Η Διαδικτυακή Ασφάλεια στη Πράξη

Κώστας Βούλγαρης

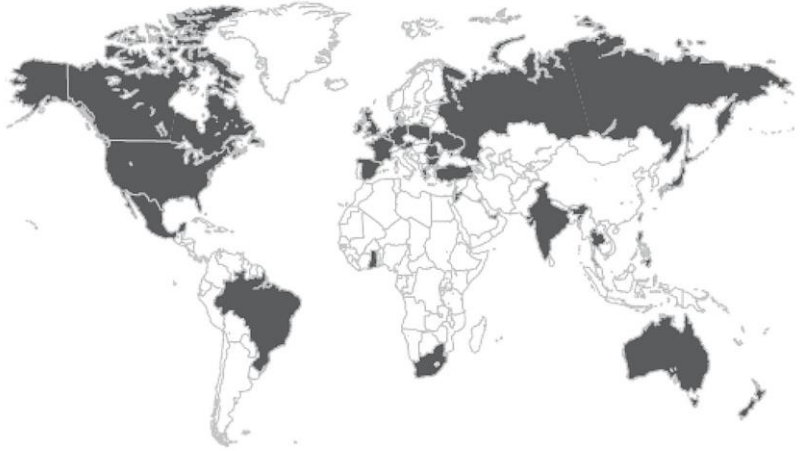
Το CyberEdge δεν είναι απλά ένα ασφαλιστικό προϊόν είναι, ένα εργαλείο **Risk Management,** παρέχοντας όχι μόνο αποζημιώσεις, αλλά κυρίως υπηρεσίες **αντιμετώπισης κρίσης!**

AIG

European & International Exposure

- 1995 EU Data Protection Directive
- Mandatory Notification
  - ENISA & NIS
- Existing Safe Harbor Laws
- New EU Legislation
- ICO
- Emerging Global Legislation
  - Consumer Protection
  - Global Economic Requirements

Figure 7. Countries represented in combined caseload



Countries in which a breach was confirmed

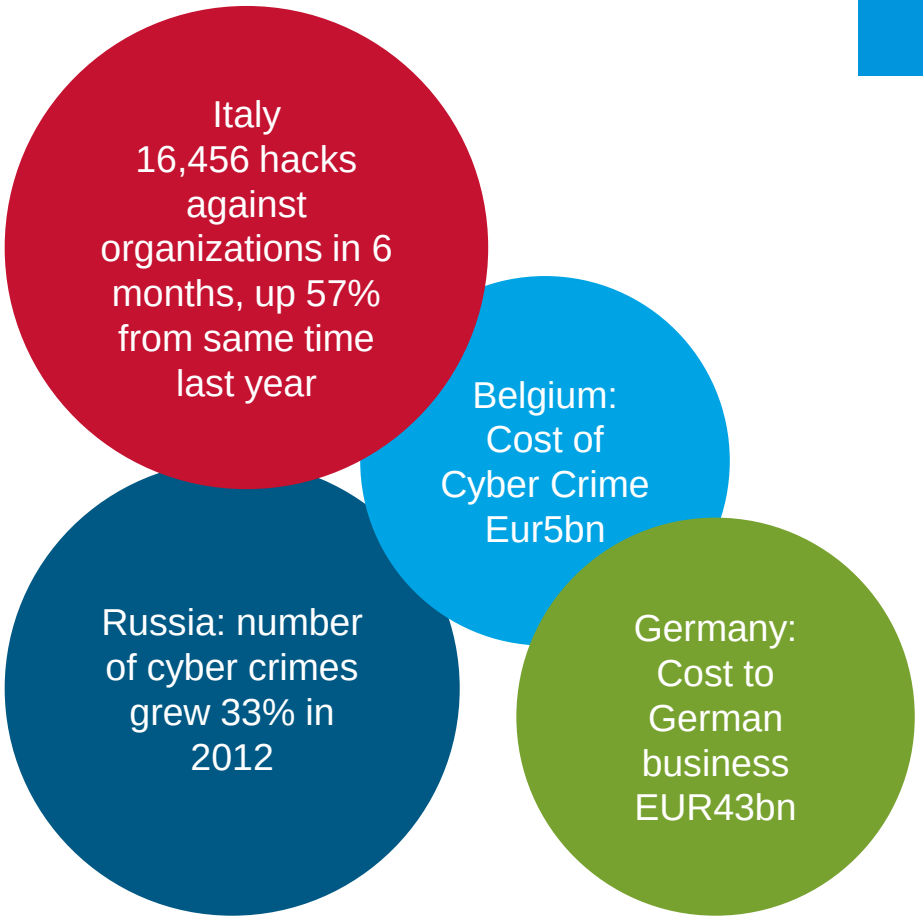
Australia	France	Jordan	Poland	United Arab Emirates
Austria	Germany	Kuwait	Romania	Ukraine
Bahamas	Ghana	Lebanon	Russian Federation	United Kingdom
Belgium	Greece	Luxembourg	South Africa	United States
Brazil	India	Mexico	Spain	
Bulgaria	Ireland	Netherlands	Taiwan	
Canada	Israel	New Zealand	Thailand	
Denmark	Japan	Philippines	Turkey	

AIG

Country Exposure

UK: Cost of Cyber Crime is £27bn

- Cost to UK Business estimated £21bn
- Average cost of resolving a data breach is £2.04m
- Ireland: 37 breaches in 2012 with 68 over last 3 years
- Scotland: total cost of cyber Crime is £5bn every min lose £158



AIG

Business Enterprise Risk

Employees can't access systems
- Assume the cost of labour associated with average downtime over $45m
- Down for an extended period

Consumers can't access your product
- Loss in Net sales
- Infrastructure
- Breach of service agreements

You disrupt a 3rd party's supply chain
- Inability for upstream production or delivery
- Legal Penalties for breach of contractual obligations

Unexpected costs
- Business continuation costs
- Critical computer components damaged
- Re-uploading and patching of system critical software
- Replacing lost or destroyed data sets

Reputation Damage
- Cost to your Brand
- Consumer churn
- Loss of contracts or other business opportunities
- Business lost to competitors
- Coupons and discounts

Stock drops
- Average stock drop related to a cyber event 5%

Investigations
- Own internal
- Regulatory
- Shareholder Discovery

AIG

The Cyber Landscape

Increase in uptake for cyber

Perception of cyber risks continues to grow

- 98 percent believe cyber risks pose at least a moderate threat, up 12 percentage points from 2013
- 76 percent believe cyber risks pose a serious or extremely serious threat, up 19 points from 2013

Cyber risks are increasingly viewed as a threat by senior executives and board members

- 76 percent say board members view cyber risks as a significant threat, up 23 points from 2013
- 83 percent say senior executives view them as a significant threat, up 12 points from 2013

Net Diligence study 2013

AIG

The Cyber Landscape

Cyber threats are no longer only perceived as a large company problem

- A higher percentage of SMEs believe cyber threats pose a serious threat to their organisation and nearly all now make network security a specific risk management focus. But most fail to take a multi-departmental approach to managing the risk.

- SMEs increasingly are concerned with their exposures from mobile devices and employee use of personal devices and despite the concerns around privacy, cloud computing is gaining in popularity among businesses of all sizes.

- Although cyber risks are perceived as a moderate threat by nearly all organisations cyber insurance is still not purchased by most but is trending in an upward direction.

Advisen study 2013

AIG

Claims Examples

Case studies from AIG

AIG

Claims Examples

Hacker

- Insured provides medical and travel assistance in 70 countries
- Works with governments, business, NGOs
- Over 5 day period, insured’s systems compromised
- Insured was advised by external security firm monitoring hackers’ websites
- Legacy system was a weakness in insured's network
- A month later, another breach
- Hacktivist arrested by FBI
- Total costs expected to be in the region of USD 2 million

AIG

Claims Examples

Rogue Employee

- Insured is multinational bank
- Senior Financial Analyst at insured's subprime lending division downloaded over 2 million records
- Sold 20,000 customer profiles each week for $500 each
- Notification required to over 10 million people
- 42 class actions
- Total loss to insured USD 40m
- Policy responded to cover USD 20m

AIG

Claims examples

Hacker

- Large US retailer
- December 2013 breach
- Insured found out from Secret Service
- Malware discovered on 43,745 point of sale terminals
- Over 20 day period, malware exposed credit and debit card info of 40m customers
- Subsequent discovery that hackers accessed customer info database, accessing personal information for an additional 70 million customers

AIG

Anatomy of a Cyber Claim

What happens and when

Anatomy of a Cyber Claim

Before

- Recognize data is at risk and have a plan in place.

After

- First need to know you had or have a breach.
- Report of lost laptop (because Human Error is an element in 75%+ of breaches)
- Log files show unauthorized access – OR
- As is the case with 86% of breaches it is discovered/reported by a third party

The 'Real' After

Companies fall into three groups:

- Overreact and make public statements without facts
- Underreact and wait days/weeks to act
- Those with a plan.

AIG

Anatomy of a Cyber Claim

Phase 1: 0 - 24 Hours

- Notification to AIG (and claims adjuster)
- Lawyers and forensic respond within 1 hour
- Assess the incident and advise
- Maintain privilege in communications
- Crisis management
- Analysis of breach, including scope of breach
- Identify geographical location of data and subjects

AIG

Anatomy of a Cyber Claim

Phase 2: 24 – 48 Hours

- Evaluation of exposure and action plan
- Recommendations on notification to data subjects
- Regulatory advice
- Continue breach analysis/advice
- Appointment of PR/event management consultants
- Cyber extortion

Anatomy of a Cyber Claim

Phase 3: 48 to 72 Hours

- Detailed consideration of notification requirements
- Various and potentially numerous notification and regulatory obligations
- Continued PR /forensic/extortion response as appropriate
- Advice on monitoring threats and maintaining security
- Credit monitoring/ID theft protection to be considered

AIG

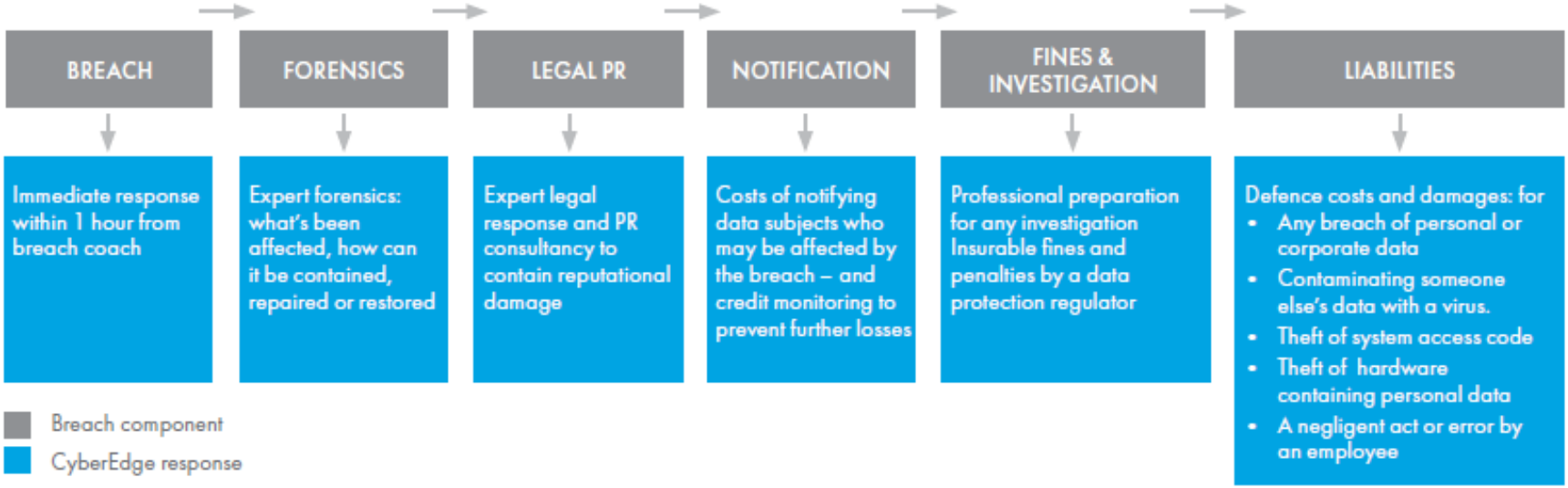
Anatomy of a Cyber Claim

Phase 4: 72+ Hours

- Valuation of initial costs/losses
- Ongoing notification/regulatory communications
- Management of third party relationships
- Liaison with law enforcement bodies
- Identification of longer term issues
- Remediation/mitigation steps
- Business interruption claim

AIG

Summary of a breach anatomy and CyberEdge response



AIG

CyberEdge Risk Management Solution

- From our innovative loss prevention tools to educate and potentially prevent a breach, to the services of our CyberEdge Breach Resolution Team if a breach does occur, insureds receive responsive guidance every step of the way.

Risk Consultation and Prevention

- The protection that CyberEdge provides is a valuable additional layer to the most powerful
- first line of defense against cyber threats, a company's own IT system. Constantly monitoring
- the cyber landscape, we keep insureds at the forefront of the industry as cyber risks continue
- to evolve. Our preventative tools provide our clients with the knowledge, training, security,
- and consultative solutions to help them stay ahead of the curve.

AIG

www.aig.com/CyberEdge

AIG