FORO EJECUTIVO

CIBERSEGURIDAD EN EL sector financiero

CIBERCRIMEN: INCERTIDUMBRE Y COMPLEJIDAD

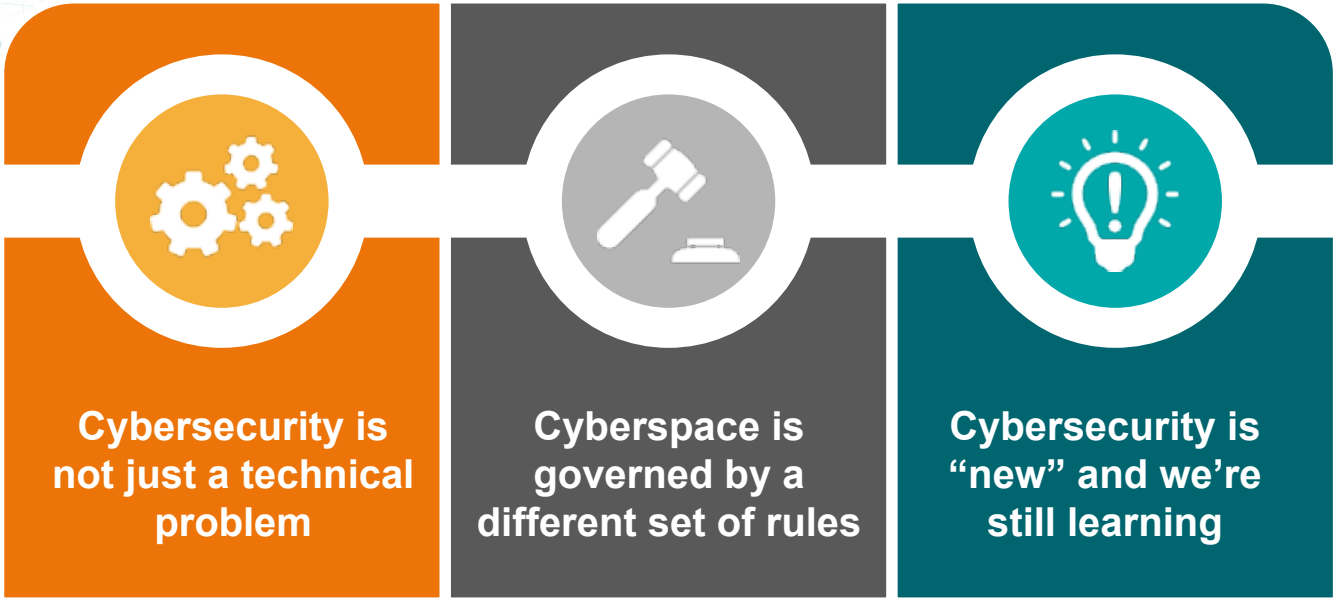
Changing the game: A different approach to cybersecurity for the Financial Sector

Michael Daniel
President & CEO

CYBER THREAT ALLIANCE

Scitum | TELMEX está contigo

why is cybersecurity hard?



Cybersecurity is also an economic, psychological, and human behavioral challenge

The concepts of distance, borders, and proximity all operate differently in cyberspace compared to the physical world

We haven't had the time or the experience to develop the comprehensive frameworks required to address cyber risk

CYBER THREAT ALLIANCE

How is the cyber threat evolving?

The four primary types of cyber adversaries

Hactivists
Act in support of a cause

Criminal organizations
Profit off malicious activity

Terrorists
Leverage cyberspace to recruit

Nation States
Pursue their national interests

Volume and diversity of connected devices increases complexity

Low barriers to entry and high ROI incentive actors

More broad
The attack surface is exponentially increasing

More frequent
Volume of malicious cyber activity is increasing

Because of these actors, the cyber threat is becoming….

More dangerous
Actors are increasingly moving to more destructive activity

More disruptive
Potential impacts of a cyber incident are increasing

Critical infrastructure is at the center of actors' malicious activity

Digital dependence is making society increasingly vulnerable

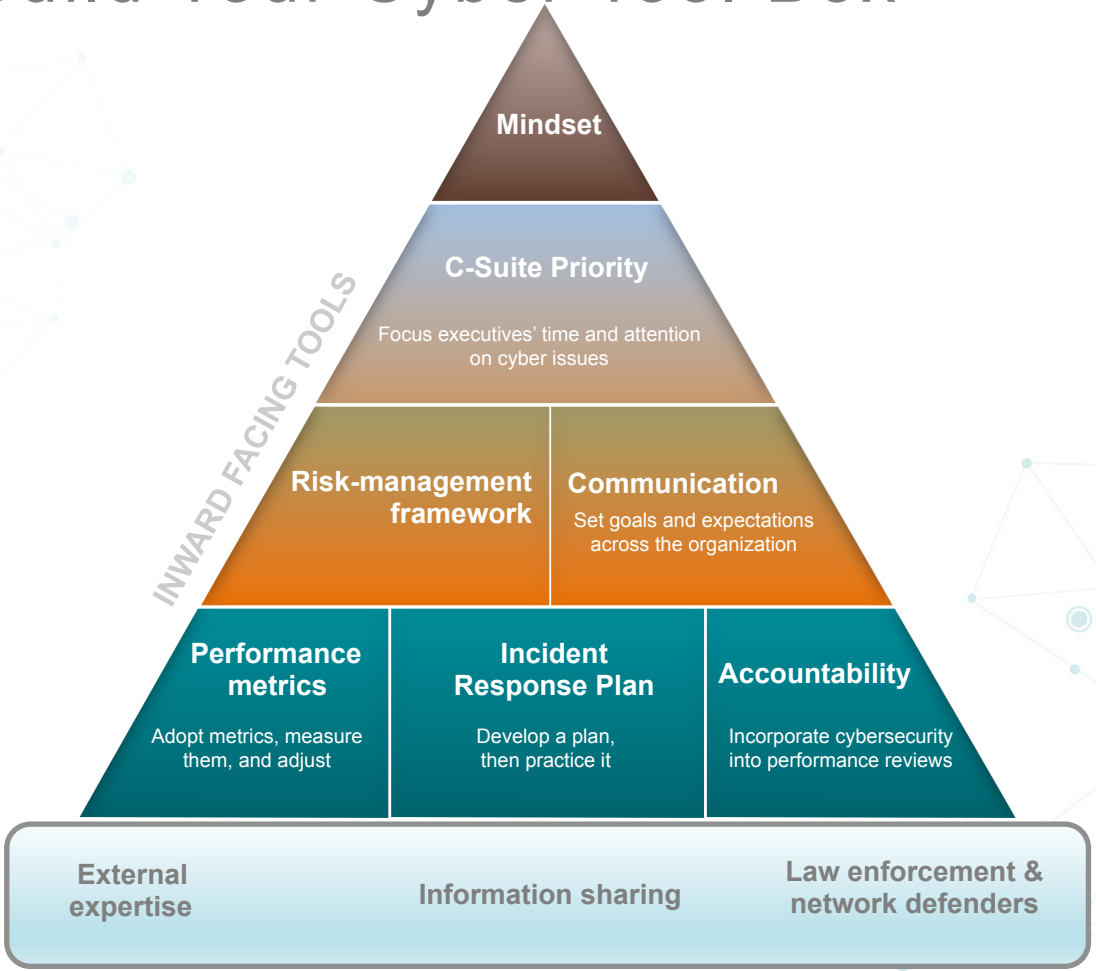
CYBER THREAT ALLIANCE

BUT, It's not all bad

All malicious actors face limitations:

- Hollywood ≠ real life
- Capacity constraints
- Limited number of paths to achieve their goals
- Operations occur on defender's networks

Take Action: Build Your Cyber Tool Box



CYBER THREAT ALLIANCE

TAKE ACTION: Collaborate externally

Cooperate with the cybersecurity industry

It's not what you know, but what you do with what you know

Undermine the criminal business model systematically

Make them undertake business process re-engineering

Coordinate disruption and response activities between governments and private sector actors

Not "hackback" but focus on comparative advantage

QUESTIONS?

Nation-State cyber capabilities: benefits, constraints, and RISKS

Benefits

- Effective
- Relatively cheap and fast
- Levels the playing field
- Deniability

Constraints

- Intelligence dilemma
- Third country conundrum
- Bureaucratic challenges
- Collateral damage uncertainty
- Tool reuse

Systemic Risks

- Attribution difficulties
- Offense favored over defense
- Unintended consequences

NATION-STATE Cyber Capabilities: dealing with the systemic risk

Analogies that don't apply:

Border security

Missile defense

Nuclear deterrence

Approaches having some promise:

Operational Collaboration

Transparency

International Norms

Confidence-building measures
Resilience

GRACIAS

DESCARGUE ESTA PRESENTACIÓN EN

resources | scitum

resources.scitum.com.mx

Scitum | TELMEX está contigo