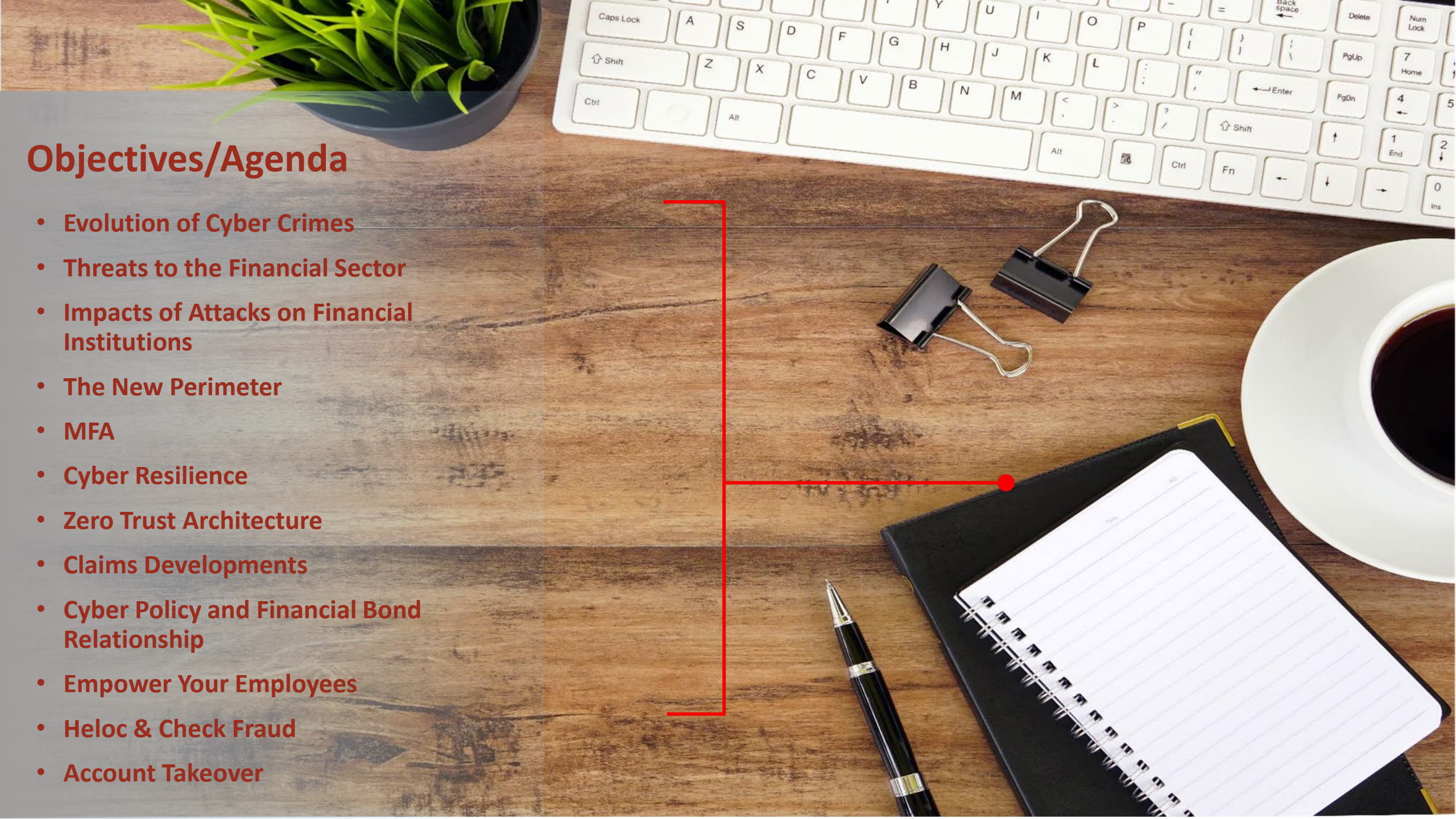

TRAVELERS
The Evolution of Cybercrime

DISCLAIMER

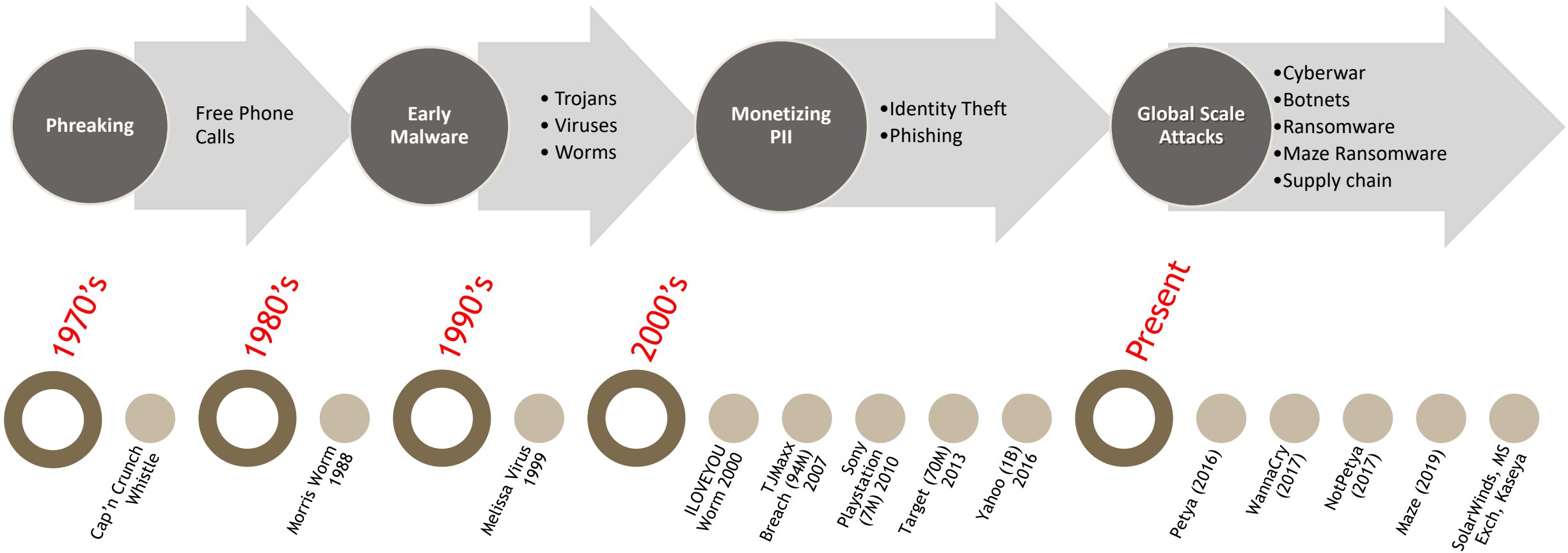
This material in this presentation is for general informational purposes only and is not legal advice. It is not designed to be comprehensive, and it may not apply to your particular facts and circumstances. Consult as needed with your own attorney or advisor. Any examples or discussions of coverages reflect those generally available in the marketplace and are not based specifically on the policies or products of any particular carrier.

Objectives/Agenda

- Evolution of Cyber Crimes
- Threats to the Financial Sector
- Impacts of Attacks on Financial Institutions
- The New Perimeter
- MFA
- Cyber Resilience
- Zero Trust Architecture
- Claims Developments
- Cyber Policy and Financial Bond Relationship
- Empower Your Employees
- Heloc & Check Fraud
- Account Takeover



Evolution of Cyber Crime



Threats to the financial Industry

Per the Verizon 2021 Data Breach Investigations Report

Financial institutions suffered up to 81% of breaches due to web application and Social Engineering attacks with close to 40% of the breaches caused by internal actors.

Financially motivated organized criminal groups continue to target this sector**, with the deployment of Ransomware being a favored tactic.**

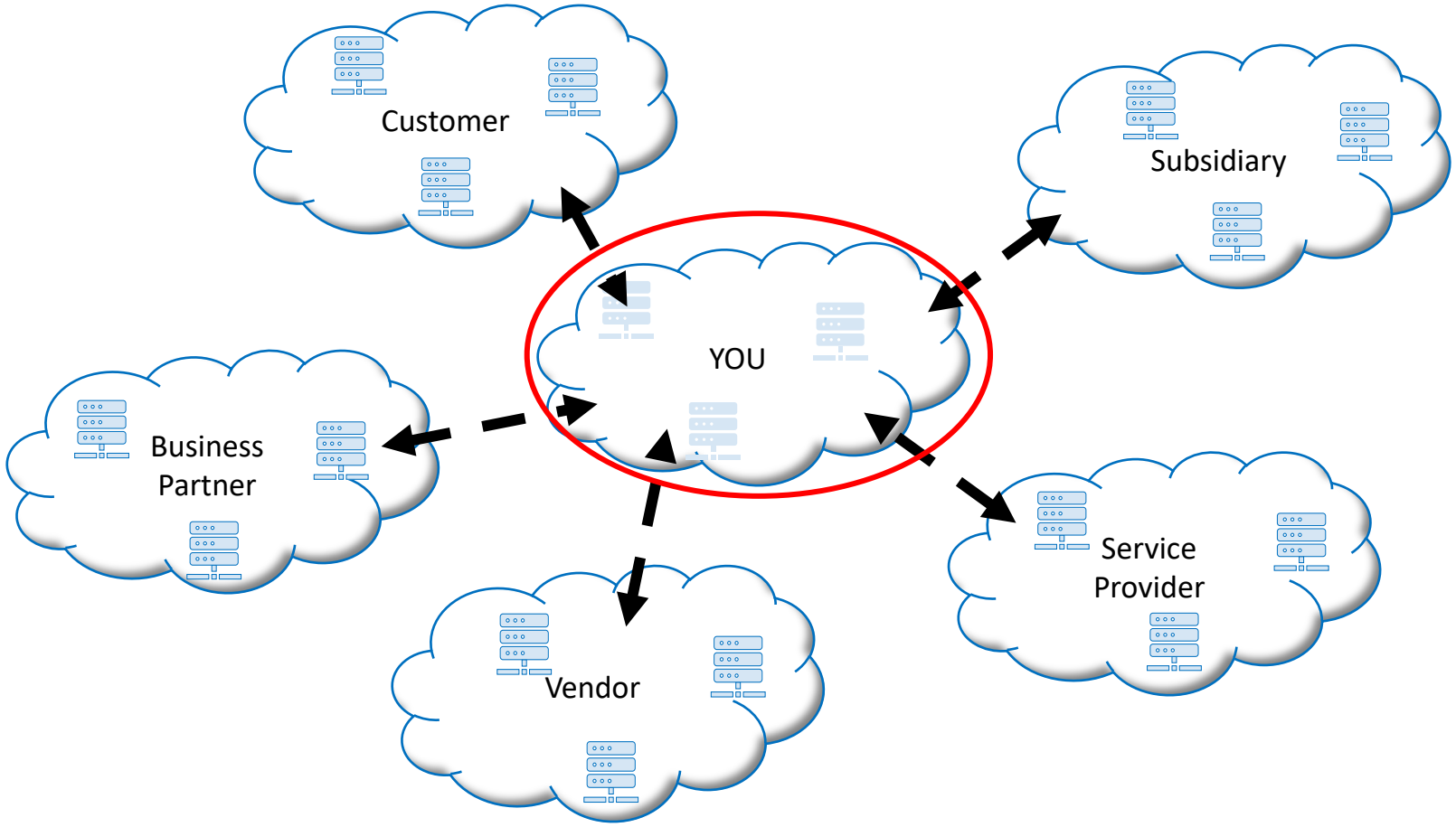
Frequency	721 incidents, 467 with confirmed data disclosure
Top Patterns	Miscellaneous Errors, Basic Web Application Attacks, and Social Engineering represent 81% of breaches
Threat Actors	External (56%), Internal (44%), Multiple (1%), Partner (1%) (breaches)
Actor Motives	Financial (96%), Espionage (3%), Grudge (2%), Fun (1%), Ideology (1%) (breaches)
Data Compromised	Personal (83%), Bank (33%), Credentials (32%), Other (21%) (breaches)
Top Protective Controls	Security Awareness and Skills Training , Secure Configuration of Enterprise Assets and Software, Access Control Management

Source: 2021 Verizon Data Breach Investigation Report

Impacts of Cyber Attacks on Financial Sector

- Attacks on financial institutions are causing direct harm to people and organizations by targeting personal, bank account and credit information of customers.
- Attacks are increasing and evolving as they continue to exploit vulnerabilities in the financial sector's complex digital infrastructure and weaknesses in its cybersecurity controls.
- Attacks on financial institutions are low-risk, high-reward crimes. Acting with near impunity, criminals and state actors are joining forces against financial institutions with varying motives and agendas.
- Small & Medium sized banks are prime targets.
- Remember the SWIFT breaches?

What's in *Your* Perimeter?



Importance of MFA from the Experts

Per Microsoft:

99.9%

of account compromise attacks can be blocked by MFA

Per Arete:

94%

of ransomware victims they investigated did not use MFA

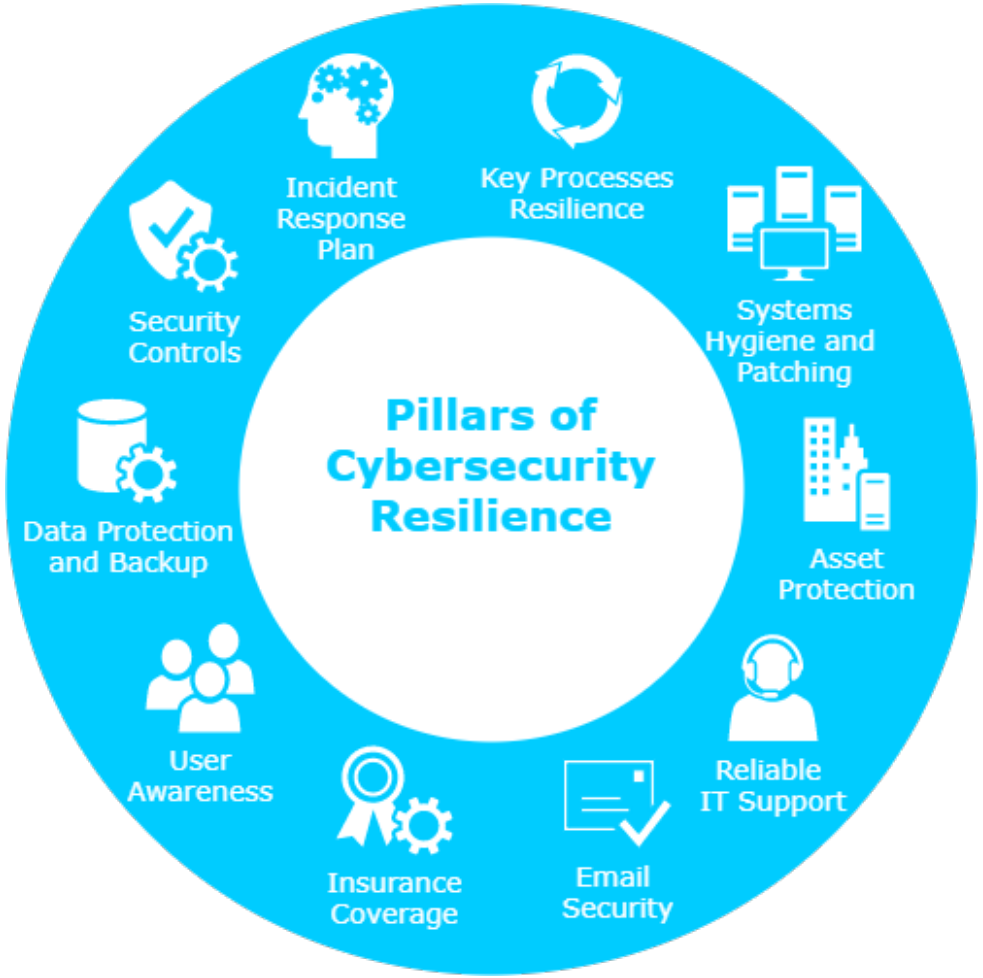
Sources: https://www.microsoft.com/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/, Arete Presentation “Ransomware Cards” 7-31-20

Cyber Resilience

The ability to:

- Anticipate,
- Withstand,
- Recover from, and
- Adapt

to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.

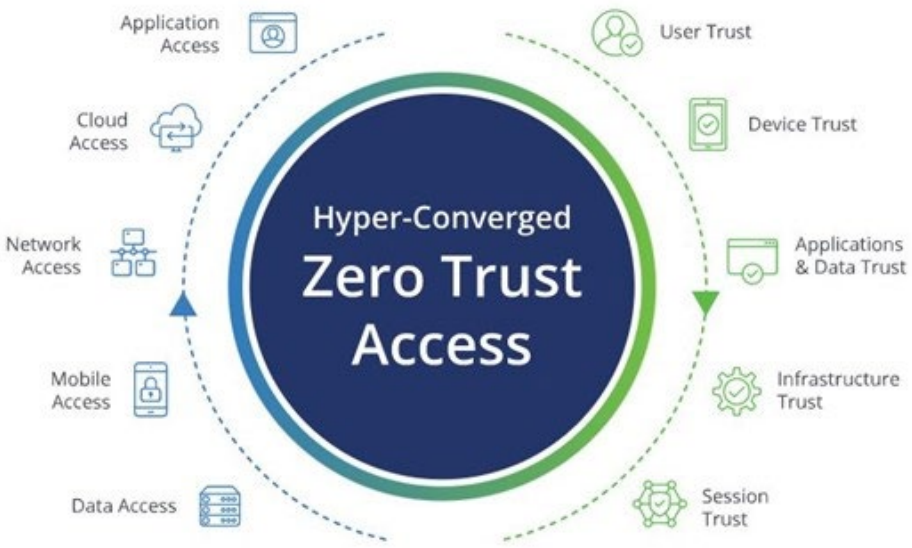


Source: NIST SP 800-160 vol. 2

Zero Trust, Aka Trust No One, Verify Always

Guiding principles of Zero Trust:

1. Verify explicitly. ALWAYS authenticate and authorize based on all available data points
   - user identity
   - location
   - device health
   - service or workload
   - data classification
   - anomalies
2. Use least privileged access. Limit user access with:
   - *Just-In-Time* and *Just-Enough Access* (JIT/JEA)
   - Risk-based adaptive polices
   - Data protection to protect both data and productivity
3. Assume breach. Minimize blast radius for breaches and prevent lateral movement by:
   - Segmenting access by network, user, devices, and application awareness
   - Verify all sessions are encrypted end to end
   - Use analytics to get visibility, drive threat detection, and improve defenses



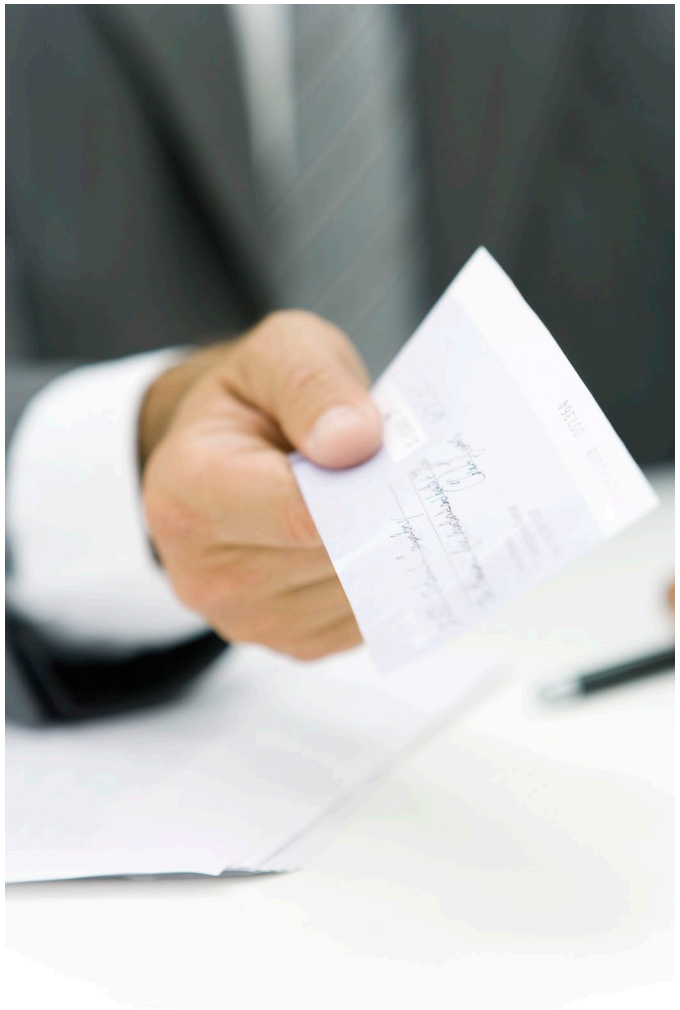
Source: https://go.microsoft.com/fwlink/p/?LinkID=2109181&clcid=0x409&culture=en-us&country=US

Claim Developments

Cyber Policy & Financial Institution Bond Relationship

Stop the Line: Empowering Employees to Speak Up

HELOC & Check Fraud



Account Takeover

THANK YOU

REHMAN KHAN

TED LANSDALE

630-961-7018

781-817-8457

rkhan7@travelers.com

tlansdal@travelers.com