure

Alternative Thinking Model: Swiss Cheese Model



- <u>Sample Metric</u>:
  - Hardening and Drift Protection: Combination of Config Change Frequency, Drift Detection Rate and Time to Remediate Drift =

    [(Number of Configuration Changes / Time Period) + (Number of Systems Detected with Drift / Total Number of Systems) + (Total Time Taken for Drift Remediation / Number of Drift Incidents)] / 3

DMARC and Anti-Phishing

Software Integrity Checks

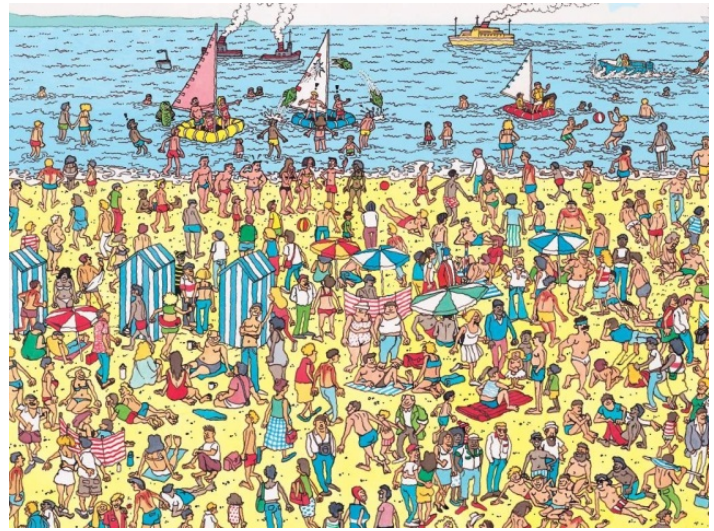
Hardening and Drift Protection

Keep Direct Data Access Away

Network Segmentation

Establish Decoy Tech Stack

Finding Cyber Threats: It's Like 'Where's Waldo?' but Riskier!



- In a digital environment filled with benign activities, malicious operations often camouflage themselves.
- Why Ransomware are sneaky?
  - Polymorphic Codes and Fileless Execution
  - Use of Legitimate Credentials (Remember Mimikatz??)
  - Tor & Decentralized Communications
- **Sample Metric**:
  - **Weighted** Dwell Time = $$\frac{\sum (\text{Dwell Time of Each Incident} * \text{Weigh of respective Threat Actor})}{\sum \textit{Weight of all Threat Actors for the incidents}}$$

Where Dwell Time = Time of detection - Time of initial breach (or intrusion)

User/Entity Behavior Analytics	Log Aggregation and Analysis	Pro-active Threat Intel
EDR Systems	Vulnerability Management PgM	Decoy Technology

Tech-tastrophes & Turbo Turnarounds

- Remember our Igloo? Sealing the Entry (Think Rapid Response): If ransomware gets a foot in the door, swift action is key
- Pre-Tech-tastrophes Planning: Everything we discussed previously; Regular backup & offline copies, MFA, and etc.
- Turbo Turnaround Execution:
  - Isolate infected devices and restore from most recent clean backup
  - Engage cybersecurity professionals and inform law enforcement
  - Post-incident analysis for Continuous Improvement
- Sample Metric:
  - Cost of Ransomware Recovery < X% of Revenue

    CRR = Ransom payment + Cybersecurity costs + Data recovery costs + System repair/replacement costs + Legal and compliance costs + PR and reputation management costs + any additional costs

Incident Response Playbooks

Redundant Hot Infras for CJAs

Incident Simulation and Drills

Logging and Retention

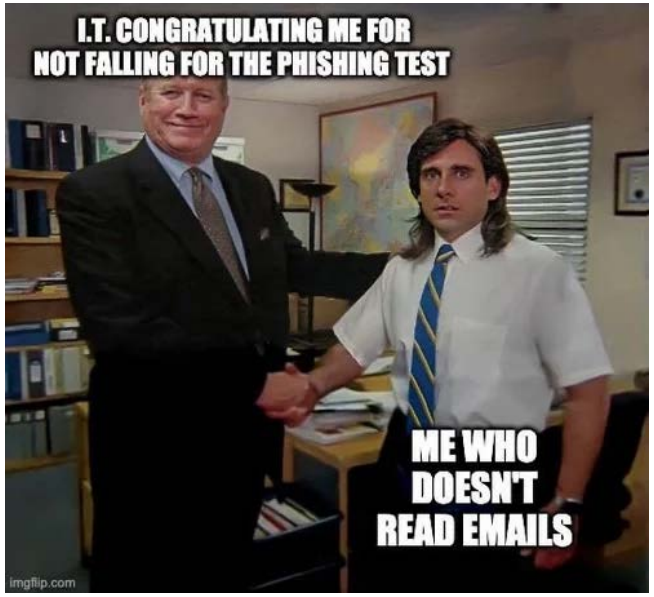
Incident Response Retainers

Established IR Comms PgM

Lights, Camera, a Cyber Resilience: A Training Odyssey

- Preparation is Key: Just as a film production team meticulously plans every scene, organizations need to prepare for potential ransomware attacks
- Cast of Characters: Compare the roles within an organization to characters in a movie. Highlight that everyone, from top executives to front-line employees
- Scripted Responses: Like actors following a script, employees should know how to respond in case of a ransomware incident
- Practice Makes Perfect: Just as actors rehearse their lines and scenes, employees should practice ransomware response through simulated exercises

- Sample Metric:
    - Simulated Exercise Performance: Assess how well employees perform in simulated ransomware exercises. Track metrics such as response time, adherence to procedures, and successful containment.



Incident Simulation and Drills

Board and Exec Training & Drills

Data Class. & Handling Drills

Phishing Simulations

Proactive PAG Trainings

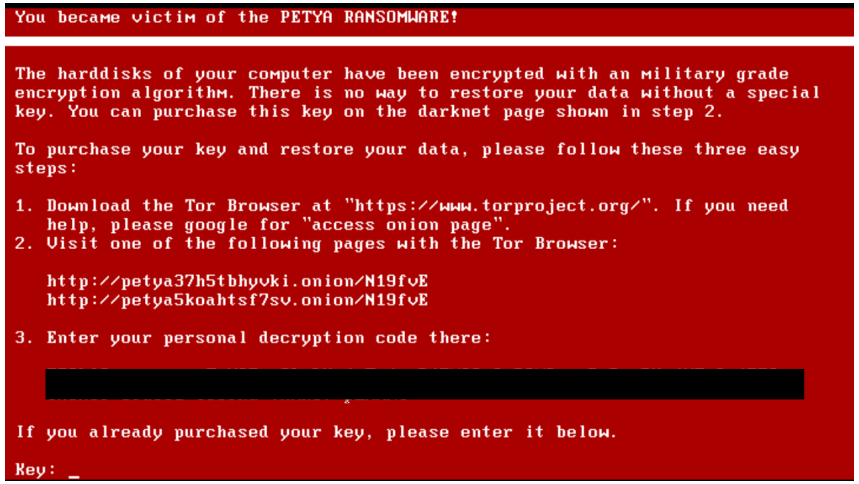
Reactive PAG Trainings

Case Study – A [$10B] Reasons to Boost Resilience: Six Packs to Withstand NotPetya & Beyond

- In June 2017, the NotPetya ransomware outbreak rapidly spread across the world, affecting multiple organizations
- The malware encrypted files, making them inaccessible, and demanded a ransom for decryption.
- NotPetya's primary target was Ukrainian businesses, but its design allowed it to spread beyond those borders quickly.
- NotPetya primarily used the EternalBlue exploit to target vulnerabilities in Microsoft Windows' SMB protocol.
- SMB stands for Server Message Block. It's a communication protocol used by Windows computers to share access to files and printer sharing (multiple computers using 1 printer)

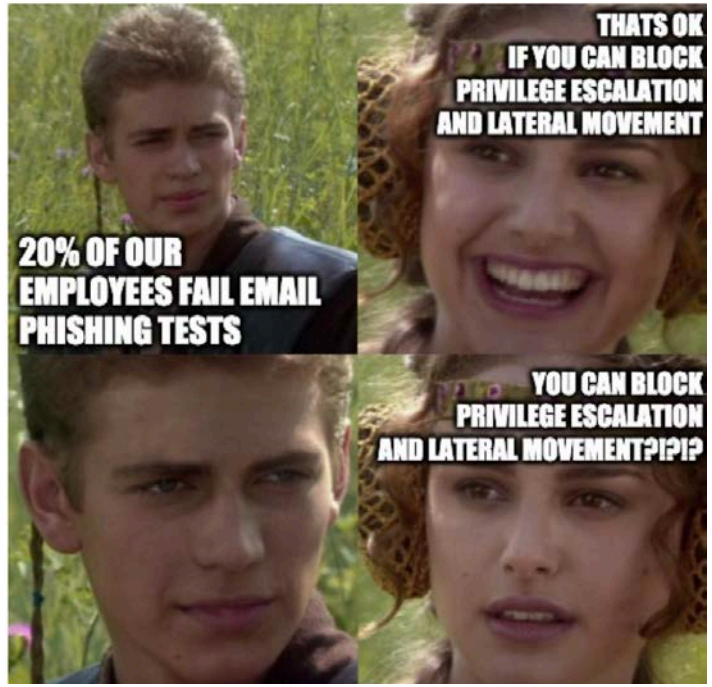
Case Study – A [$10B] Reasons to Boost Resilience: Six Packs to Withstand NotPetya & Beyond

1. Initial Infection Vector: The primary initial infection vector for NotPetya was a compromised update for a popular Ukrainian tax software called MEDoc. This allowed it to infiltrate many Ukrainian organizations quickly.
2. Exploitation: NotPetya used the EternalBlue exploit and other vulnerabilities in the Microsoft Windows SMB protocol to penetrate systems.
3. Lateral Movement: NotPetya used multiple techniques, such as Mimikatz, to extract credentials and move laterally across networks. This allowed it to spread rapidly and infect machines that did not have the vulnerable SMB protocol version.
4. Encryption: Modified the Master Boot Record, rendering systems unbootable. Modified the Master Boot Record, rendering systems unbootable.
5. Ransom Note: Infected systems displayed a ransom note demanding payment in Bitcoin. However, given the design of the malware and its payment infrastructure, it became evident that monetary gain was not the primary objective; rather, it aimed to cause widespread disruption.
6. Destruction: NotPetya's encryption was more about destruction than ransom.



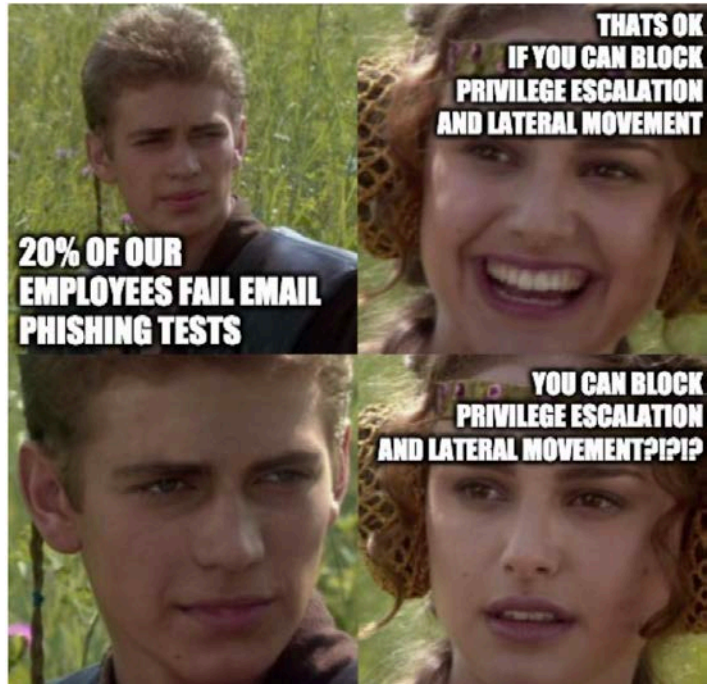
Case Study – A [$10B] Reasons to Boost Resilience: Six Packs to Withstand NotPetya & Beyond

1. Data Protection:.
    a. Actual Situation: Many affected organizations didn't have proper backup systems in place or had backups that were also compromised in the attack.
    b. Enhanced Resilience: A robust backup strategy, with regular backups stored offline or in isolated environments, would ensure that even if primary systems were compromised, data could be rapidly restored without paying the ransom.
2. Identity and Access Management:
    a. Actual Situation: Exploited administrative privileges to propagate and execute its malicious payload.
    b. Enhanced Resilience : By implementing least privilege policies, where users and systems only have the minimal access necessary to perform their roles, the malware's spread could have been significantly reduced.
3. Infrastructure Protection:
    a. Actual Situation : Exploited vulnerabilities in outdated software.
    b. Enhanced Resilience : A strong patch management system ensures that all software, especially mission-critical ones, are regularly updated to protect against known vulnerabilities.



Case Study – A [$10B] Reasons to Boost Resilience: Six Packs to Withstand NotPetya & Beyond

4. Detection:.
    a. Actual Situation : NotPetya spread rapidly, indicating that many organizations did not detect the intrusion in its early stages.
    b. Enhanced Resilience : Advanced threat detection systems, along with network monitoring tools, would identify unusual behavior and raise red flags, allowing for quicker containment of the malware.
5. Incident Response:
    a. Actual Situation : Many affected companies had slow or uncoordinated responses, resulting in extended downtimes and significant financial losses.
    b. Enhanced Resilience : A well-practiced incident response plan would have enabled quicker decision-making, minimizing the attack's operational and financial impacts.
6. Infrastructure Protection:
    a. Actual Situation : Initial infection vectors included phishing emails and malicious downloads.
    b. Enhanced Resilience : Regular training of employees to recognize and avoid suspicious emails or links could have reduced the malware's entry points.



A $10B Conclusion

While the NotPetya attack was particularly virulent and sophisticated, a robust cyber resilience strategy touching on the six pillars would have significantly reduced its impact.

This case study underlines the importance of a holistic approach to cybersecurity, emphasizing not just prevention, but also effective overall resilience strategy.

Thank You!!

LinkedIn