Munich RE

Cyber Lunch & Learn

Agenda

Munich RE

Meet The Team

1. Introductions
2. Performance & Results

Introduction to Cyber

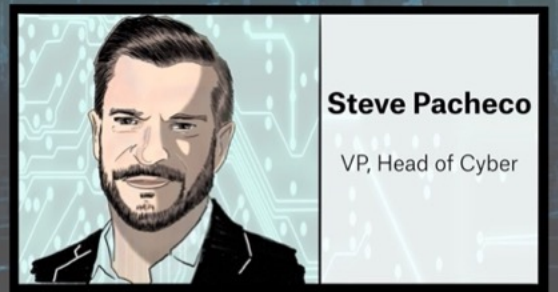
3. Cyber Product
4. State of The Market

Exploring Coverage Application

5. Coverage Demonstration
6. Safeguards Demonstration
7. The Future

Meet The Team

Munich RE

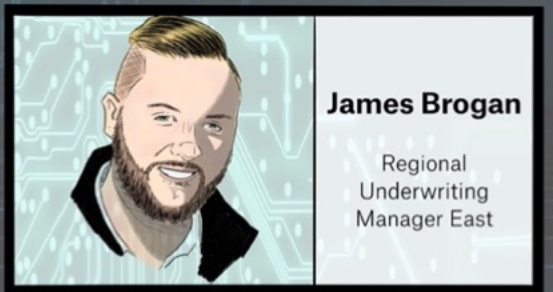


Steve Pacheco

VP, Head of Cyber

Interests

Munich RE

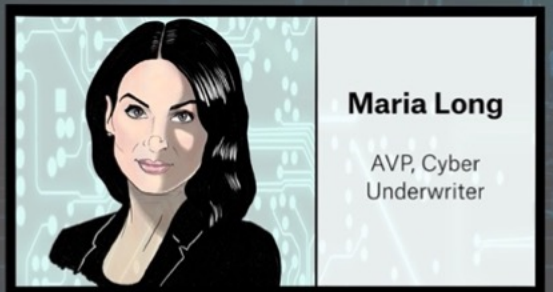


James Brogan

Regional Underwriting Manager East

Interests

Munich RE

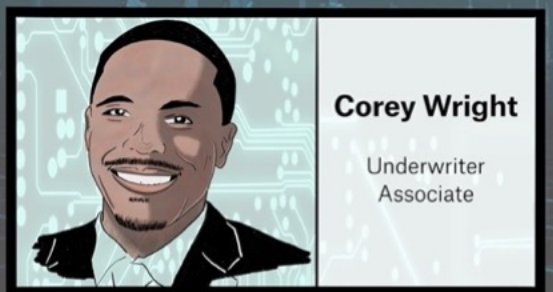


Maria Long

AVP, Cyber Underwriter

Interests

Munich RE



Corey Wright

Underwriter Associate

Interests

Munich RE

Performance/Results

Munich RE

Products

Munich RE

Cyber Liability

1st and 3rd party liability coverage. Covers financial loss for data breach events. Costs include income loss from a business interruption event, breach notification expenses, cyber extortion loss (i.e. ransomware) etc.

Example:

Maersk – 2017 Cyberattack

Cause:

A malware worm variant dubbed “NotPetya”

Effect:

49,000 laptops destroyed; 1,200 applications inaccessible; 1,000 applications destroyed; 3,500 of 6,200 servers destroyed. Roughly $300M in total losses.

Products

Munich RE

Technology Errors & Omissions Liability

1st and 3rd party liability coverage. Covers financial loss for data breach events. Costs include income loss from a business interruption event, breach notification expenses, cyber extortion loss (i.e. ransomware) etc. Tech E&O is designed for Technology service providers – hardware or software. Affords coverage for financial loss when products or services fail. This should not be conflated with product liability insurance.

Example:

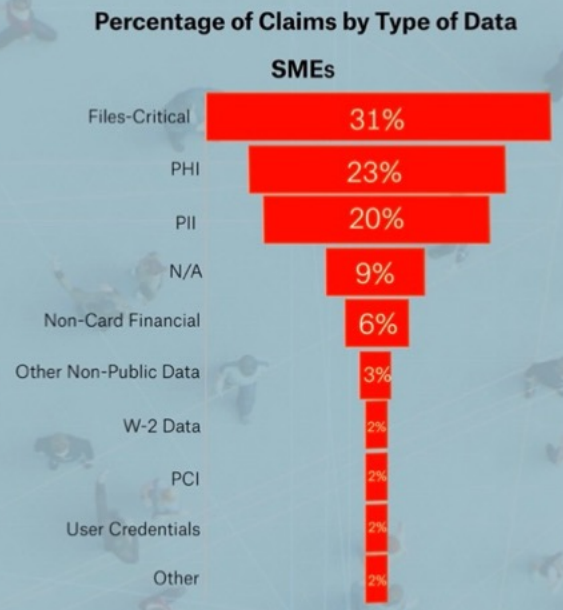
A supply chain visibility (SCV) software enterprise was hired by a Logistics firm to develop an SCV platform for real time insights into their supply chain. The logistics firm alleged problems with the roll out of the platform and its functionality. The logistics firm terminated the agreement and commenced a lawsuit alleging damages in excess of $5M.

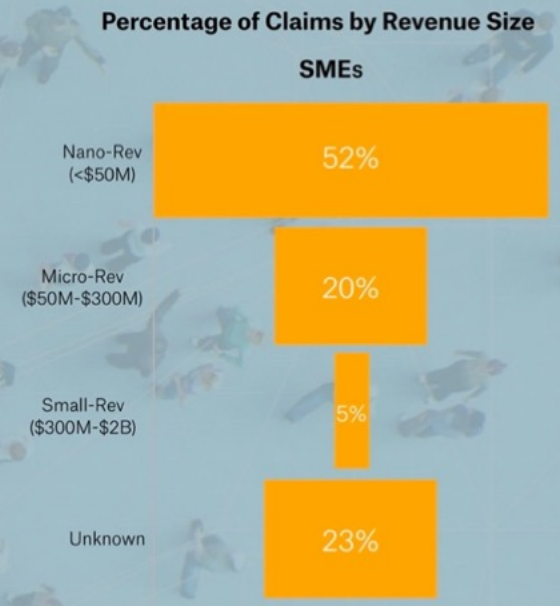
State of the Market

Munich RE

- **Hard market – an underwriter's market (real estate reference)**

NetDiligence 2021 Cyber Claims Study





Outlook

Munich RE

- Pre-breach services
- Expansion of the team
- Evolution of products
- Claims information to inform underwriting appetite
- GWP target

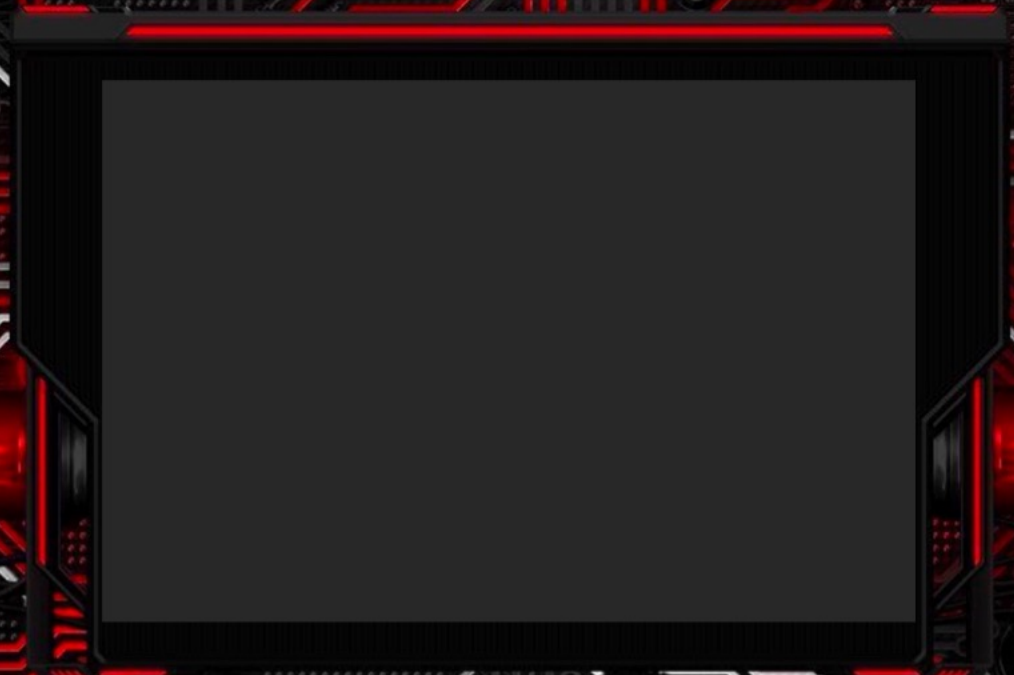
Social Engineering

Munich RE

What Is Social Engineering?

A form of attack that exploits human nature and human behavior. People are the weakest link in security because they can make mistakes, be fooled into causing harm, or intentionally violate company security. Social engineering attacks take two primary forms: convincing someone to perform an unauthorized operation or convincing someone to reveal confidential information.

Example:

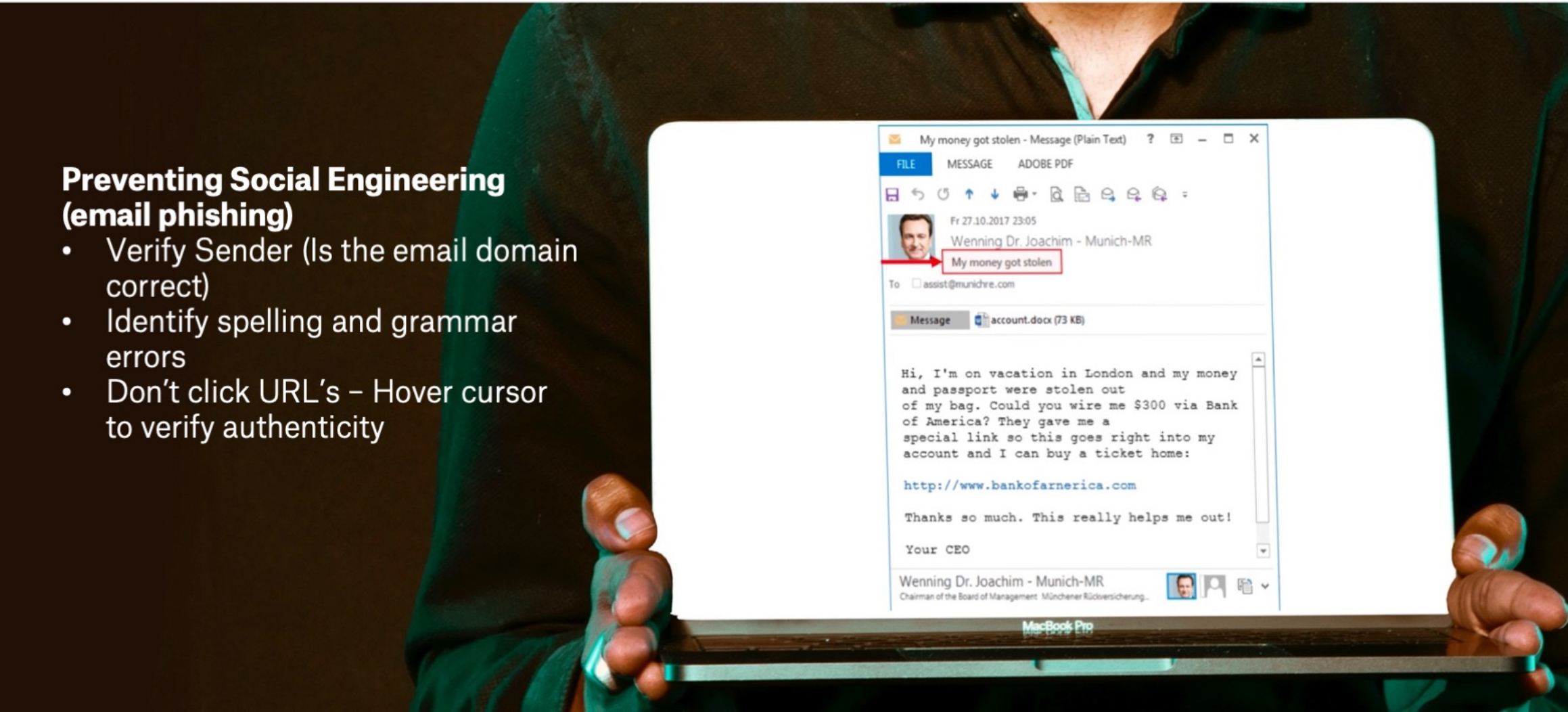


Social Engineering

Munich RE

Preventing Social Engineering (email phishing)

- Verify Sender (Is the email domain correct)
- Identify spelling and grammar errors
- Don't click URL's – Hover cursor to verify authenticity



Social Engineering

Munich RE

Deepfake information