6th Information Security Conference

Ασφάλεια για την Ασφάλεια

A. Security for Insurance

B. Insurance for Security

ΕΘΝΙΚΗ
Η ΠΡΩΤΗ ΑΣΦΑΛΙΣΤΙΚΗ

Γιώργος Τσινός

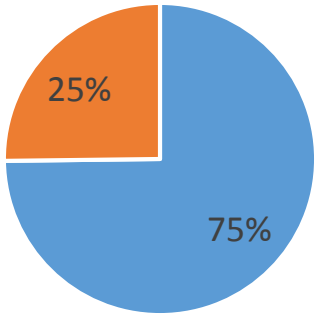
Υπεύθυνος Ασφάλειας Πληροφορίας (CISO)

14/02/2019

“The Ethniki” Hellenic General Insurance Co. SA

- **128 years** of uninterrupted operation in Greece
- **Leads the domestic Insurance Sector**, with the largest market share, 14.94% (31/12/2017).
- In the first nine months of 2018, **“The Ethniki” Hellenic General Insurance Co. SA** Group posted earnings, before taxes, of **€ 50.1 million**, while gross written premiums (including contractual rights) amounted to **€ 444.6 million** for Life and Non-Life (Cars, Fire etc.).

Life **332,6 εκατ. €**



Non-Life **112 εκατ. €**

- Under the new **Solvency II** supervisory framework, the solvency **Capital Requirement** is set at 31/12/2017 at **200%** at Group level.

Ασφάλεια για την Ασφάλεια… means PREVENTION

A. Security for Insurance → Prevention

B. Insurance for Security → Prevention

«κάλλιον το προλαμβάνειν ή το θεραπεύειν»*
Ιπποκράτης

«των φρονίμων τα παιδιά πριν πεινάσουν μαγειρεύουν»
Λαϊκή σοφία

«An ounce of prevention is worth a pound of cure»
Benjamin Franklin

* *It's better to prevent than to cure.*
Hippocrates of Kos (460 - 377 BC)

Security Awareness

«Sell» the security

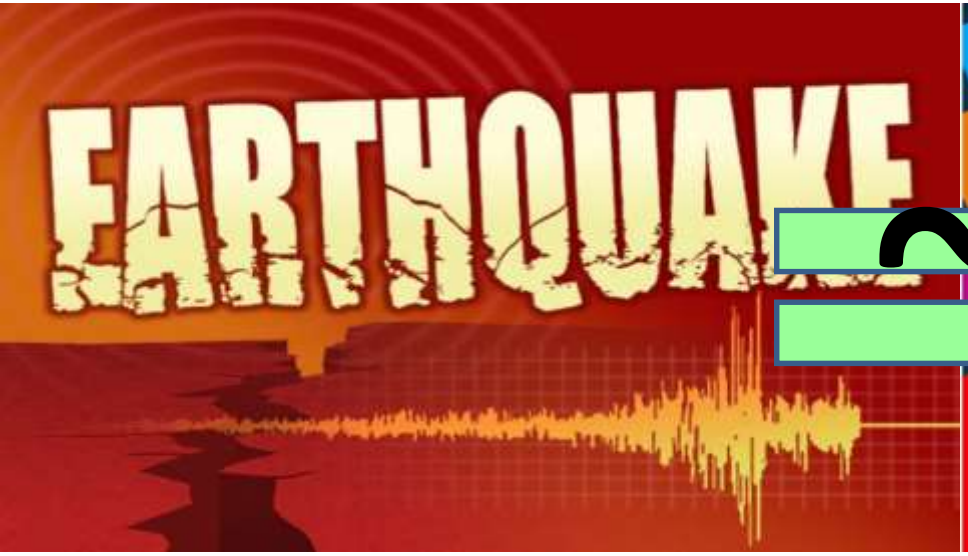
What do you want:

- You want the information security chain to be strong.
- You want the human link to be your strong and faithful ally in cyberwar, through understanding rather than coercion (the carrot is more efficient than whip!).
- You want every employee to be your reliable “antenna” that will react properly and will recognize the danger in time (neither with terror, nor with apathy).

What to do:

- Use simple and understandable scenarios to "sell" security to your company.
- Scenarios should spur the worker's mood for their adoption, since they will help him / her in his / her everyday life, work / personal / family.

1st Scenario. Earthquake vs Data Breach



≈

There is no 100% protection	There is no 100% protection
The better you are prepared, the less the impact. Holistic approach (Procedures-People-Technology).	The better you are prepared, the less the impact. Holistic approach (Procedures-People-Technology).
It is not if, but when. The sooner the reactions, the smaller the losses.	It is not if, but when. The sooner the reactions, the smaller the losses.

2nd Scenario. Fire/Liability Insurance vs Cyber-crime protection (In Greek, ready for use!)

Ασφάλεια Κατοικίας / Αστική Ευθύνη 	Προστασία από το Κυβερνοέγκλημα 
Έχεις πόρτα ασφαλείας με σύγχρονο κλειδί ασφαλείας που είναι αποκλειστικά για δική σου χρήση;	Έχεις κωδικό ασφάλειας (password) με αυξημένη πολυπλοκότητα που δεν το γνωρίζουν άλλοι; Τον αλλάζεις περιοδικά;
Βλέπεις στη θυροτηλεόραση και ελέγχεις αν θα ανοίξεις την πόρτα; Ρωτάς στο κουδούνι;	Βλέπεις τα αναδυόμενα παράθυρα ενώ βρίσκεσαι στο Διαδίκτυο (πχ τεστ ευφυίας) και πατάς πάνω τους να ανοίξουν; Ανοίγεις emails από άγνωστους λογαριασμούς και ακολουθείς τους συνδέσμους που προτείνουν (phishing);
Προστατεύεις / ασφαλίζεις τα αντικείμενα αξίας ξεχωριστά από τα υπόλοιπα αντικείμενα του σπιτιού, σε χώρο αυξημένης ασφάλειας;	Προστατεύεις τη διαβαθμισμένη πληροφορία του υπολογιστή σου; (πχ κρυπτογράφηση, επιπλέον κωδικός πρόσβασης σε δεδομένα καρτών / passwords / ιατρικά / οικονομικά κλπ. με χρήση ειδικής εφαρμογής;)
Φοράς τα ακριβά σου κοσμήματα και βγαίνεις απροστάτευτος από το σπίτι για νυχτερινή βόλτα με τα πόδια σε κακόφημους δρόμους;	Μπαίνεις σε «περίεργα sites» και χωρίς προστασία (antivirus); Μπαίνεις στο Διαδίκτυο από δημόσια WiFi (συνήθως χωρίς κωδικό ασφάλειας που μπορούν να βλέπουν ό,τι κάνεις, όπως τους κωδικούς ασφαλείας που γράφεις);
Αφήνεις όλα τα παράθυρα ανοιχτά, αν δε θέλεις να σε δει κάποιος άγνωστος;	Έχεις «κλείσει» την κάμερα του laptop σου με κάτι αδιαφανές (πχ μονωτική ταινία), ώστε σε περίπτωση μόλυνσης από ιό να μην μπορεί κάποιος να σε βλέπει;
Έχεις εφαρμόσει μέτρα αποτροπής επίδοξων κλεφτών (πχ συναγερμό / σκύλο);	Εγκαθιστάς τις τελευταίες εκδόσεις του λογισμικού που επιλύουν θέματα ασφάλειας (πχ. Microsoft security patches), ενημερώνεις το πρόγραμμα κατά των ιών (antivirus), έχεις ενεργοποιημένο το τείχος προστασίας (firewall);
Βρίσκεις κάποιο αντικείμενο μικρής αξίας στο δρόμο / σκουπίδια. Το συλλέγεις, το παίρνεις σπίτι σου και το βάζεις πάνω στο τραπέζι της κουζίνας, αδιαφορώντας από βρωμιές / μολύνσεις;	Βρίσκεις ένα USB stick (συσκευή μεταφοράς δεδομένων). Το παίρνεις και το συνδέεις στον υπολογιστή σου, αδιαφορώντας αν έχει κάποιο κακόβουλο λογισμικό;
Νοιώθεις έντονη μυρωδιά καπνού. Δεν εξετάζεις από πού προέρχεται; Αν επιβεβαιώσεις τον κίνδυνο (πχ φωτιά), δεν ενημερώνεις άμεσα την Πυροσβεστική Υπηρεσία;	Υποψιάζεσαι μόλυνση από κακόβουλο λογισμικό, παραβίαση δεδομένων, προσπάθεια υποκλοπής κωδικών κλπ. Δεν αναφέρεις άμεσα το περιστατικό στο CISO@insurance.nbg.gr ή στο Aeega-helpdesk@insurance.nbg.gr (Τηλ. 29300);
Έχεις συμβόλαιο ασφάλειας κατοικίας;	Έχεις αντίγραφα ασφαλείας δεδομένων (backup) για να επαναφέρεις κάτι που θα χαθεί / μολυνθεί; Έχεις ασφάλεια κυβεροεγκλήματος (κυρίως για επιχειρήσεις / επαγγελματίες);

Cyber Insurance

Risk Treatment Option: Sharing (…is caring!). Transfer risk when Impact >> and Probability <<

- Quantitative risks are shared through insurances, so that by means of fee, the policyholder reduces the impact of potential threats and the insurer accepts the consequences.
- Clauses in Insurance products specify the degree of responsibility of each part.
- [Note: Liability is not transferred].

Magerit Risk Assessment methodology: PILAR

Scenario: Cyber extortion, business interruption and privacy breach on a Telecom Organization

The CEO of a telecom organization receives an email demanding a ransom of €500,000 in bitcoins within 24 hours, or else anonymous hackers will release sensitive customer information (a sample of which is provided in the email) and shut down critical business systems.

The CISO **hires a third-party forensic firm**, which determines that the threat is real and that more than 500,000 sensitive customer records have been accessed.

The organization **notifies law enforcement**, but before it can make a decision regarding the ransom, the ***hackers release half of the records obtained***. They have also managed to ***make some critical networks inaccessible***, so clients/employees are not able to access critical systems or process orders.

The organization **hires legal counsel** to assist with notifications to individuals impacted by the breach. Another **vendor is hired to handle the public relations** response.

The critical systems remain down for ten days, impacting customer orders and general operations. The organization ***suffers loss of income and incurs significant expenses*** related to the outage and to restore the business to operation. Two weeks after the breach notice was issued, ***a class action suit is filed alleging failure to properly protect private information.***

Preparing for cyber insurance (Insurance Europe, Ferma, bipar, Aon, March)

Outcome

As the CISO may reasonably suspect a breach of the system given the anomalies discovered, the organization may proactively:

- **Pay for a forensic firm to end the threat and secure the systems**.
- Additional **forensic costs may be incurred to determine exactly what information was accessed** by the hacker.

Further costs may include:

- **Breach coach** to assist with notices to affected individuals and to help the organization determine what obligations it has and which laws (potentially in various jurisdictions) it will need to comply with.
- **Credit monitoring and possibly call center** costs to respond to enquiries from concerned clients.
- **Crisis management/public relations** team to help develop and execute a media strategy and control the public narrative relating to the breach.
- **Defense costs and possibly damages as a result of the class action lawsuit**; more lawsuits may also follow.
- **Coverage of the loss of revenue**.

Preparing for cyber insurance (Insurance Europe, Ferma, bipar, Aon, March)

Interplay between cyber insurance policies and other lines of insurance

A cyber insurance policy in this scenario could potentially cover **costs incurred to maintain or return the business to operational; loss of revenue and costs incurred to recreate/restore data and information.**

A cyber insurance policy could potentially also cover **legal costs and damages from claims alleging privacy breach or network security failure**. The telecom organization may benefit from the **assistance of forensic investigation specialists, legal services, credit monitoring, call center services, crisis management and public relations services** offered in a cyber insurance policy.

Other insurance policies may **respond to** elements of this type of **incident**, for example, a professional indemnity policy might **cover the costs incurred to defend/settle claims** against the organization and due to **the lack of access to the system that causes clients financial harm**.

A professional indemnity policy might cover the costs to **mitigate the breach**, such as **credit monitoring, public relations and a breach coach**, if coverage includes loss mitigation.

Preparing for cyber insurance (Insurance Europe, Ferma, bipar, Aon, March)

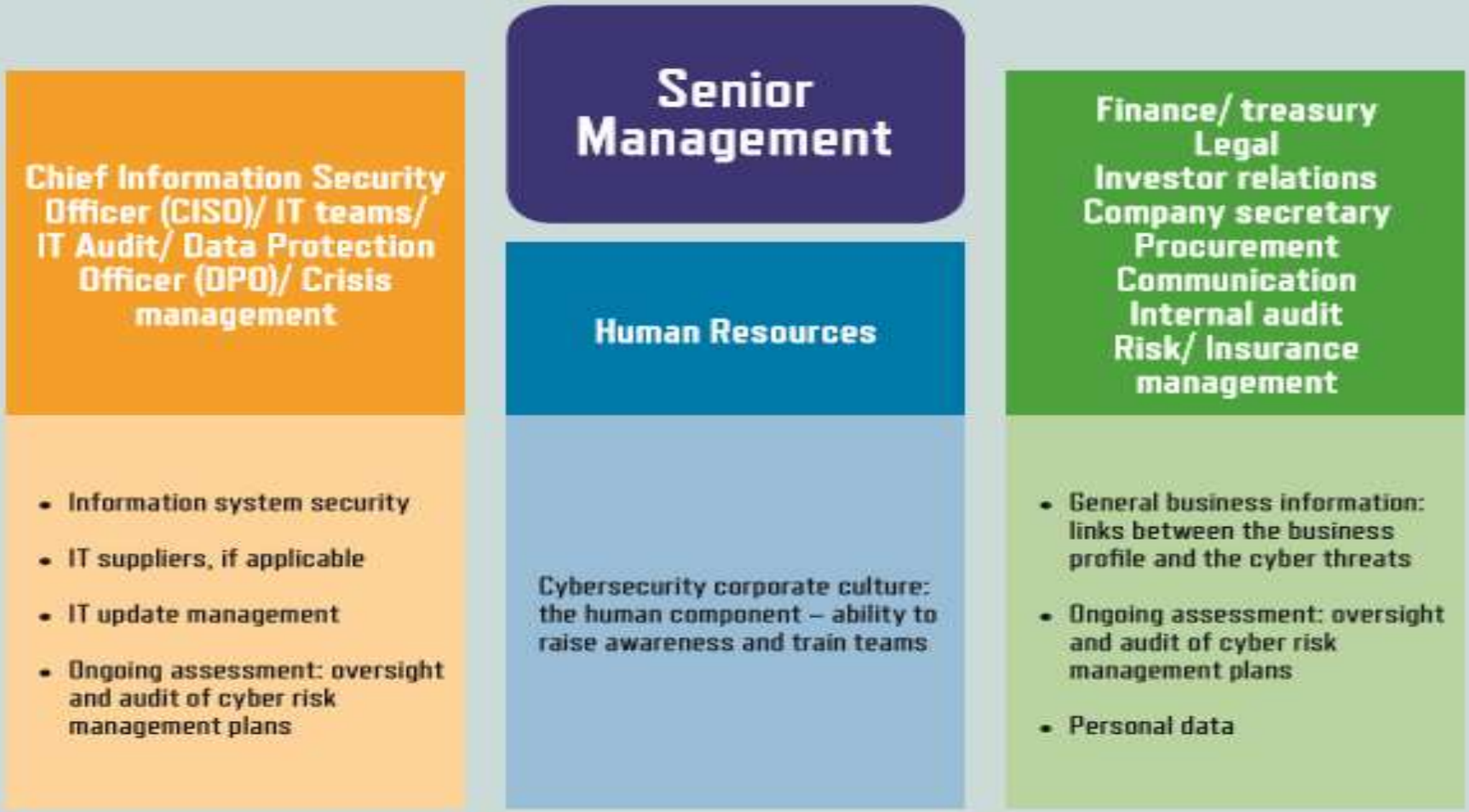
Coverage considerations of this scenario in the various cyber insurance offers

With respect to indemnity under different cyber insurance policies, it is important to understand that some policies **require the insured organization to receive express, written permission from the insurer**, before incurring any costs in relation to managing/mitigating a breach. Otherwise, the insurer has the right to decline payment for costs incurred before it gave its consent.

The CISO or technical team and the risk management team should, therefore, **coordinate actions**. **Understanding the requirements of the insurance policy is critical**. Mitigating actions by the technical team in particular — however well intended — could impact the organization's ability to recover financial loss through insurance.

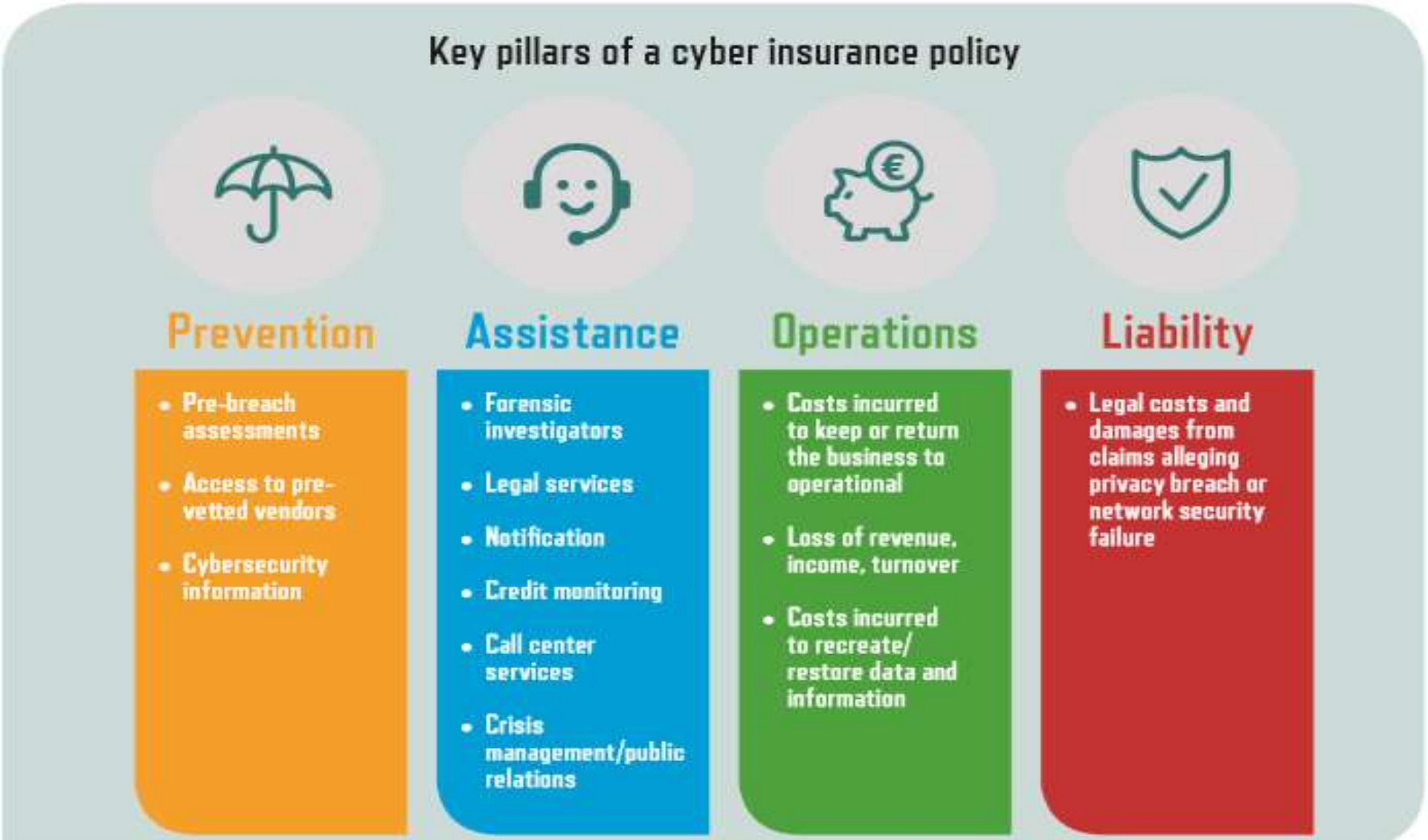
Preparing for cyber insurance (Insurance Europe, Ferma, bipar, Aon, March)

Preparing Cyber Underwriting Information



Preparing for cyber insurance (Insurance Europe, Ferma, bipar, Aon, March)

Understanding Cyber Insurance Offers



Preparing for cyber insurance (Insurance Europe, Ferma, bipar, Aon, March)

Cyber Coverage Components

Possible actions following a cyber attack or data loss	Examples of cyber coverage components
Investigate what happened	These issues likely require the specialised assistance of forensic investigators. Cyber policies may include coverage for forensic investigation costs following a cyber-attack or data loss.
Deploy technical measures to contain the loss and repair the IT system	
Assess legal/regulatory obligations	Legal services/assistance can be covered by cyber policies for breaches where it is reasonably suspected that confidential information has been compromised, generally in two forms: (i) post incident discovery and assistance in managing a breach (ii) defence costs following a claim alleging a breach of information
Execute a plan to comply with your obligations	
Assess the complaints/legal challenges you receive	
Implement the emergency plan to continue servicing clients	Cyber policies may include coverage for costs incurred as a result of a cybersecurity breach to maintain or restore operations and for income that is lost during the outage period.
Assess the cost of the cyber-attack, including possible loss of turnover	
If you are facing extortion: - Hire a response/threat consultant - Pay ransom, if legally allowed	Cyber policies may include services and costs to investigate and manage an extortion threat, including forensic experts and threat consultants.
If you are facing a regulatory investigation or a legal suit from third parties: - Hire legal advisers; prepare defence strategy - Pay damages	Cyber policies may include coverage for defence costs and damages that are agreed and/or assessed.

Preparing for cyber insurance (Insurance Europe, Ferma, bipar, Aon, March)

“The Ethniki” Approach

“The Ethniki” is using “tailor made” approach solutions on Cyber Insurance products. It combines third-party liability coverage and first party losses. More specifically:

- Liability arising out of design errors and omissions
- Liability arising out of negligence and / or dishonest employees
- Liability and costs of data and security systems breaches
- Liability out of copyright infringement and property violations
- Damage caused to third parties’ reputation
- Damage caused to third parties’ information systems
- Damage caused due to third parties’ business interruption
- Data recovery costs
- Public relations and restoration of the company's reputation
- Provision of technical and advisory services
- Crisis Management and Loss Management Costs
- Expenses related to system unavailability, theft of electronic data, ransom payment in case of threats & extortion and electronic damages

End note

Prevent a loss you can't afford tomorrow,

with a wise move you can do today!