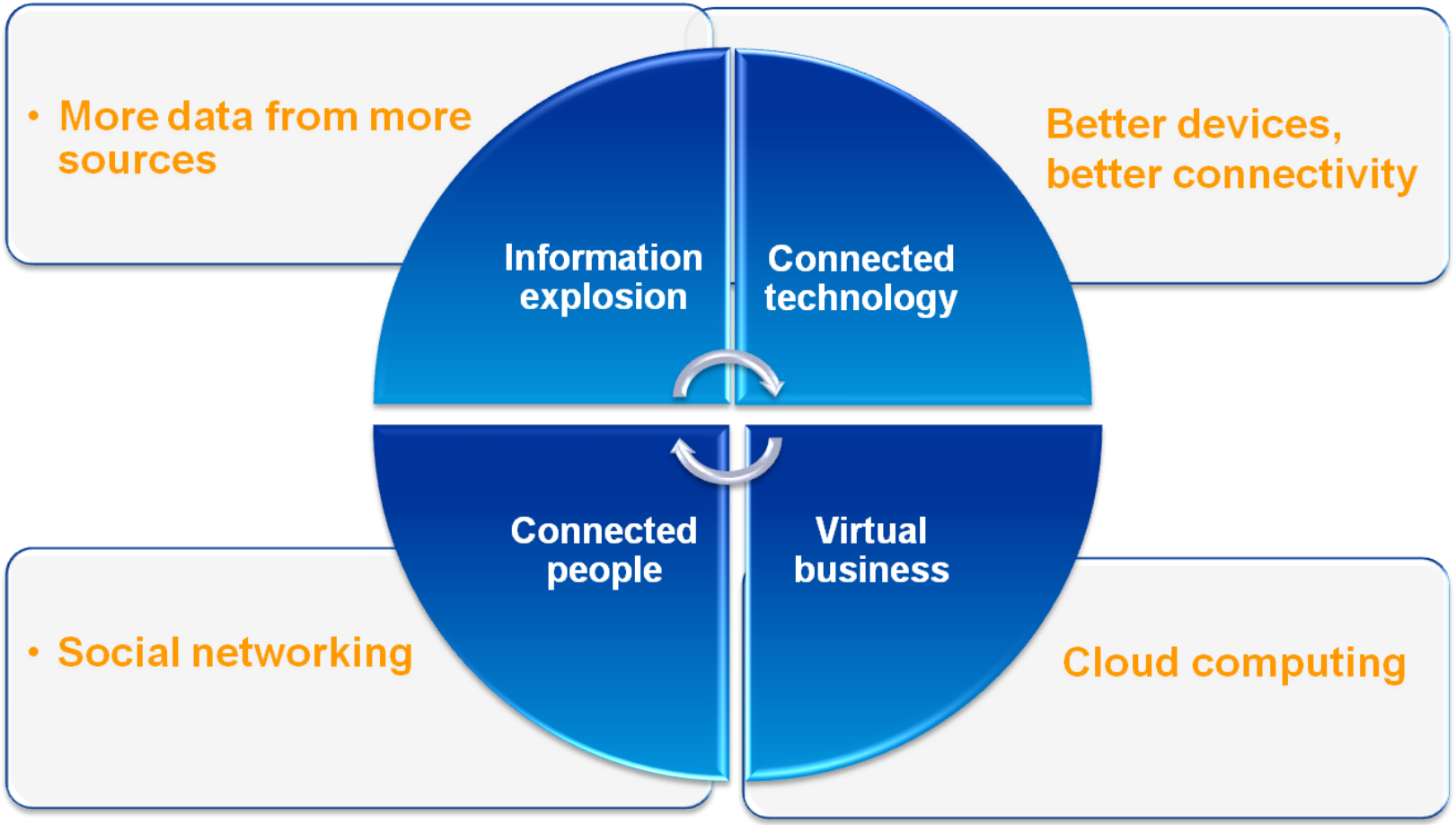
Cyber Risks and Insurance Solutions

Malaysia, November 2013

AIG

Dynamic but vulnerable IT environment



AIG

Cyber risks are many and varied

Malicious attacks

- Cyber theft/cyber fraud
- Cyber terrorism
- Cyber warfare
- Hacking
- Insider attacks
- Industrial espionage

Non-malicious attacks

- Massive disruption/ System failure
- Human error

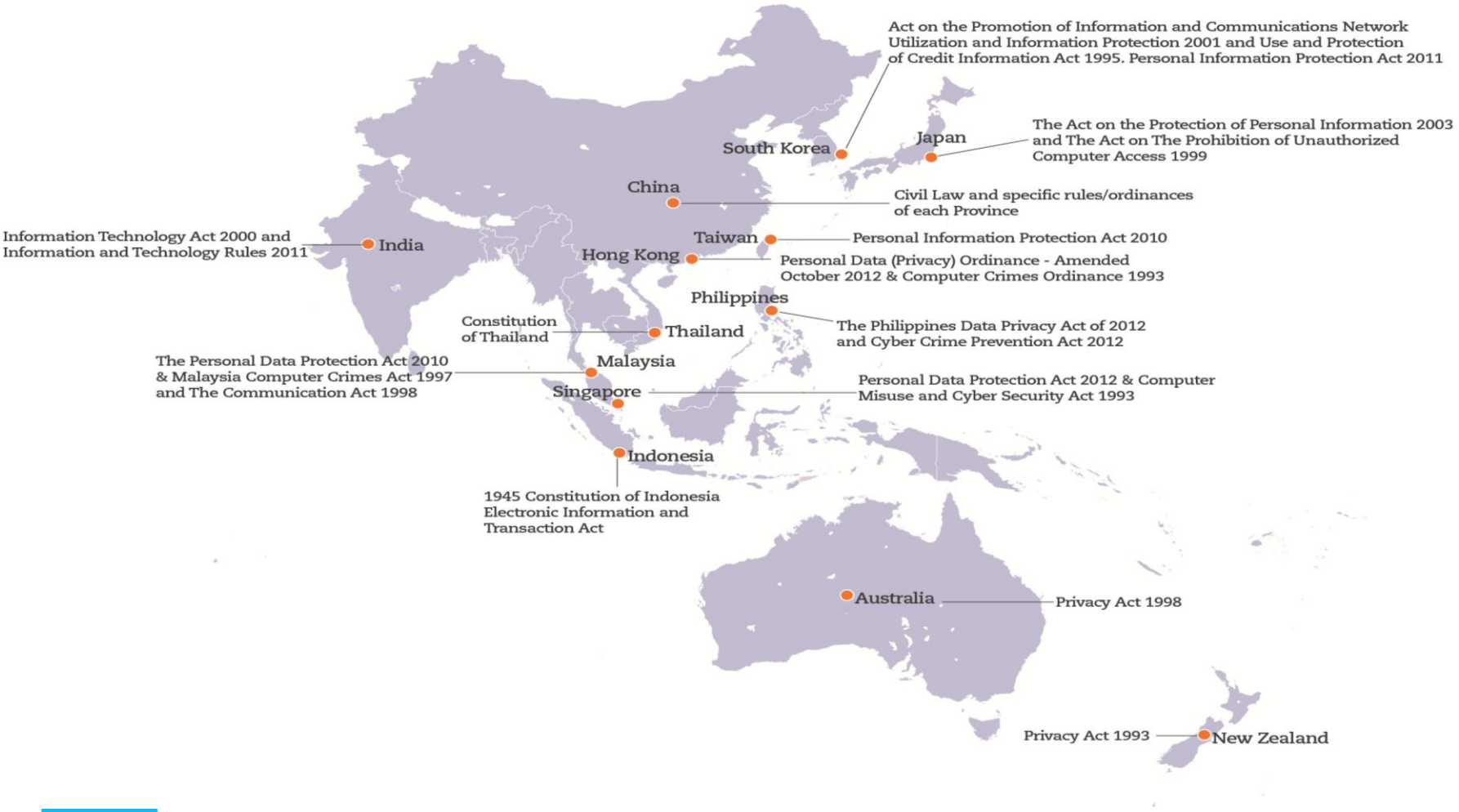
AIG

The Rising Costs of Cyber Threats

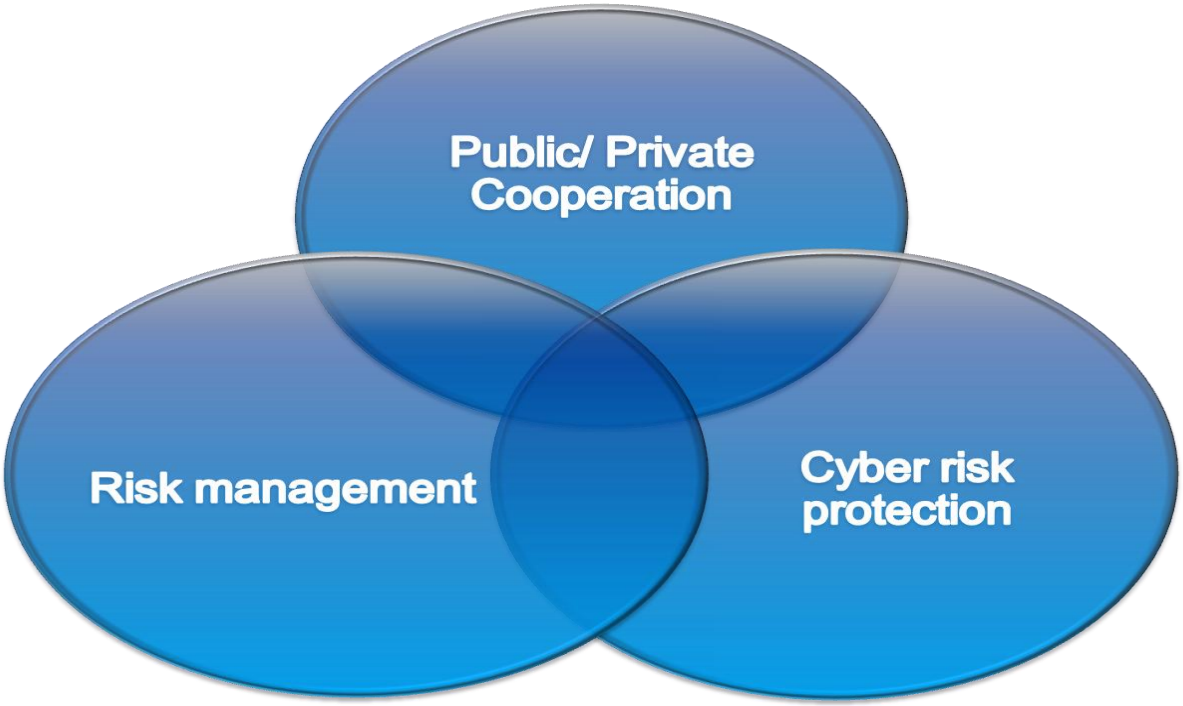
- Operational
- Financial
- Intellectual property
- Legal and Regulatory
- Reputational

AIG

Law and Regulation on the increase



What can Companies do to protect themselves?

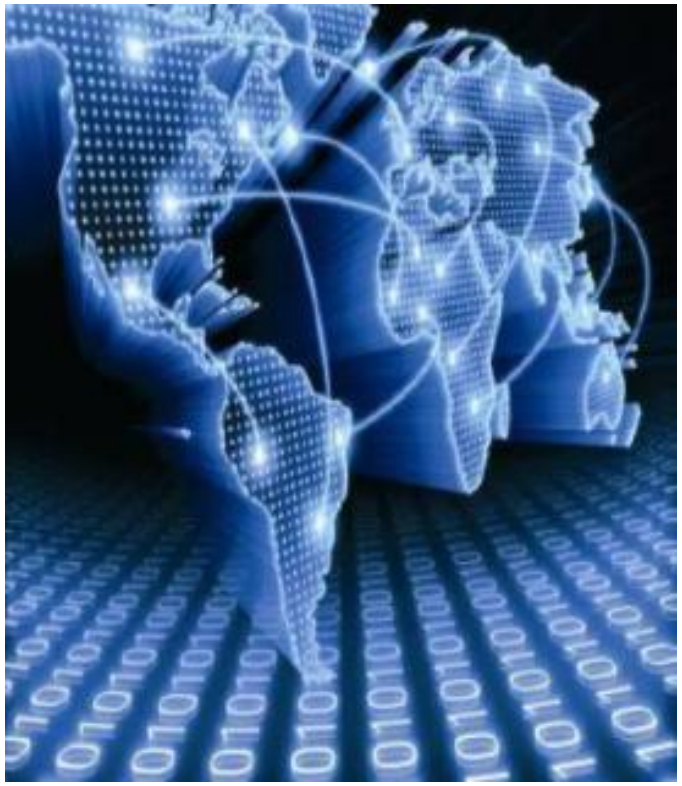


AIG

Closer and stronger cooperation

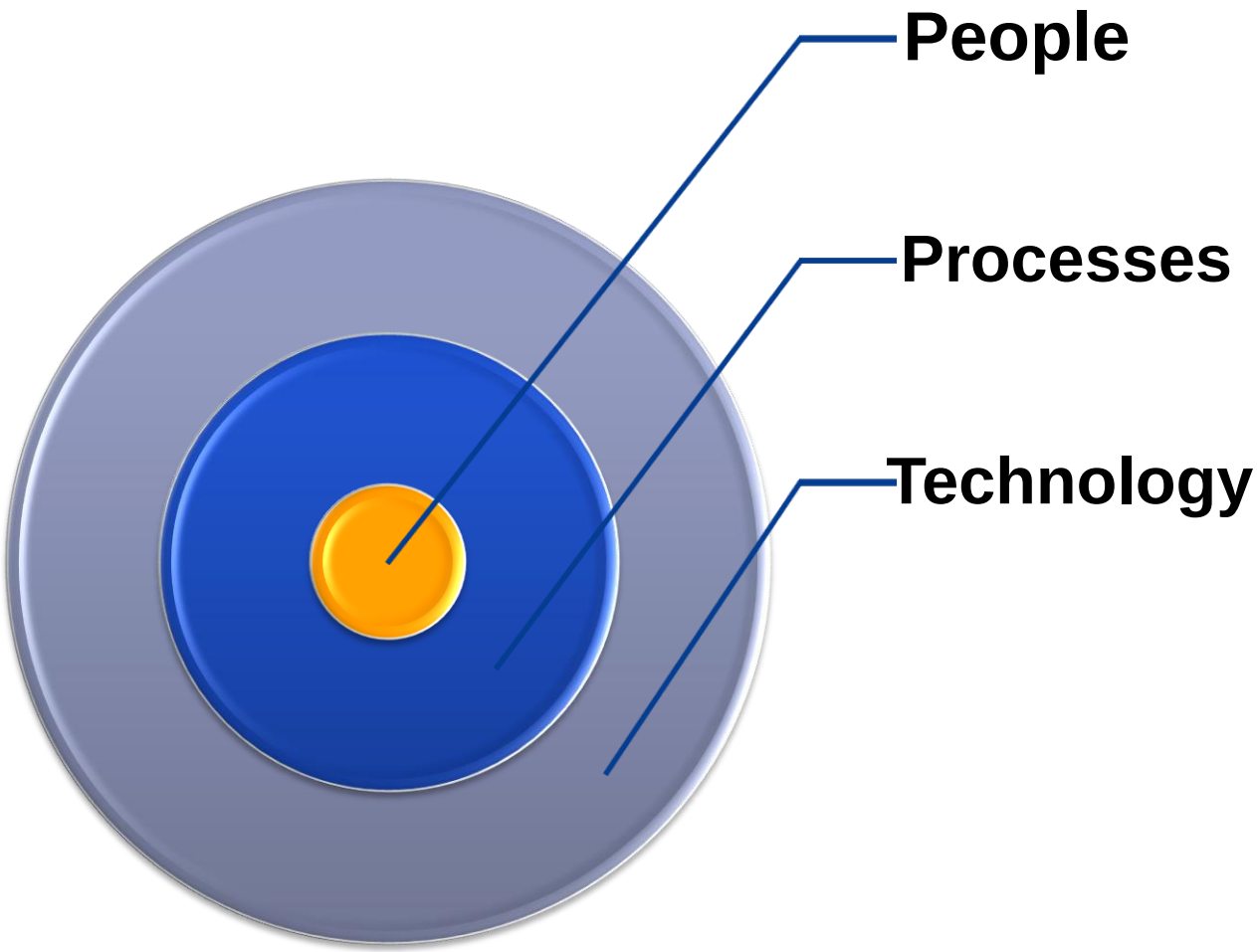
Global challenge requiring a global response

- International bodies (UN)
- Governments
- Industry experts/ IT companies
- Multinationals
- Academia
- Think Tanks



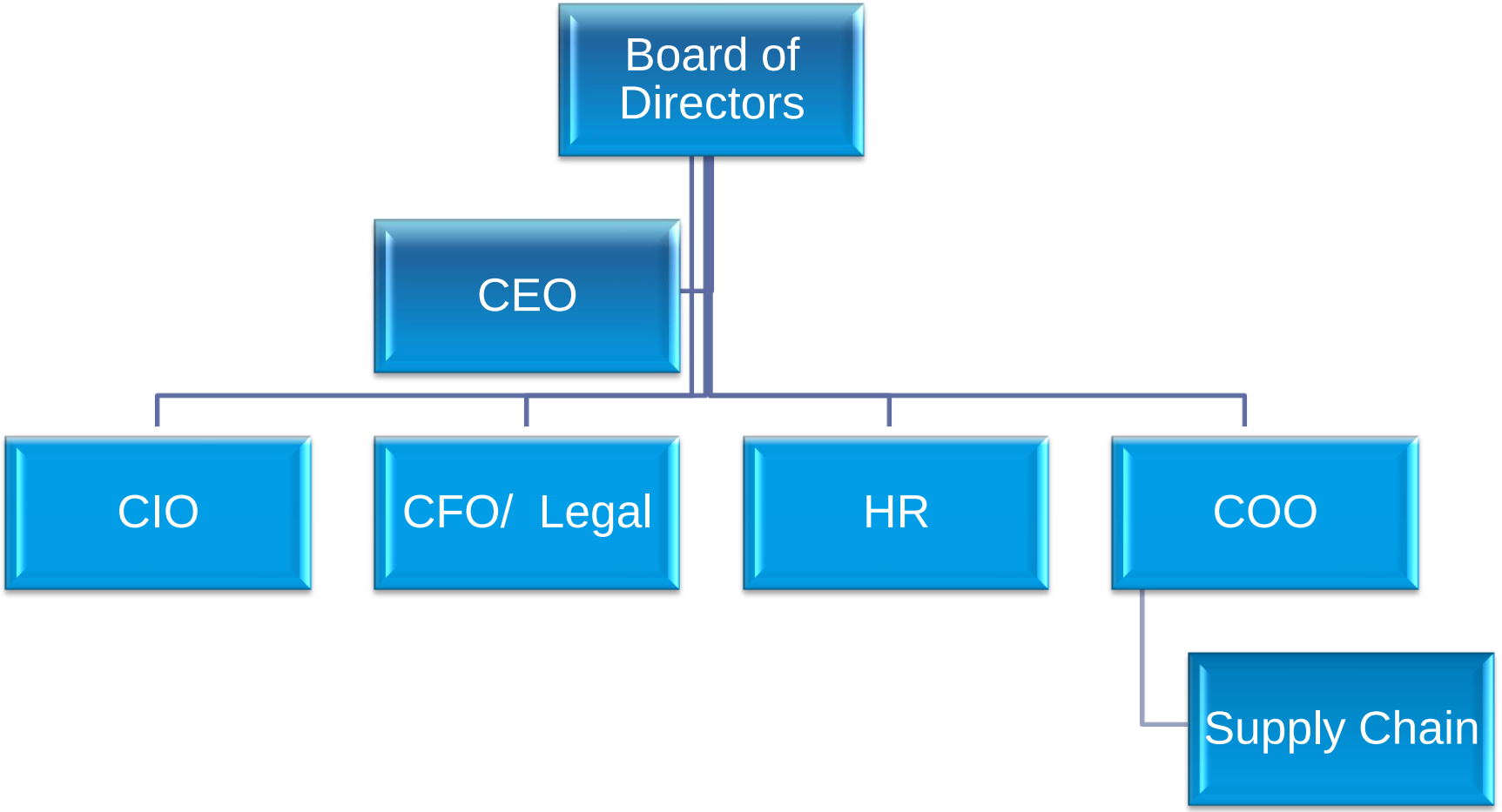
AIG

The Best Practices in Cyber Risk Management



AIG

The Cyber Risk Management should involve all levels of an organization



AIG

What Does Coverage Look Like?

First Party Coverage

- Data disclosure due to a Breach of Data Security
- Prosecution brought by a Data Protection Authority
- Electronic Data Restoration
- Cyber Extortion
- Network Interruption Insurance

Third Party Coverage

- Personal Data Liability
- Corporate Data Liability
- Outsourcing
- Data Security
- Defence Costs - both Civil and Criminal
- Media Content

Tangible Offering/Benefits

- Data Crisis Response – Legal and Reputational
- Pro-active Forensic Services
- Data Administrative Investigation
- Data Administrative Fines
- Notification & Monitoring Costs
- Repair of the Company's and Individual's Reputation

AIG

Constantly evolving coverage's

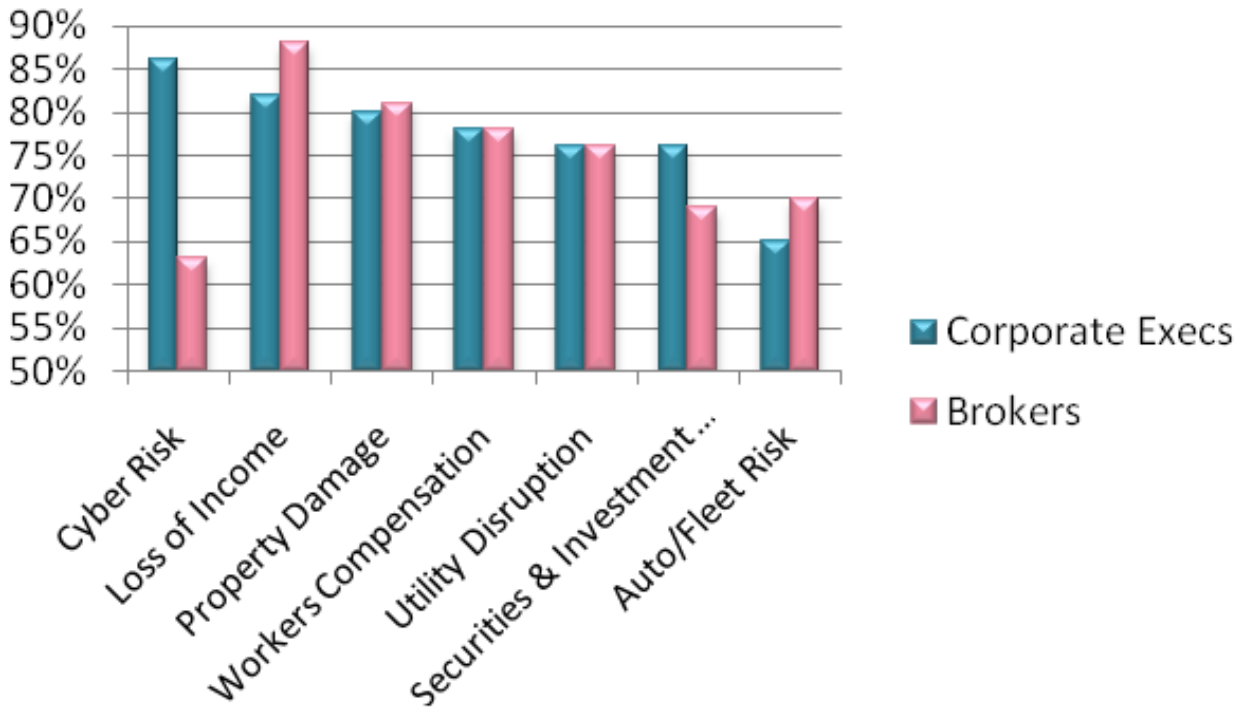
New Covers Introduced

- Cloud Coverage – Definition
- Cloud Failure Coverage – Network Interruption
- Mitigation Instead of Notification Costs
- Cyberterrorism – War and Terrorism?
- Network System Usage Fraud
- PCI Fines

AIG

Cyber opportunity

Somewhat concerned or very concerned about . .



AIG

How we view exposures?

With most clients concerned about cyber risk, the potential market is large. Below are examples of companies that represent a top priority.

Manufacturing / Utilities / Industrial

Manufacturing and production facilities require integrated, reliable operations systems to ensure their production is timely and effective. The supply chain, outsourcing and equipment failures are just a few areas that raise the cyber threat risk.

Retail

Retailers hold a wealth of client information including credit and debit card numbers. Clients who typically use the same password and save login details across several accounts are also placed at greater risk for fraud.

Professional, Office Based & Healthcare

The rise of electronic records, other digital platforms and connected devices have made these segments more vulnerable to security breaches than almost any other industry.

Banking/Finance

Financial institutions have been high on the radar of hackers given the sensitive data at stake. Malware, non-approved devices and third-party business applications all pose unique challenges to banks and other financial companies.

Large Business

Most large companies believe their "IT department is effectively managing the risk from cyber threats." This is similar to doctors not carrying malpractice insurance because they have years of medical experience and expertise.

Small & Mid-Sized Business

Small & Mid-size companies may house large amounts of valuable data, and are more likely to be using legacy systems, but lack the data security budgets of their big business peers.

CLAIMS NARRATIVE – APAC Case Study

Background

The insured was a professional services firm which operated a computer network.

Trend Micro Anti-virus software was installed on servers and all desktop workstations. Anti-virus definitions were up-to-date .

An overnight virus scan ran once a week

Incident Overview

A virus infection was discovered Multiple computers were infected and the virus was spreading via the Insured's network.

Initial attempts to eradicate the virus were unsuccessful; the infection was present the following week. Eventually, the infection was eradicated by wiping and reinstalling all computers on the network.

Damage & Response

The virus left the Insured's computer systems impaired, requiring clean-up work to restore normal operation.

There was no apparent loss of data or privacy breach.

The incident was contained by quick action / solution in conjunction with the CyberEdge Data Crisis Response Team.

AIG's quick response time prevented subsequent reputational damage or harm.

The insured may have missed business opportunities and income during the period of business interuption

Recovery

The initial recovery steps (from 12 October) were focused on cleaning the subset of workstations infected.

The virus was still present on 16 Oct all computer workstations rebuilt, with electronic data restored, recollected and recreated in the process.

Incident Costs

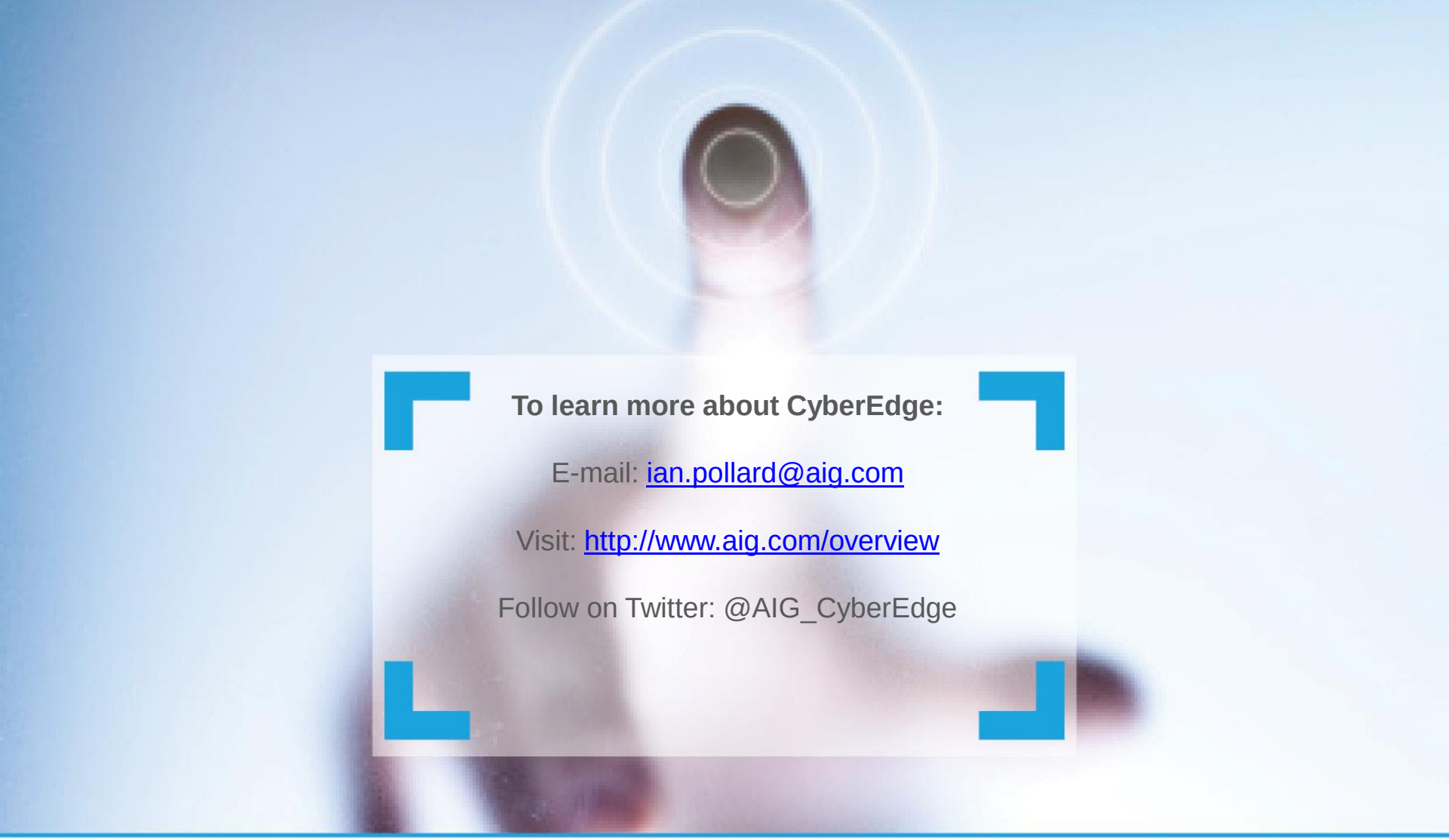
This incident was minor relative to many cyber claims, due in part to the speed of response. No legal or reputational costs were incurred but costs related to data restoration and business interruption were still significant given the size of the company.

Costs covered by AIG:

Restoration of data incl fees for forensic partners: $15,265

Revenue Loss 2: >$20,000

AIG



CyberEdge vs Traditional Insurance

	Property	General Liability	Crime/ Bond	K&R	PI	CyberEdge
1st Party Data Protection Privacy Risks						
Network Interruption						
Cyber Extortion						
Data Restoration, Recollection, Recreation (Determination and Action)						
Employee sabotage of Data						
Virus/ Hacker damage to Data						
Denial of Service attack						
Physical damage to Data Only						
3rd Party Data Protection Privacy Risks						
Breach of Personal Information						
Breach of Corporate Information						
Outsourcing Liability / Vicarious Liability						
Contamination of Third Party Data by any unauthorized software, computer code or virus						
Denial of access to third party data						
Theft of an access code from the Company's premises						
Destruction, modification, corruption, damage or deletion of Data						
Physical theft of the Company's hardware						
Data disclosure due to a Breach of Data Security						
Costs and expenses for legal advice and representation in connection with an Investigation						
Data Administrative Fines						
Repair of Company / Individuals Reputation						
Media Content Liability (IP, Plagiarism, defamation, tresspassing)						
Notificaton Costs						
Monitoring Costs (with identity theft education and credit file or identity monitoring)						

Coverage Provided

Coverage Possible

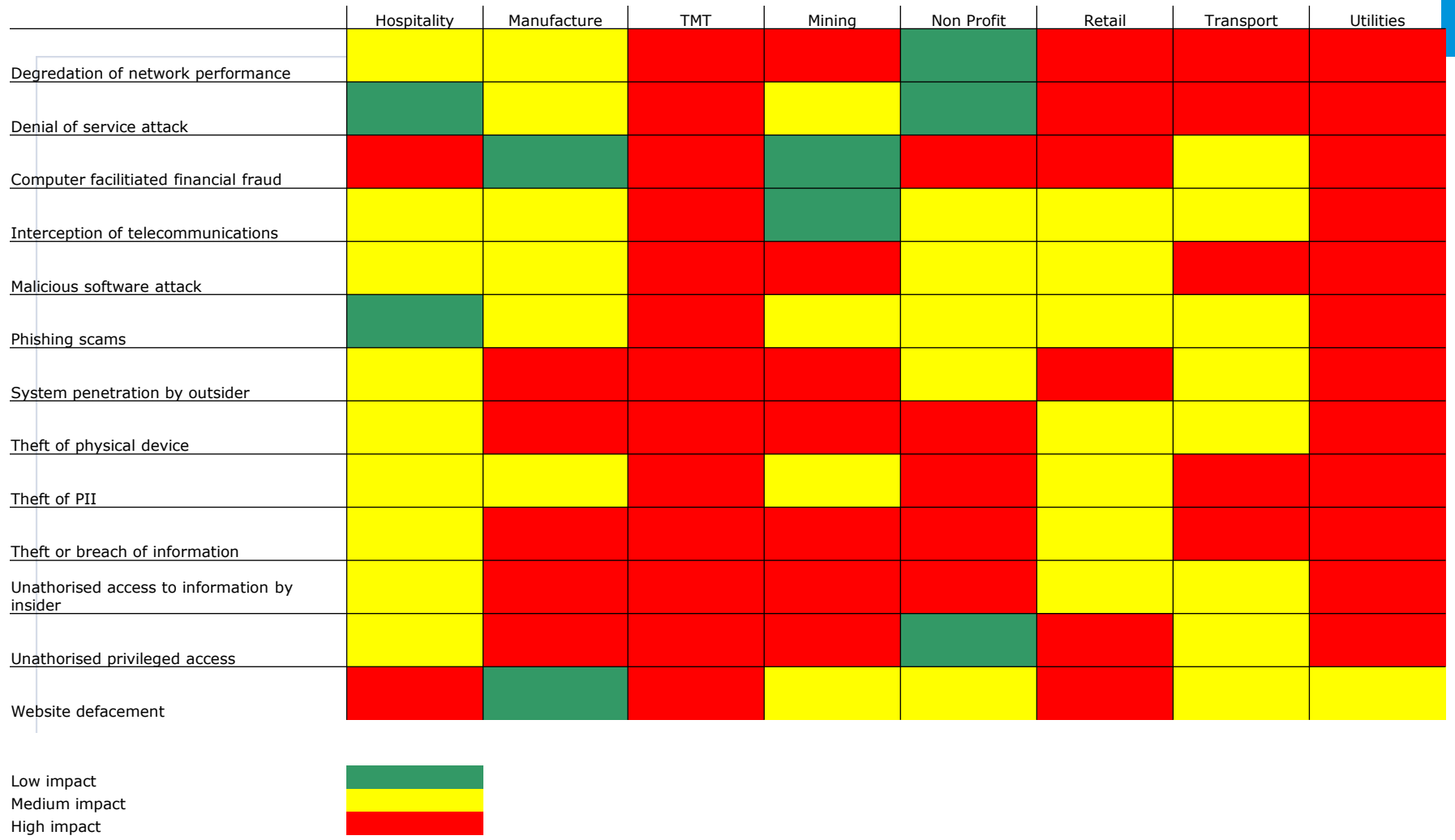
No Coverage

For reference and discussion only: policy language and facts of claim will require further analysis

AIG

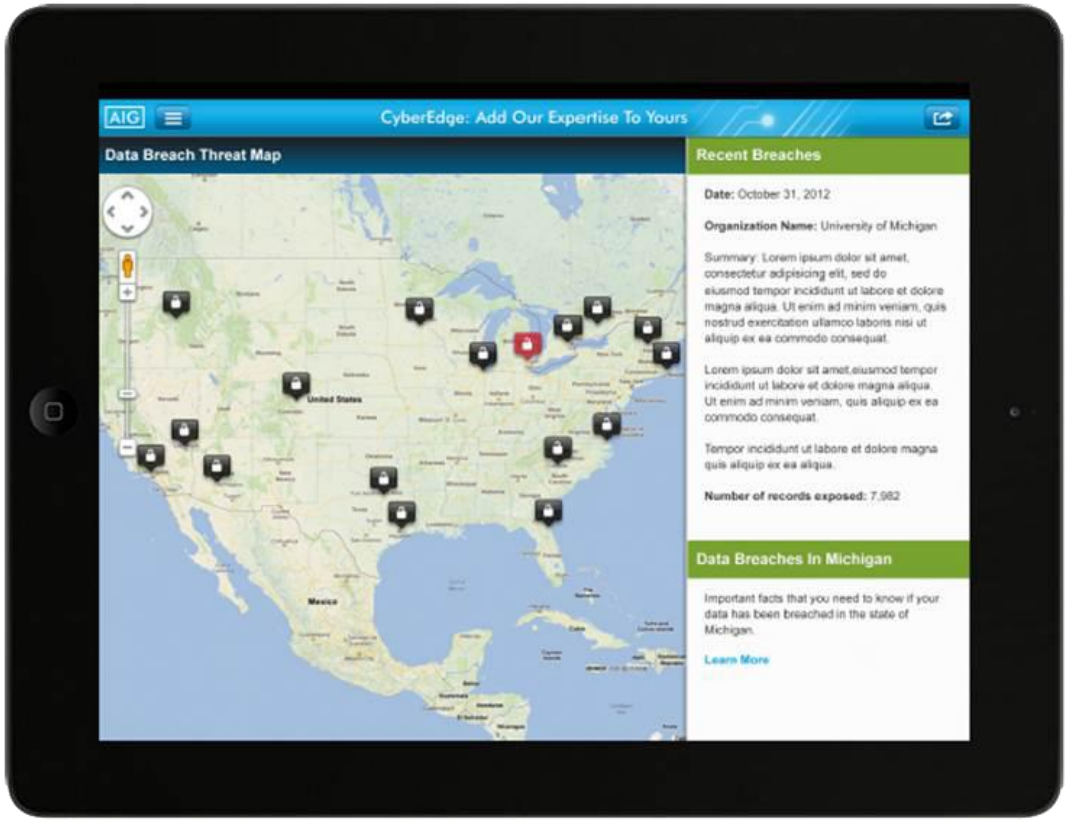
Industry Exposures

Industry Exposures



CyberEdge® Mobile App

The CyberEdge Mobile App for iPads combines the latest cyber news, opinion and risk analysis with real-time updates on country-wide data breaches, to put the cyber information users want at their fingertips. The app is available for free on the App Store.



User Benefits

- All the latest cyber news from industry-leading news providers
- Up-to-the-minute information on country-wide data breaches
- An extensive database of cyber resources
- Risk analysis tools to help determine potential liability costs
- Information on CyberEdge and contact details to learn more

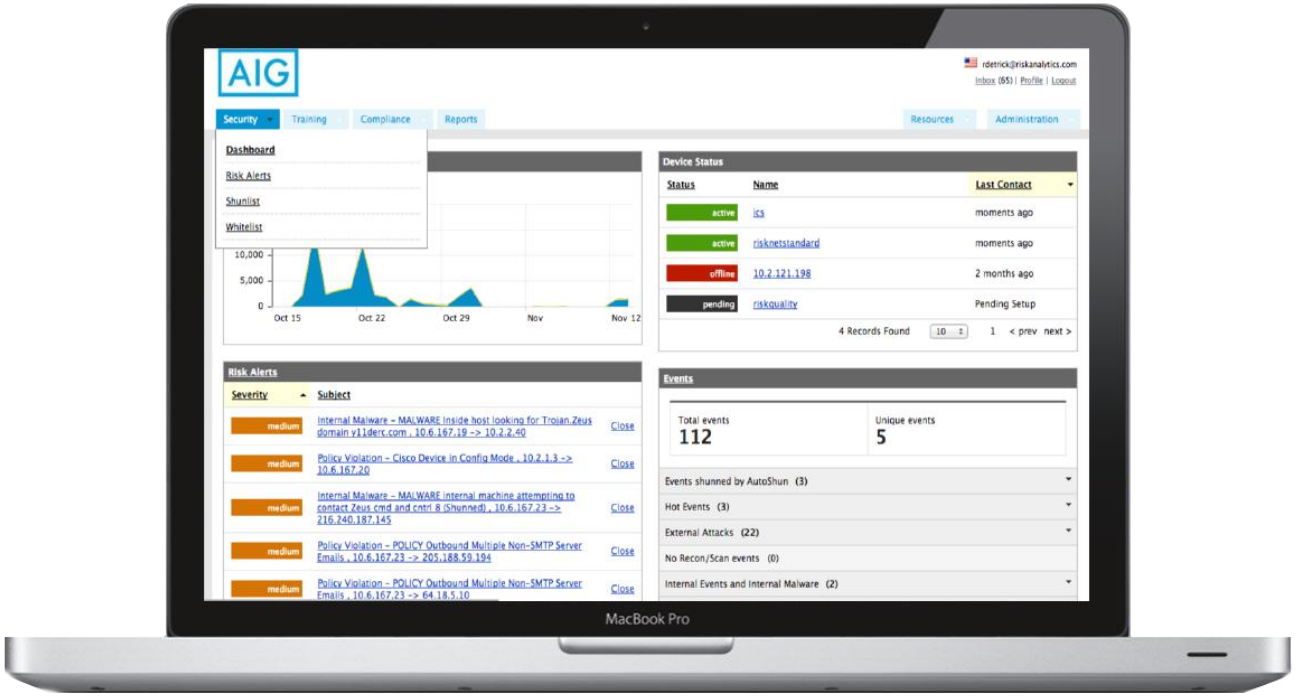
AIG

CYBEREDGE RISKTOOL

While AIG is here for clients when cyber attacks occur, the best way to protect against them is to prevent them in the first place. CyberEdge RiskTool helps companies stay ahead of the curve by managing and automating risk mitigation through a custom portal and a hardware device.

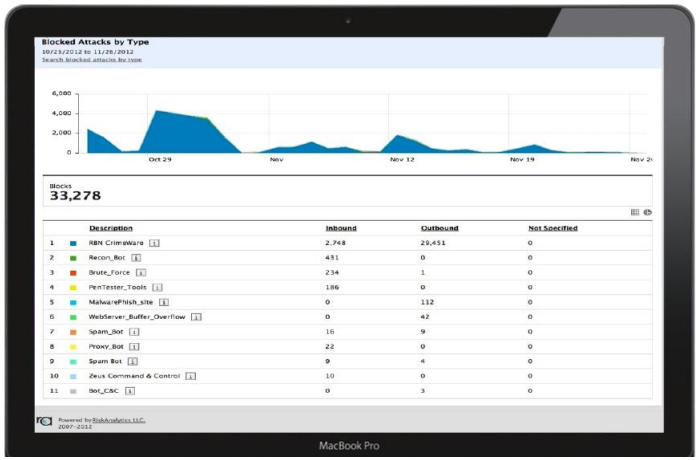
CyberEdge RiskTool

CyberEdge RiskTool is an online website that simplifies the risk management process regardless of the size or complexity of the company. The portal offers a comprehensive solution to compliance and regulatory risk management through a single web-based platform. It also organizes and produces reports on a company's security policies, training and compliance in a way that greatly simplifies the process.



AUTOSHUN®

While AIG is here for clients when cyber attacks occur, the best way to protect against them is to prevent them in the first place. AutoShun® offers peace of mind that the risks to companies' sensitive information and electronic assets are removed, limited or transferred.



AutoShun®

AutoShun® is a simple proactive way of improving your security through a hardware device. Operating in real-time, AutoShun® stops an attack by blocking inbound and outbound communication with known "bad" IP addresses, thus keeping them out of your network. This provides another critical layer in your defence plan.

DASHBOARD


AIG
rdetrick@riskanalytics.com
Inbox (65) | Profile | Logout
Security
Training
Compliance
Reports
Resources
Administration
Dashboard
Risk Alerts
Shunlist
Whitelist
10,000
5,000
0
Oct 15
Oct 22
Oct 29
Nov
Nov 12
Device Status
Status
Name
Last Contact
active
ics
moments ago
active
risknetstandard
moments ago
offline
10.2.121.198
2 months ago
pending
riskquality
Pending Setup
4 Records Found
10
1
< prev
next >
Risk Alerts
Severity
Subject
medium
Internal Malware - MALWARE Inside host looking for Trojan.Zeus domain y11derc.com , 10.6.167.19 -> 10.2.2.40
Close
medium
Policy Violation - Cisco Device in Config Mode , 10.2.1.3 -> 10.6.167.20
Close
medium
Internal Malware - MALWARE internal machine attempting to contact Zeus cmd and cntrl 8 (Shunned) , 10.6.167.23 -> 216.240.187.145
Close
medium
Policy Violation - POLICY Outbound Multiple Non-SMTP Server Emails , 10.6.167.23 -> 205.188.59.194
Close
medium
Policy Violation - POLICY Outbound Multiple Non-SMTP Server Emails , 10.6.167.23 -> 64.18.5.10
Close
Events
Total events
112
Unique events
5
Events shunned by AutoShun (3)
Hot Events (3)
External Attacks (22)
No Recon/Scan events (0)
Internal Events and Internal Malware (2)