EMEA Update on Claims and Loss Prevention

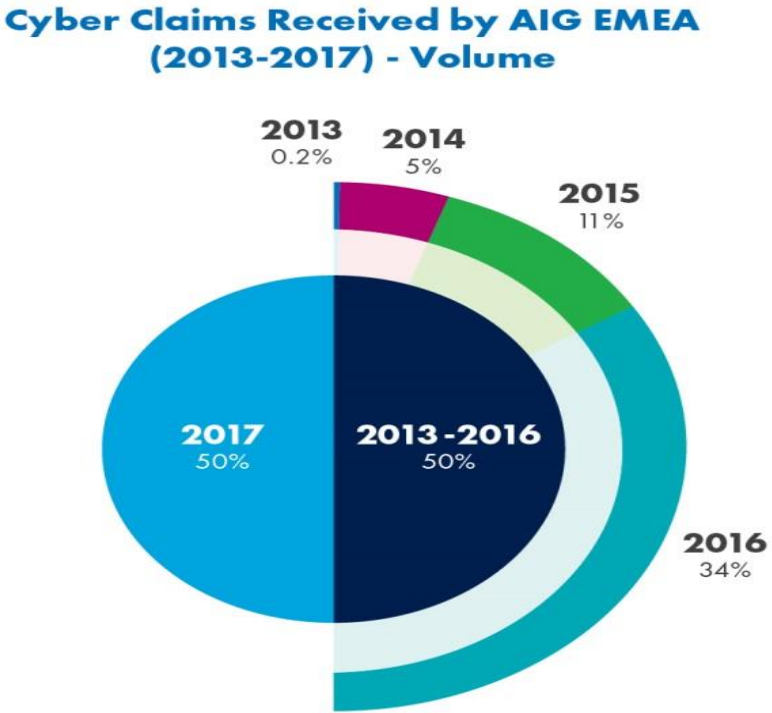
Mark Camillo
Head of Cyber, EMEA
Mark.Camillo@AIG.com

Introduction

- Cyber continuing to expand (moving towards affirmative coverage across lines viewing cyber as a peril)
- Largest segment still FI's but interest across all industries
- Cyber claims on the rise – over 300 cyber claims reported across EMEA in 2017
- Moving towards more transparency in the underwriting process with enhanced underwriting questionnaire/model
- Loss prevention services growing trend

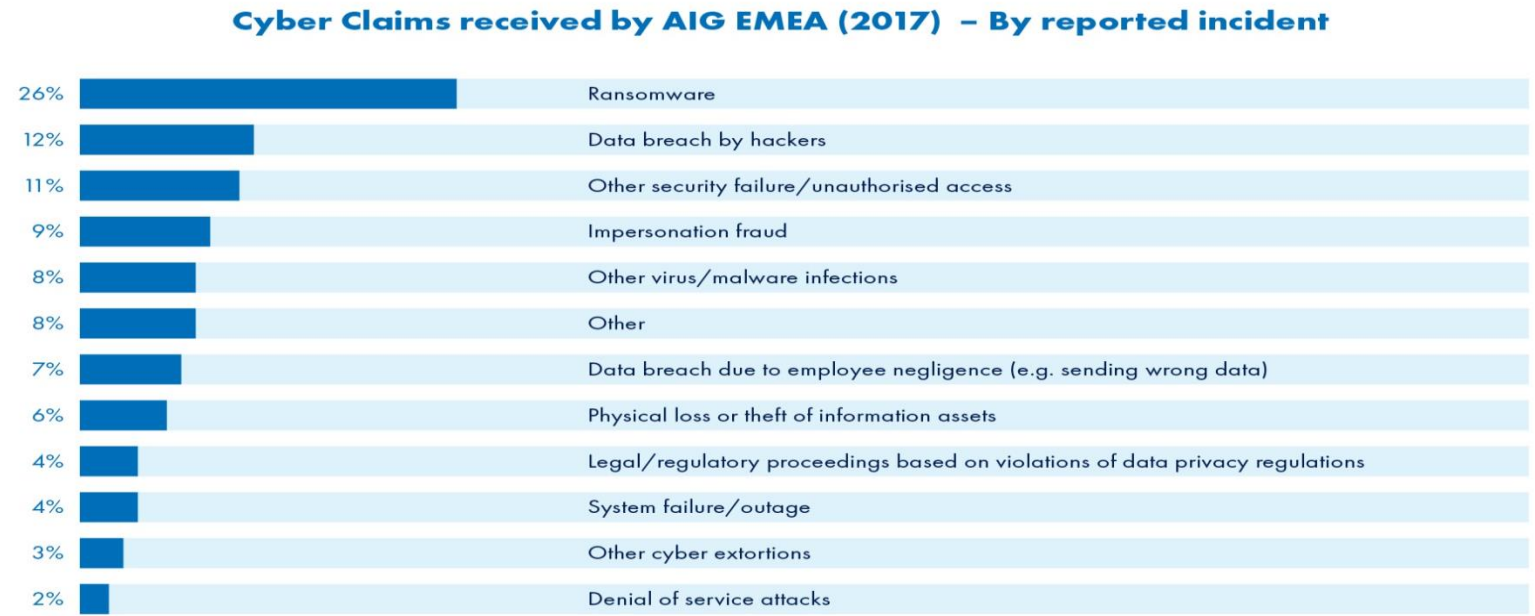
AIG

As many claims in 2017 as in the previous 4 years



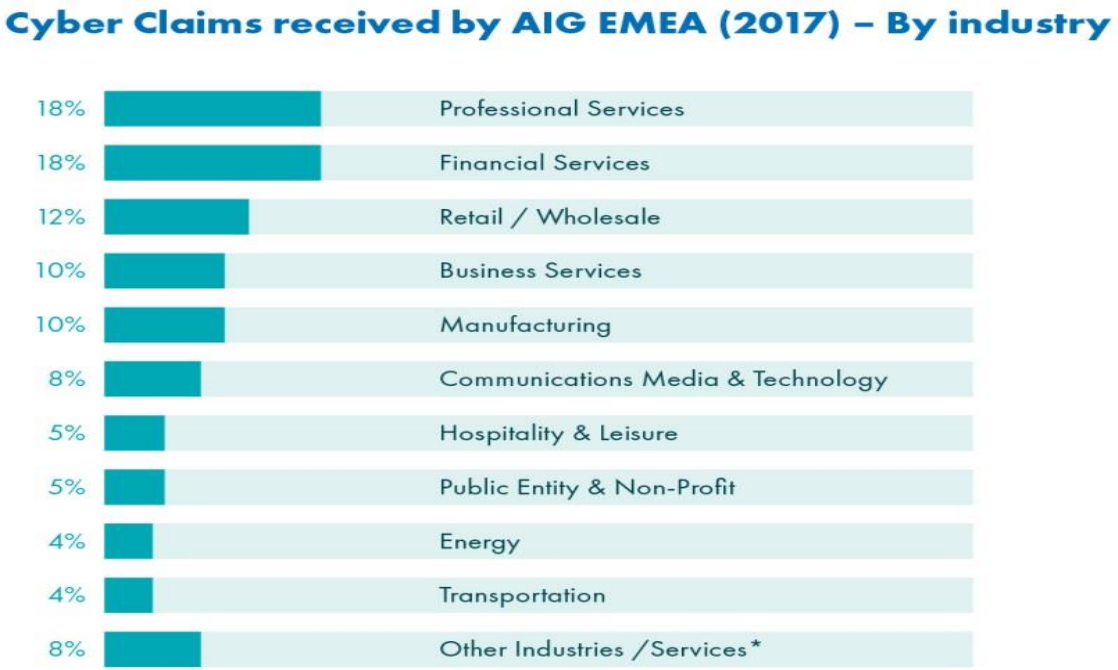
Source: AIG Cyber Claims Study 2018

Ransomware continues to be widespread



Source: AIG Cyber Claims Study 2018

Incidents are spreading across a wider range of industries



Source: AIG Cyber Claims Study 2018

Cyber Insurance in Action (1)

An insured manufacturer of cranes, excavators and lifting equipment experienced business interruption following a ransomware attack.

Its 300 production staff and engineers were unable to work on key projects, dependent on access to IT equipment.

The insured called the AIG CyberEdge hotline and received incident response services from an IT forensic firm.

The advice led to restoration of data from back-ups – and coverage was provided for extra cost of engineering staff to ensure continuity of operations and timely project completion.

Cyber Insurance in Action (2)

An insured financial institution received a threat of a DDoS attack from an established Latvian-based cybercrime group (although later intelligence suggested a copycat).

An email ransom demand was issued for 1 bitcoin – increasing to 10 – if not paid.

AIG provided assistance to the insured in engaging a DDoS protection service.

No threat materialised – website and digital platforms remained online and only losses were costs from legal and crisis management advice.

Incident response costs were paid by AIG.

Cyber Insurance in Action (3)

An insured luxury goods business appeared to fall victim to phishing, targeting employees and then clients (potentially using data obtained from the employees).

False links phished for log-in credentials, payment card details and other personal info.

Forensic IT specialists engaged on advice from AIG blocked access to the suspect url and investigated affected mailboxes to see what data was accessed.

Once determined, this allowed the insured to create a personalised response for affected clients (many of whom were high-net-worth, high-profile).

CyberMatics – Current Model Overview

Underwriters

Completes initial risk assessment in portal based on client manual and some automated input, for policy pricing determination.

Underwriting Portal

Utilizes developed Risk model for Risk score at underwriting.

Data Store

Central data repository for risk analysis

Flexible Technology

Pre-approved list of technology partners that AIG has vetted for CyberMatics.

If already have technology from the list, establish connections.
- OR -
Recommend and implement technology from partner list.

Cyber Risk Consulting

After the policy is bound, utilize portal client risk data to help client:

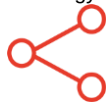
- Understand Risk Ratings
- Develop roadmap for risk improvement
- Coordinate and implement CyberMatics
- Reaches out to policy holders if risk score is trending down to offer assistance.

Cyber Policy Holder

Monitors risk score, takes action on risk improvement and alerts to reduce risk and receive cyber policy incentives.

Client Dashboard

Client access to scoring, risk score modeling, and improvement actions.
(Mobile App for C-level.)



Client IT Environment

Customer Name	Primary Industry	Annual Revenue	Revenue Tier	Peer Universe	Average Peer Residual Risk
Acme, Inc.	Retail Trade	$560,000,000	$500 million to $999 million	100 to 499 peers	Moderate (15.623)

Current Residual Risk Score

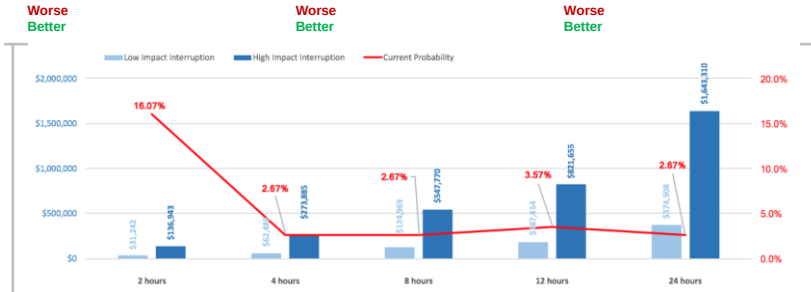
Moderate
19.861

View History

Absolute and Relative Risk Scores

View Analysis

Cyber Maturity	Threat Likelihood	Business Impact	Implicit Risk	Control Effectiveness	Residual Risk
Developing	Moderate	Very High	High	Minimal	Moderate
32.82% Relative Score	4.283 Relative Score	7.243 Relative Score	29.565 Relative Score	30.1 Relative Score	19.861 Relative Score



Worst-Case Values

Worst-Case Breach
$61,321,994

Worst-Case Interruption
$4,606,452

Top Risk Scenarios

1. DoS Attack: Server/Apps	Very High (56.312)
2. DoS Attack: Network	Very High (48,362
3. WebApp Attack: Server/Apps	High (28.494)
4. PoS Intrusion: End User Systems	High (21.384
5. PoS Intrustion: Terminal	Medium (20.963)

Most Risk Reducing Questions

1. DoS: DoS Mitigation	52.466
2. DoS: Incident Response	44.960
3. General: Employee Training	40.467
4. PoS: DLP Solution	37.073
5. PoS: Point-to-Point Encryption	29.090

Expected & Catastrophic Loss Values

Expected Loss (Low Estimate)
$199,510

Expected Loss (High Estimate)
$2,638,316

Catastrophic Loss Estimate
$61,321,994

Premium & Retention Analysis

Suggested Minimum Retention
$300,000

Suggested Threshold Retention
$750,000

Suggested Premium
$40,000

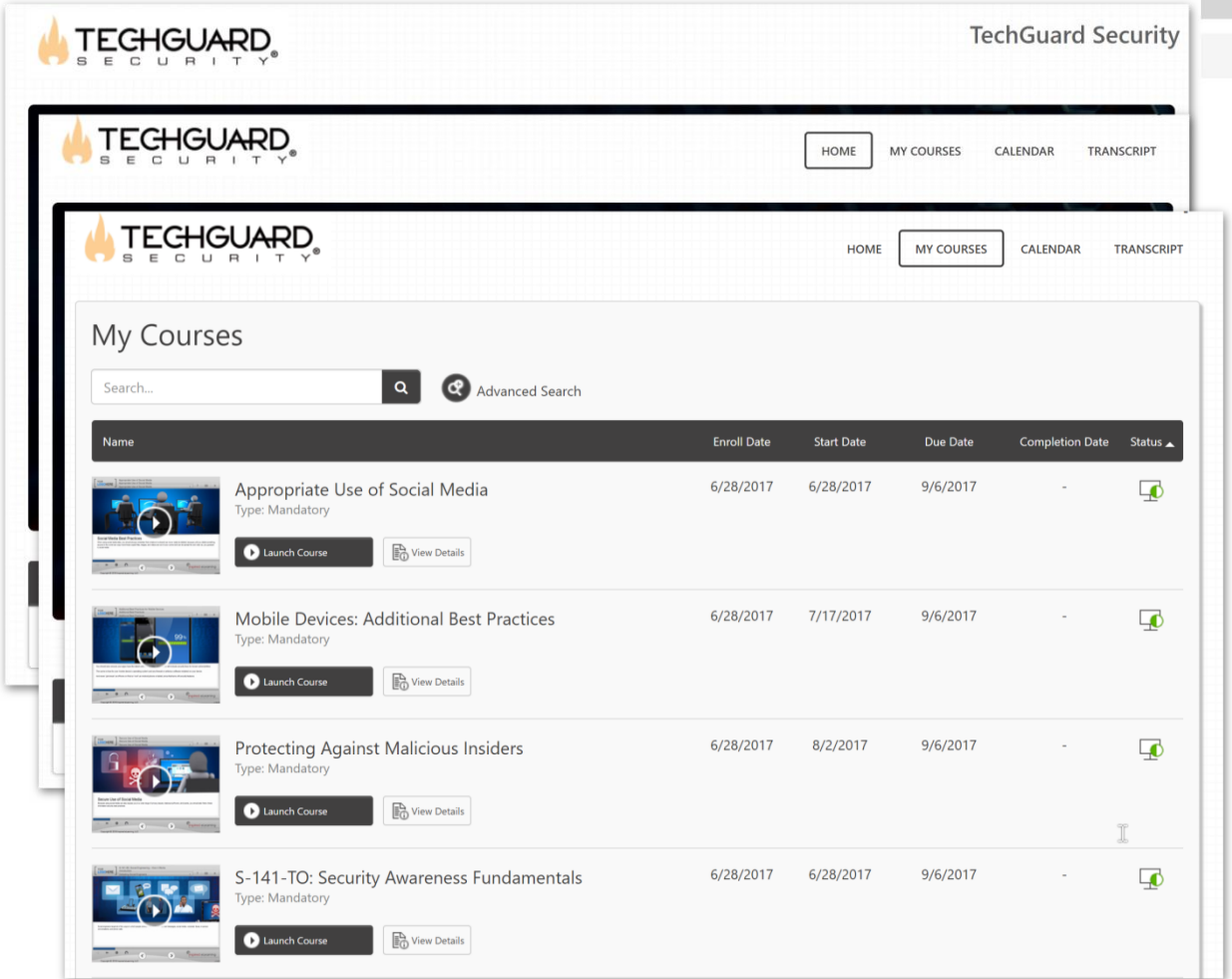
Bending The Risk Curve Down Through The Policy Life…

- Industry shifting focus from post-incident to pre-loss prevention services to help avoid a breach in the first place
- Examples of services being packaged with cyber insurance policies:
  - Vulnerability Scan
  - Employee Cyber Security eLearning
  - IP Blocking/Threat Intelligence
- Other services discounted and/or available with preferred terms
- All loss mitigation services are optional

AIG

eLearning

- 40 training modules
- 11 languages
- Interactive
- Track employee completion
- Helps to build defence/privacy by design



Conclusion

- Cyber coverage will continue to expand (and claims)
- More partnerships between insurance and technology companies
- Loss prevention services critical addition for end-to-end risk management solution

AIG

Questions?

Mark Camillo
Head of Cyber, EMEA
Mark.Camillo@AIG.com