

EMEA Update on Claims and Loss Prevention

Mark Camillo

Head of Cyber, EMEA

Mark.Camillo@AIG.com

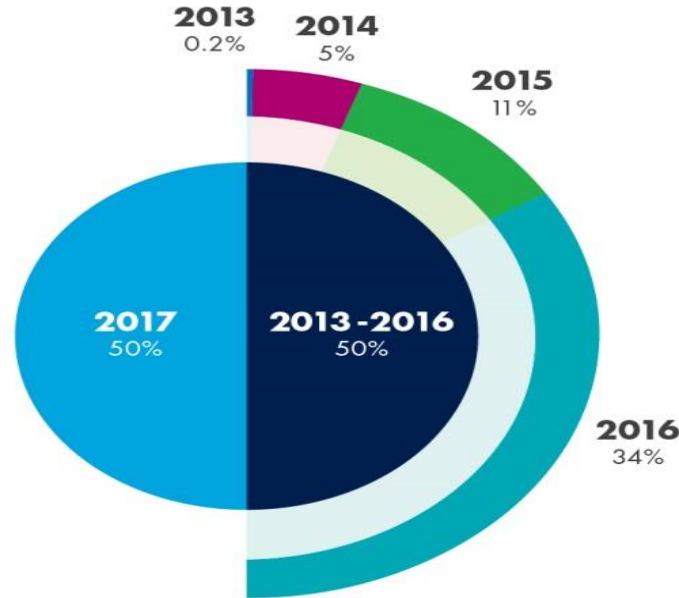


Introduction

- 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

As many claims in 2017 as in the previous 4 years

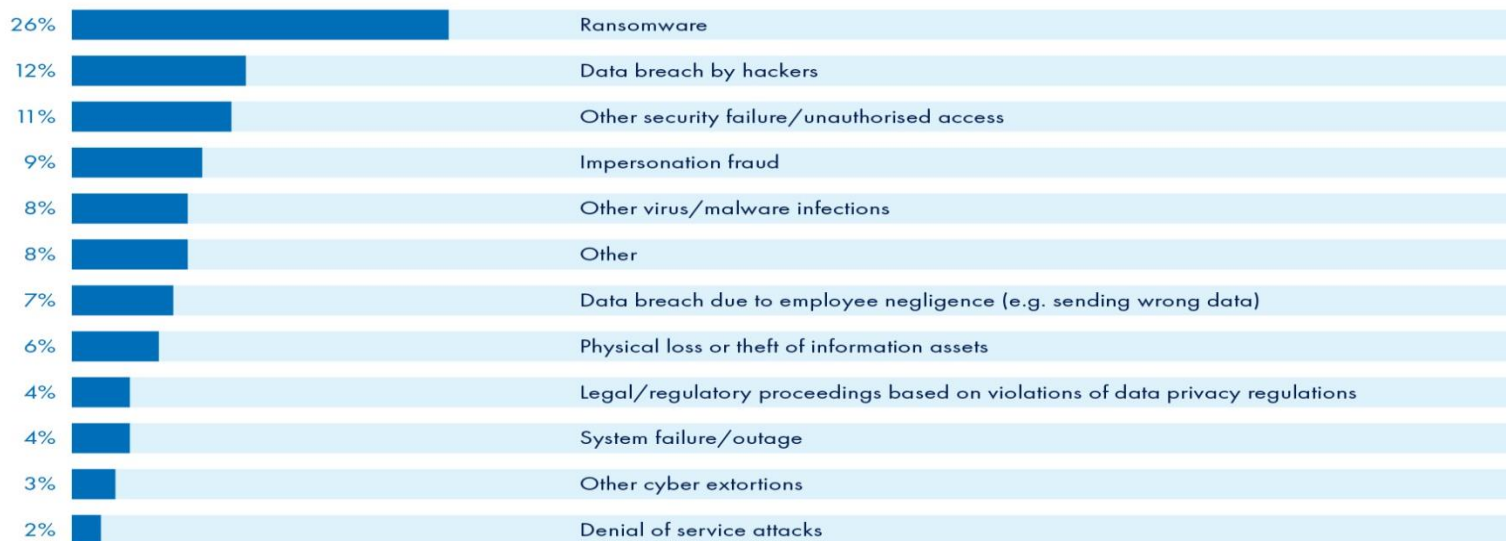
**Cyber Claims Received by AIG EMEA
(2013-2017) - Volume**



Source: AIG Cyber Claims Study 2018

Ransomware continues to be widespread

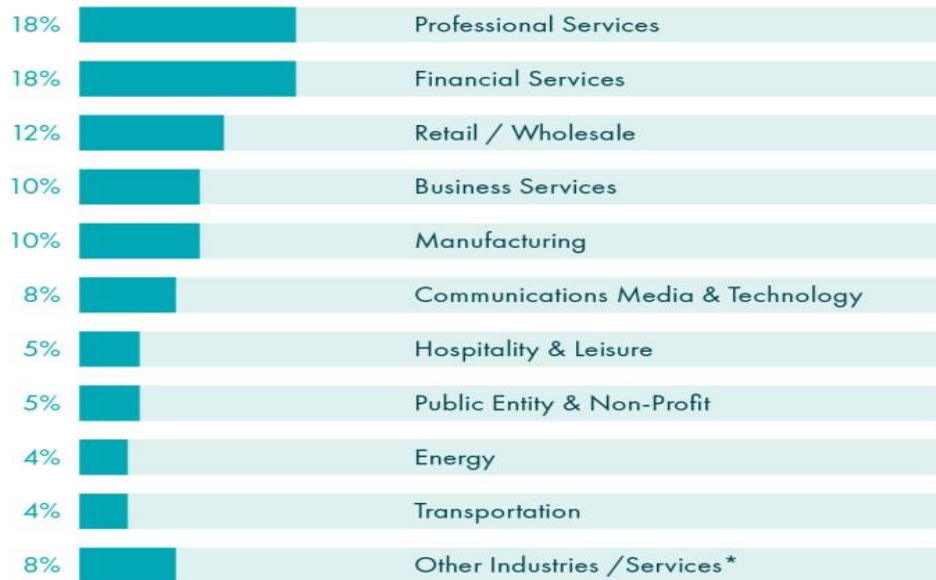
Cyber Claims received by AIG EMEA (2017) – By reported incident



Source: AIG Cyber Claims Study 2018

Incidents are spreading across a wider range of industries

Cyber Claims received by AIG EMEA (2017) – By industry



*Food & Beverage, Construction, Real Estate, Agriculture, Information Services

Note: Figures may not add up to 100% due to rounding

Source: AIG Cyber Claims Study 2018

Cyber Insurance in Action (1)



THE CLAIM

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.



AIG'S RESPONSE

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)



THE CLAIM

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'S RESPONSE

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)



THE CLAIM

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.



AIG'S RESPONSE

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.



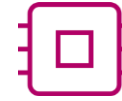
Underwriting Portal

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.



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

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

Customer Name Acme, Inc.		Primary Industry Retail Trade	Annual Revenue \$560,000,000	Revenue Tier \$500 million to \$999 million	Peer Universe 100 to 499 peers	Average Peer Residual Risk Moderate (15.623)																																																
Current Residual Risk Score Moderate 19.861 View History		<div>Absolute and Relative Risk Scores</div> <div><div><div>Cyber Maturity</div><div>Developing</div><div>32.82%</div><div>Relative Score</div></div><div><div>Threat Likelihood</div><div>Moderate</div><div>4.283</div><div>Relative Score</div></div><div><div>Business Impact</div><div>Very High</div><div>7.243</div><div>Relative Score</div></div><div><div>Implicit Risk</div><div>High</div><div>29.565</div><div>Relative Score</div></div><div><div>Control Effectiveness</div><div>Minimal</div><div>30.1</div><div>Relative Score</div></div><div><div>Residual Risk</div><div>Moderate</div><div>19.861</div><div>Relative Score</div></div></div> <div>View Analysis</div>																																																				
<table><caption>Breach Impact by Record Count</caption><tr><th>Record Count</th><th>Low Impact Breach</th><th>High Impact Breach</th><th>Current Probability</th></tr><tr><td>10k Records</td><td>\$34,320</td><td>\$365,403</td><td>51.52%</td></tr><tr><td>50k Records</td><td>\$79,310</td><td>\$659,347</td><td>11.35%</td></tr><tr><td>100k Records</td><td>\$91,561</td><td>\$756,307</td><td>2.60%</td></tr><tr><td>500k Records</td><td>\$110,076</td><td>\$1,617,228</td><td>1.42%</td></tr><tr><td>1M Records</td><td>\$141,826</td><td>\$1,806,439</td><td>1.10%</td></tr></table>		Record Count	Low Impact Breach	High Impact Breach	Current Probability	10k Records	\$34,320	\$365,403	51.52%	50k Records	\$79,310	\$659,347	11.35%	100k Records	\$91,561	\$756,307	2.60%	500k Records	\$110,076	\$1,617,228	1.42%	1M Records	\$141,826	\$1,806,439	1.10%	<table><caption>Interruption Impact by Duration</caption><tr><th>Duration</th><th>Low Impact Interruption</th><th>High Impact Interruption</th><th>Current Probability</th></tr><tr><td>2 hours</td><td>\$51,242</td><td>\$136,943</td><td>16.07%</td></tr><tr><td>4 hours</td><td>\$62,493</td><td>\$273,885</td><td>2.67%</td></tr><tr><td>8 hours</td><td>\$114,969</td><td>\$427,770</td><td>2.67%</td></tr><tr><td>12 hours</td><td>\$172,115</td><td>\$621,655</td><td>3.57%</td></tr><tr><td>24 hours</td><td>\$374,308</td><td>\$1,448,310</td><td>2.67%</td></tr></table>					Duration	Low Impact Interruption	High Impact Interruption	Current Probability	2 hours	\$51,242	\$136,943	16.07%	4 hours	\$62,493	\$273,885	2.67%	8 hours	\$114,969	\$427,770	2.67%	12 hours	\$172,115	\$621,655	3.57%	24 hours	\$374,308	\$1,448,310	2.67%
Record Count	Low Impact Breach	High Impact Breach	Current Probability																																																			
10k Records	\$34,320	\$365,403	51.52%																																																			
50k Records	\$79,310	\$659,347	11.35%																																																			
100k Records	\$91,561	\$756,307	2.60%																																																			
500k Records	\$110,076	\$1,617,228	1.42%																																																			
1M Records	\$141,826	\$1,806,439	1.10%																																																			
Duration	Low Impact Interruption	High Impact Interruption	Current Probability																																																			
2 hours	\$51,242	\$136,943	16.07%																																																			
4 hours	\$62,493	\$273,885	2.67%																																																			
8 hours	\$114,969	\$427,770	2.67%																																																			
12 hours	\$172,115	\$621,655	3.57%																																																			
24 hours	\$374,308	\$1,448,310	2.67%																																																			
Top Risk Scenarios		Most Risk Reducing Questions		Expected & Catastrophic Loss Values		Premium & Retention Analysis																																																
1. DoS Attack: Server/Apps		1. DoS: DoS Mitigation		Expected Loss (Low Estimate)		Suggested Minimum Retention																																																
Very High (56.312)		52.466		\$199,510		\$300,000																																																
2. DoS Attack: Network		2. DoS: Incident Response		Expected Loss (High Estimate)		Suggested Threshold Retention																																																
Very High (48,362)		44.960		\$2,638,316		\$750,000																																																
3. WebApp Attack: Server/Apps		3. General: Employee Training		Catastrophic Loss Estimate		Suggested Premium																																																
High (28.494)		40.467		\$61,321,994		\$40,000																																																
4. PoS Intrusion: End User Systems		4. PoS: DLP Solution																																																				
High (21.384)		37.073																																																				
5. PoS Intrusion: Terminal		5. PoS: Point-to-Point Encryption																																																				
Medium (20.963)		29.090																																																				









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

eLearning

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

The screenshot displays the TechGuard Security eLearning platform. The top navigation bar includes the TechGuard Security logo and the text 'TechGuard Security'. Below this, a secondary navigation bar contains links for 'HOME', 'MY COURSES', 'CALENDAR', and 'TRANSCRIPT'. The main content area is titled 'My Courses' and features a search bar with a magnifying glass icon and a link to 'Advanced Search'. A table lists four mandatory courses, each with a video thumbnail, a 'Launch Course' button, a 'View Details' button, and a progress indicator. The table columns are: Name, Enroll Date, Start Date, Due Date, Completion Date, and Status.

Name	Enroll Date	Start Date	Due Date	Completion Date	Status
 Appropriate Use of Social Media Type: Mandatory	6/28/2017	6/28/2017	9/6/2017	-	
 Mobile Devices: Additional Best Practices Type: Mandatory	6/28/2017	7/17/2017	9/6/2017	-	
 Protecting Against Malicious Insiders Type: Mandatory	6/28/2017	8/2/2017	9/6/2017	-	
 S-141-TO: Security Awareness Fundamentals Type: Mandatory	6/28/2017	6/28/2017	9/6/2017	-	

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

Questions?

Mark Camillo

Head of Cyber, EMEA

Mark.Camillo@AIG.com

