Age-Old and Newer Risks: What Every Public Pension Attorney Should Know About Insurance

NOSSAMAN LLP

Presentation to the National Association of Public Pension Attorneys' Legal Education Conference

Austin, TX, June 25, 2015

James H. Vorhis

nossaman.com

Overview

- Why Buy Insurance?
- Got Risk? Immunity – Indemnity – Defense
- Types of Insurance?
  - 3rd Party?
  - 1st Party?
- How Much Insurance?
- The Role of Brokers/Attorneys
- What to Watch for
- Conclusions

NOSSAMAN LLP

Got Risk?


R
I
S
K


LAWSUIT
IN THE (STATE) COURT OF COUNTY
Plaintiff/Petitioner
vs
Defendant/Respondent
QUALIFIED ORDER
AND NOW, THIS


THE UNIT
THIS NOTE IS LEGAL TENDER
FOR ALL DEBTS, PUBLIC AND PRIVATE
K 72390245 A
ONE DOLLAR

Got Risk?

- What are the risks?
  - Lawsuits?
    - From whom? For what?
- Immunity
  - Typically state statutes provide immunity to public officials and employees.
    - Negligent or intentional misrepresentation
    - Entry onto property
    - Initiation of legal proceedings
    - Failure to enforce statute
    - Public employer is immune from vicarious liability where employee would be immune

KNOW YOUR STATE LAW.

Got Risk?

- Indemnity – Typically Mandatory Defense
  - Defense of civil actions
  - Upon request of employee or former employee
  - Act or omission within the scope of his employment
  - Board members are "employees" under some states' authority (*See, e.g.,* 57 Op. Atty Gen. Cal. 358 (1974))
- Typical Exceptions
  - No defense if the public entity determines:
    - Acts or Omissions not within scope of employment; or
    - Actual fraud, corruption or actual malice; or
    - Conflict of interest

Got Risk?

- Indemnity – Typically Defense is Discretionary where:
  - Defense of administrative or criminal proceedings
  - <u>May</u> defend it:
    - Acts within scope of employment;
    - Defense in best interest of public entity; and
    - Employee acted in
      - » Good faith;
      - » Without actual malice; and
      - » In the apparent interests of the public entity

Got Risk?

- Indemnity – Judgments or settlements
  - Typically public entity shall pay judgment or settlement if:
    - Injury arises out of an act or omission;
    - Within the scope of employment; and
    - Employee reasonably cooperates in defense of the claim or action
  - Common exceptions
    - Reservation of rights re scope of employment
    - Punitive/exemplary damages not covered unless:
      - Course and scope of employment;
      - Employee acted in good faith;
      - Without actual malice and in the apparent best interests of the public entity; and
      - Payment would be in “best interests” of the public entity

Types of Insurance

- Third Party
  - General Liability
  - Fiduciary Liability
  - Errors & Omissions
  - Management/D&O
  - Employment Practices Liability
  - Cyber Insurance (Data Breach)

Types of Insurance

- First Party
  - Property
  - Fidelity

How Much Insurance?

- Limits? Sublimits?
  - Defense Costs
    - Burning
    - Outside Limits
  - Indemnity
  - Benchmarking
  - Deductibles / Self-Insured Retention
  - Coverage for non-monetary relief?

The Role of A Broker

Why do I need an insurance broker?

- Who is your broker?
  - Relationship
  - Knowledge
  - Experience

The Role of An Attorney

- Why do you need an attorney?
  - Plays a role different than the broker
  - Analyze coverage and likely legal issues raised by structure of policy
  - Recommend alternative language, coverage terms or exclusions

What to Watch For

- What is a “Claim?”
- Reporting Requirements
  - Claims made
  - Claims made and reported
  - “Occurrence”-based
- Notice of Circumstances

What to Watch For

- Reporting Requirements – Claims Made and Reported
  - *Root v. American Equity Specialty Ins. Co.*, 130 Cal. App. 4th 926 (2005)
  - Three days before his legal malpractice insurance expired, Mr. Root received a phone call about a lawsuit (by a client for whom he had recovered $2.75M)
  - He thought it was a prank and took no further action. Mr. Root went away for the long weekend.
  - A new policy period with a different insurer incepted while he was gone.
  - Upon his return, Mr. Root read about the lawsuit in papers and immediately notified his carriers.
  - The first carrier denied coverage because Mr. Root had not reported the claim during its policy period.
  - The second carrier denied coverage on the ground that Mr. Root had known of the circumstances giving rise to claim prior to the inception of coverage.

Understand your Insurance

- *Zurich American Ins. Co. v. Sony Corp. of America* (N.Y. Sup. Ct. Feb. 21, 2014)
- Hackers stole personal information of Sony PlayStation users
- Over fifty class action lawsuits were filed against Sony for breach of privacy
- Sony sought a defense, contending that there was an improper "publication" as a result of the data breach
- Zurich denied coverage, contending there was no "publication," and that Sony needed to have been the party publishing the information
- The trial court sided with Zurich and denied the duty to defend. It ruled that there was a "publication," but not by Sony. The case was appealed and then reportedly settled
- The Lesson: You cannot count on coverage under traditional policies

What to Watch For

- Choice of Counsel
- Right to Control Defense
- Arbitration Provisions
- Choice of Law Provisions
- Contract Interpretation Provisions

- What's Covered and What's Not (e.g., notices to consumers and identity protection services?)
- Contractual Statute of Limitations
- Recourse Against Fiduciaries; and Waiver of Recourse

Conclusions

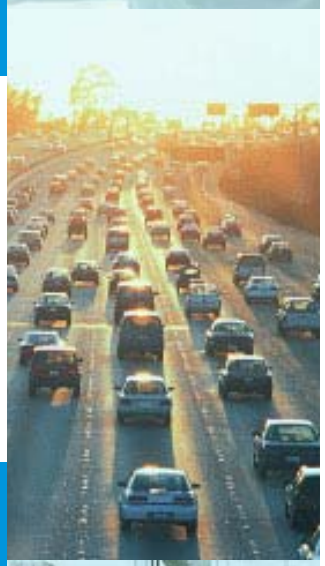
- Choosing Your Broker and Attorney
- Read the Policy!
  - No surprises
- Read the Policy!

Any Questions?




CYBER LIABILITY

Network Security and Privacy




AGENDA

I. Identify Exposures
II. Third Party Liability
III. First Party Losses
IV. Ancillary Coverage Sections
V. Claims
VI. AIG CyberEdge Risk Management Solutions
VII. Questions & Answers

AIG

HOW DO WE IDENTIFY EXPOSURES?

DO THEY HANDLE INFORMATION? IF SO, WHAT KIND?

- Their own company (including employees)
- Their clients (Confidential - personal or commercial)

WHERE DO THEY STORE THE INFORMATION, ONLINE - OFFLINE

- Computer Network - Do they operate the network themselves or outsource to a vendor?
- Paper Records

DO THEY HAVE A WEBSITE?

- What is the content on the site?
- Can employees or third parties upload content (e.g. blog, post pictures, post comments)?

AIG

HOW CAN A BREACH OCCUR?

INTERNALLY

- Employees/Vendors
    - Stealing Information (Card Skimming)
    - Lost Resources (Laptop, Smart Phone, Tablet)
    - Mishandling Of Paper Files

EXTERNALLY

- Individual Hackers/Organized Crime
    - Stealing Information
    - Sending Viruses/Malicious Code
    - Disruption Of Business (Vandalism)

AIG

THIRD PARTY COVERAGE

NETWORK SECURITY FAILURE

- A Failure of a Company to Protect their Computer System
  - Virus, Malicious Code, Malware Attacks

PRIVACY EVENT

- A Failure to Protect Confidential Information
  - Personal or Corporate
  - Online or Offline
- Violation of any Federal, State or Local Privacy Statute
- Failure to Comply with PCI-DSS Standards

ALLEGATIONS CAN BE BROUGHT BY

- Individuals, Businesses, Administrative or Government Agencies

AIG

FIRST PARTY COVERAGE

EVENT MANAGEMENT – BREACH RESPONSE PLAN

- Breach Consultation
- Forensic Investigation
- Public Relations Services
- Notification To Consumers Based On State Mandate
- Providing Id-monitoring/Credit Monitoring Or Other Remediation Services To Help Minimize Damages To Those Victimized
- Lost Electronic Data

AIG

FIRST PARTY COVERAGE

NETWORK INTERRUPTION

- Addresses loss of income and operating expenses when business operations are interrupted or suspended due to a failure of network security

CYBER EXTORTION

- Network security related extortion demands made against the insured
- Kidnap & ransom insurance for a computer network

AIG

THIRD PARTY COVERAGE

MEDIA CONTENT LIABILITY

Liabilities Faced By Companies Have Published Content:

- Website, Print, Broadcast, etc
- Responds to claims arising out of all media distributed by the insured (Website Only, Online and/or Offline)

Typical Types Of Claims:

- Trademark Infringement; Copyright Infringement;
- Defamation; False Light; False Imprisonment;
- Product Disparagement; Infliction of Emotional Distress;

AIG

BREACH RESPONSE TIMELINE

AIG

CYBEREDGE BREACH RESOLUTION TEAM

24/7 Hotline *Supported by* ***IBM : 1—800-CYBR -345***

- Insureds have access to an IBM operated hotline for IT professionals to consult on identifying key indicators of a breach
- If a breach is suspected, insureds will be connected with our in- house claims team
- Provides the additional layer of support an IT department needs to face a cyber attack

Unprecedented Claims Handling Experience

- 2011 to 2014 U.S. claim volume increased 148%
- Two breaches per business day reported to AIG in 2014
- Average cost of defense > $500,000
- Number of $1M+ reserves: increased by225% from 2011 to 2014

AIG

CyberEdge Risk Management Solution

Tools for Tomorrow

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 and our breach resolution team provides responsive guidance based on years of experience.

CyberEdge Mobile App for iPhone,® iPad,® and Android™

The CyberEdge Mobile App combines the latest cyber breach information, news, opinion, and risk analysis users want at their fingertips. With a sleek look and many features globalized, the app is the first-of-its-kind and is now available for the iPad,® iPhone,® and Android.™

Going Global

- Data Breach Threat Map displays breaches from around the world.
- Available in English, French, and Spanish.
- CyberEdge marketing documents, applications, and specimen policy language for many countries where coverage is available.

User Friendly

- Share, Tweet, or email content from pages in the app.
- Drop down news filter provides focused and relevant search results.
- Learn more about breach notification regulations in the state where the breach occurred right from the Data Breach Threat Map.

Infrastructure Vulnerability Scanning *Powered by* ***IBM***

Our qualified clients receive infrastructure vulnerability scanning powered by IBM. IBM will leverage its robust Managed Security Services capability to conduct remote scanning for clients' web-facing external infrastructure, which will help to identify potential vulnerabilities that could be exploited by a remote hacker via the Internet.

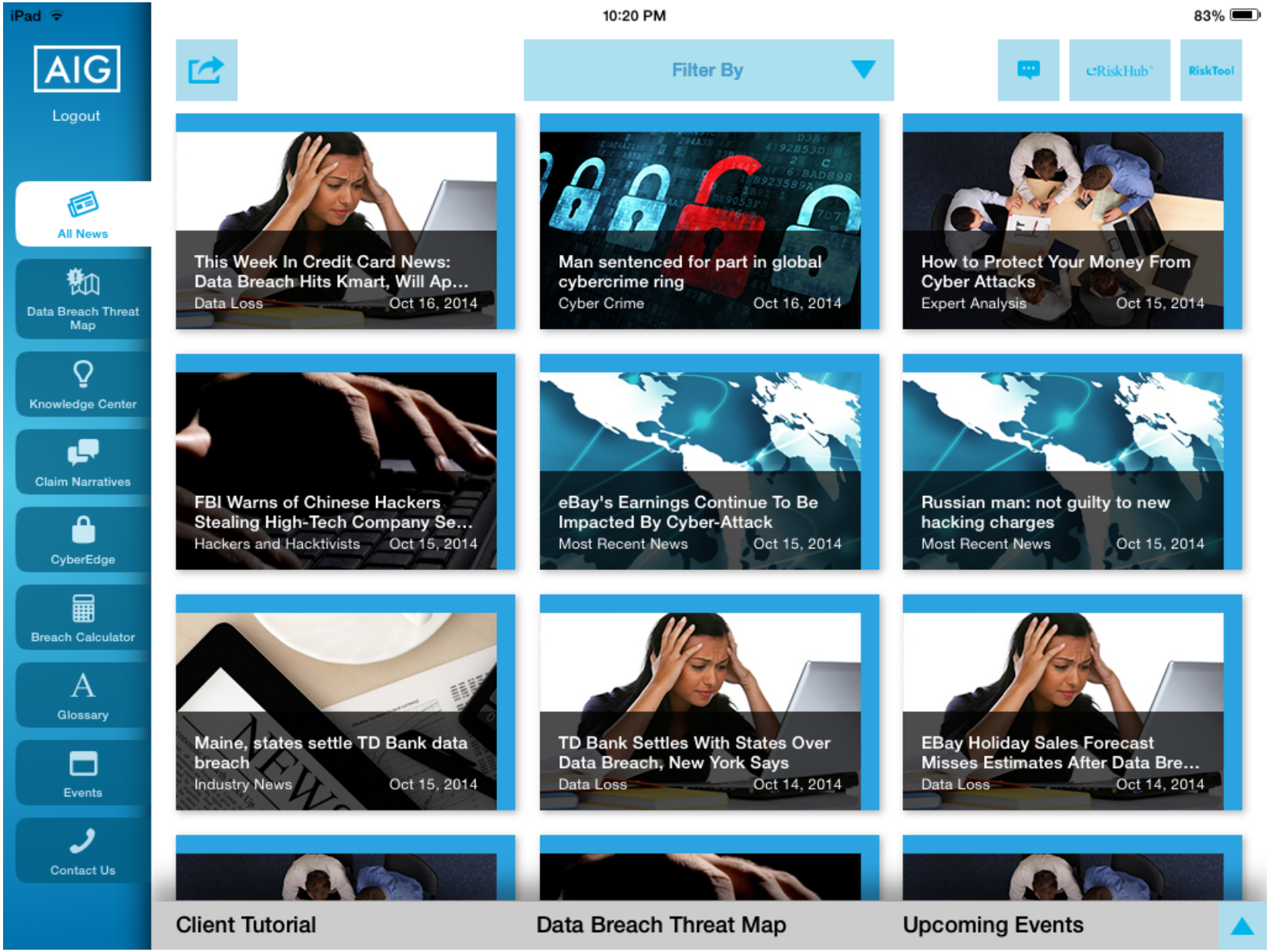
In addition, the infrastructure vulnerability scanning service:

- Leverages advanced scanning capabilities to detect and prioritize hidden risks on public-facing and internal network infrastructure.
- Provides a detailed view of a company's vulnerability status so clients can better track, understand, and report on their security posture.
- Prioritizes vulnerabilities so clients reduce their overall threat exposure.
- Unique reporting capabilities to help speed vulnerability identification and remediation.

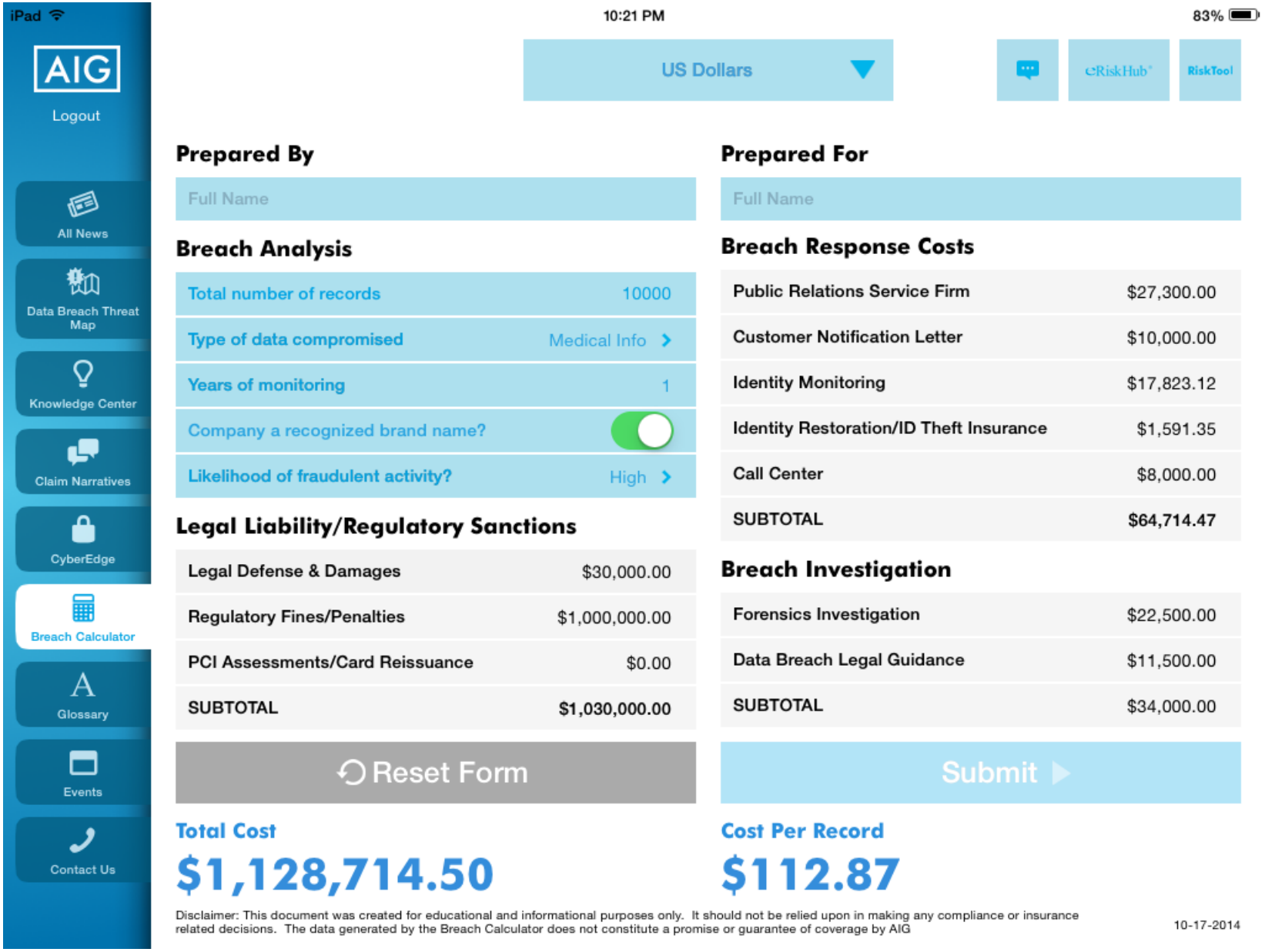
Key Components

- Reports help demonstrate compliance with federal, state, and industry regulations
- Assess an environment from either the external or internal perspective
- IBM Security expertise improves accuracy of findings and reduces mitigation time
- Consultation on recommendations for improved security

AIG


iPad
10:20 PM
83%
AIG
Logout
All News
Data Breach Threat Map
Knowledge Center
Claim Narratives
CyberEdge
Breach Calculator
Glossary
Events
Contact Us
Filter By
eRiskHub
RiskTool
This Week In Credit Card News: Data Breach Hits Kmart, Will Ap...
Data Loss
Oct 16, 2014
Man sentenced for part in global cybercrime ring
Cyber Crime
Oct 16, 2014
How to Protect Your Money From Cyber Attacks
Expert Analysis
Oct 15, 2014
FBI Warns of Chinese Hackers Stealing High-Tech Company Se...
Hackers and Hacktivists
Oct 15, 2014
eBay's Earnings Continue To Be Impacted By Cyber-Attack
Most Recent News
Oct 15, 2014
Russian man: not guilty to new hacking charges
Most Recent News
Oct 15, 2014
Maine, states settle TD Bank data breach
Industry News
Oct 15, 2014
TD Bank Settles With States Over Data Breach, New York Says
Data Loss
Oct 14, 2014
EBay Holiday Sales Forecast Misses Estimates After Data Bre...
Data Loss
Oct 14, 2014
Client Tutorial
Data Breach Threat Map
Upcoming Events

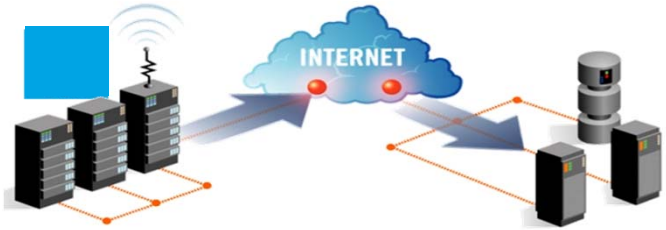

iPad
10:21 PM
83%
AIG
Logout
All News
Data Breach Threat Map
Knowledge Center
Claim Narratives
CyberEdge
Breach Calculator
Glossary
Events
Contact Us
Map View
eRiskHub
RiskTool
CANADA
Hudson Bay
ALTA.
B.C.
SASK.
MAN.
ONT.
QUE.
N.L.
P.E.I.
Edmonton
Regina
Winnipeg
MONT.
IDAHO
WYO.
NEB.
MEXICO
Hermosillo
Culiacán
Monterrey
Guadalajara
Mexico City
Veracruz
Acapulco
Gulf of Mexico
Havana
CUBA
JAMAICA
DOMINICAN REPUBLIC
San Juan
BELIZE
Royal Inland H...
Kamloops, BC, Ca...
Haley Chiropra...
Tacoma, WA 9840...
WorkSource Or...
Salem, OR, USA
Essentia Health
Fargo, ND, USA
Indian Health S...
Rapid City, SD, USA
National Resea...
Kent Record M...
Council on Ene...
Option Courier...
Provo City Sch...
Fort Havs St
George Mason...
Cancer Special...
Cedars-Sinai M...
California, USA
SuperValu, Inc.
Santa Fe Famil...
Home Depot
Urological Ass...
Tucson, AZ, USA
Baltimore Jewi...
Dallas, TX, USA
Bulloch Pediatr...
Goa News
San Antonio, TX, U...
Beef 'O' Brady's
Aventura Hospi...
Aventura, FL, USA
Legal


iPad
10:21 PM
83%
AIG
Logout
US Dollars
eRiskHub
RiskTool
All News
Data Breach Threat Map
Knowledge Center
Claim Narratives
CyberEdge
Breach Calculator
Glossary
Events
Contact Us
Prepared By
Full Name
Prepared For
Full Name
Breach Analysis
Total number of records 10000
Type of data compromised Medical Info
Years of monitoring 1
Company a recognized brand name?
Likelihood of fraudulent activity? High
Legal Liability/Regulatory Sanctions
Legal Defense & Damages $30,000.00
Regulatory Fines/Penalties $1,000,000.00
PCI Assessments/Card Reissuance $0.00
SUBTOTAL $1,030,000.00
Breach Response Costs
Public Relations Service Firm $27,300.00
Customer Notification Letter $10,000.00
Identity Monitoring $17,823.12
Identity Restoration/ID Theft Insurance $1,591.35
Call Center $8,000.00
SUBTOTAL $64,714.47
Breach Investigation
Forensics Investigation $22,500.00
Data Breach Legal Guidance $11,500.00
SUBTOTAL $34,000.00
Reset Form
Submit
Total Cost
$1,128,714.50
Cost Per Record
$112.87
Disclaimer: This document was created for educational and informational purposes only. It should not be relied upon in making any compliance or insurance related decisions. The data generated by the Breach Calculator does not constitute a promise or guarantee of coverage by AIG
10-17-2014

AIG

INFRASTRUCTURE VULNERABILITY SCANNING *POWERED BY* IBM

- Provides vulnerability management led by an experienced security consultant
- Detects vulnerabilities across network devices, servers, web applications, and databases to help reduce risk exposure and better manage compliance requirements
- Strong security expertise provides vulnerability identification with resulting prioritized plan for remediation and improved security



Key Components

- Reports help demonstrate compliance with federal, state and industry regulations
- Assess an environment from either the external or internal perspective
- IBM Security expertise improves accuracy of findings and reduces mitigation time
- Consultation on recommendations for improved security

AIG

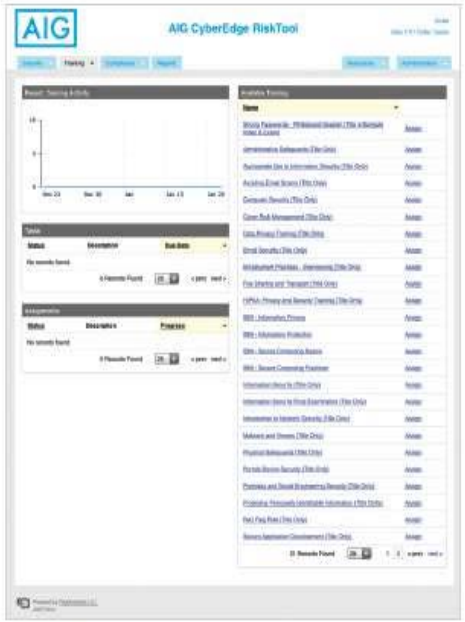
CyberEdge Risk Management Solution

CyberEdge RiskTool

CyberEdge RiskTool, our single, web-based platform, helps clients streamline the risk management process. The platform's content is highly customizable and can be tailored specifically to meet a number of risk management needs.

Risk management modules include:

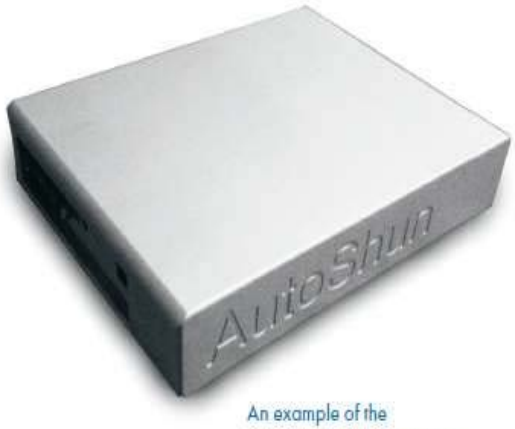
- **Security:** Provides an interface where an IT department can manage a company's shunning technology, which blocks known cyber criminals from communicating with a company's network.
- **Training:** Includes pre-populated training content and tests with an online assignment engine to deploy employee training and awareness with the click of a mouse.
- **Compliance:** Comes pre-loaded with security policy templates that can be accepted or modified to fit each company's needs. Existing policies can also be uploaded and tasked to employees or third-party vendors to confirm receipt and acceptance.



Proactive Shunning Service *Powered by* ***RiskAnalytics***

RiskAnalytics provides qualified clients with leading edge intelligence that isolates and shuns bad IP addresses, preventing them from entering and exiting a company's network. With millions of known "bad" actors constantly updated on the current shun list, RiskAnalytics' technology identifies and blocks the largest sources for malware, crimeware, and fraud.

RiskAnalytics will provide qualified insureds with the most appropriate cloud services and/or appliance that best fits an insured's needs and network speeds.



An example of the AutoShun hardware device.

AIG

WHAT IS IP SHUNNING?

- Service blocks CrimeWare through multiple appliance options

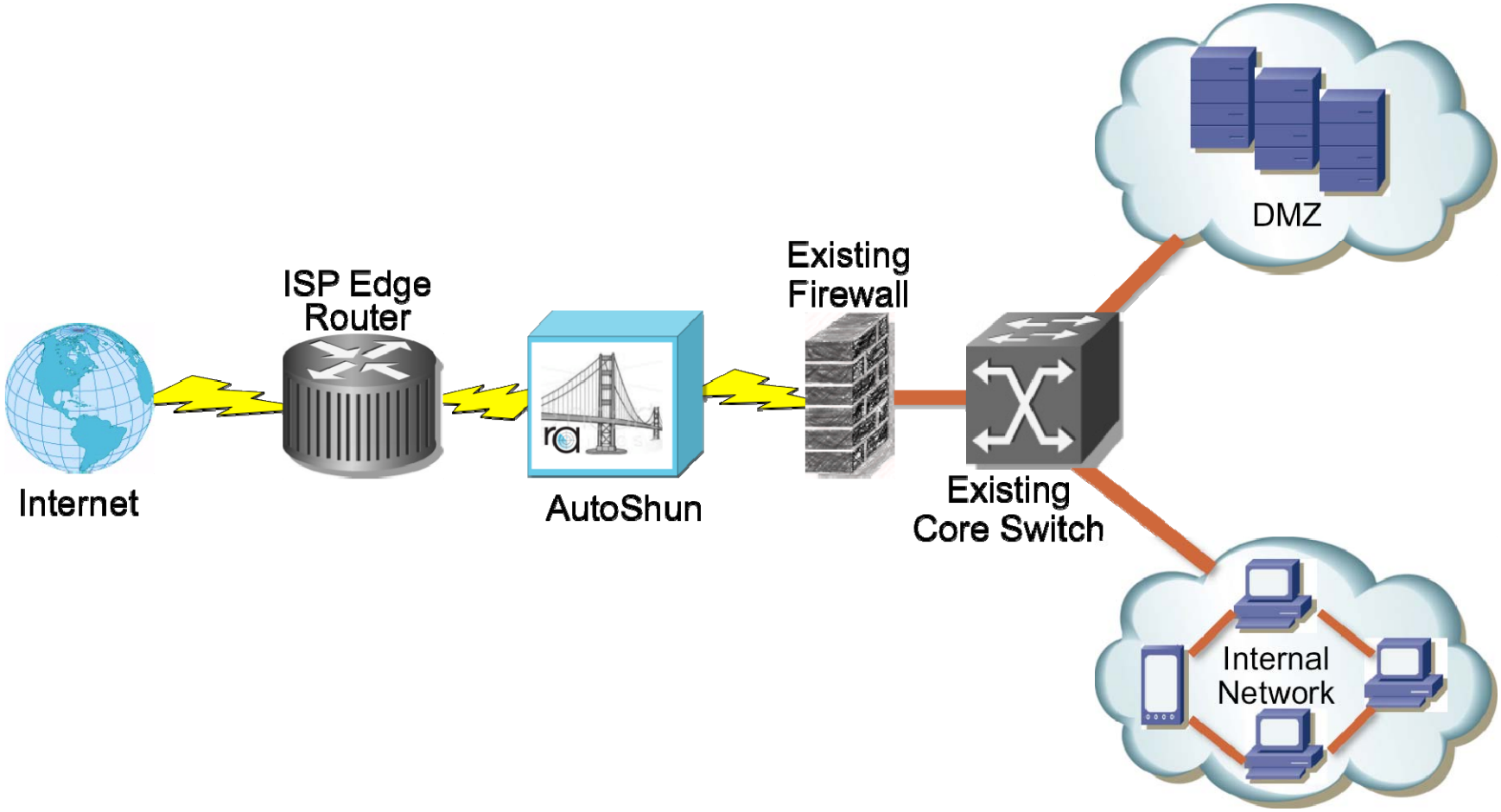
- Matched to network speed and failover requirements
- Positioned outside the firewall, no impact to existing network
- Real-time updates

AIG

DYNAMIC THREAT MATRIX

AIG

IP SHUNNING TYPICAL DEPLOYMENT



AIG

BLOCKED ATTACKS BY TYPE

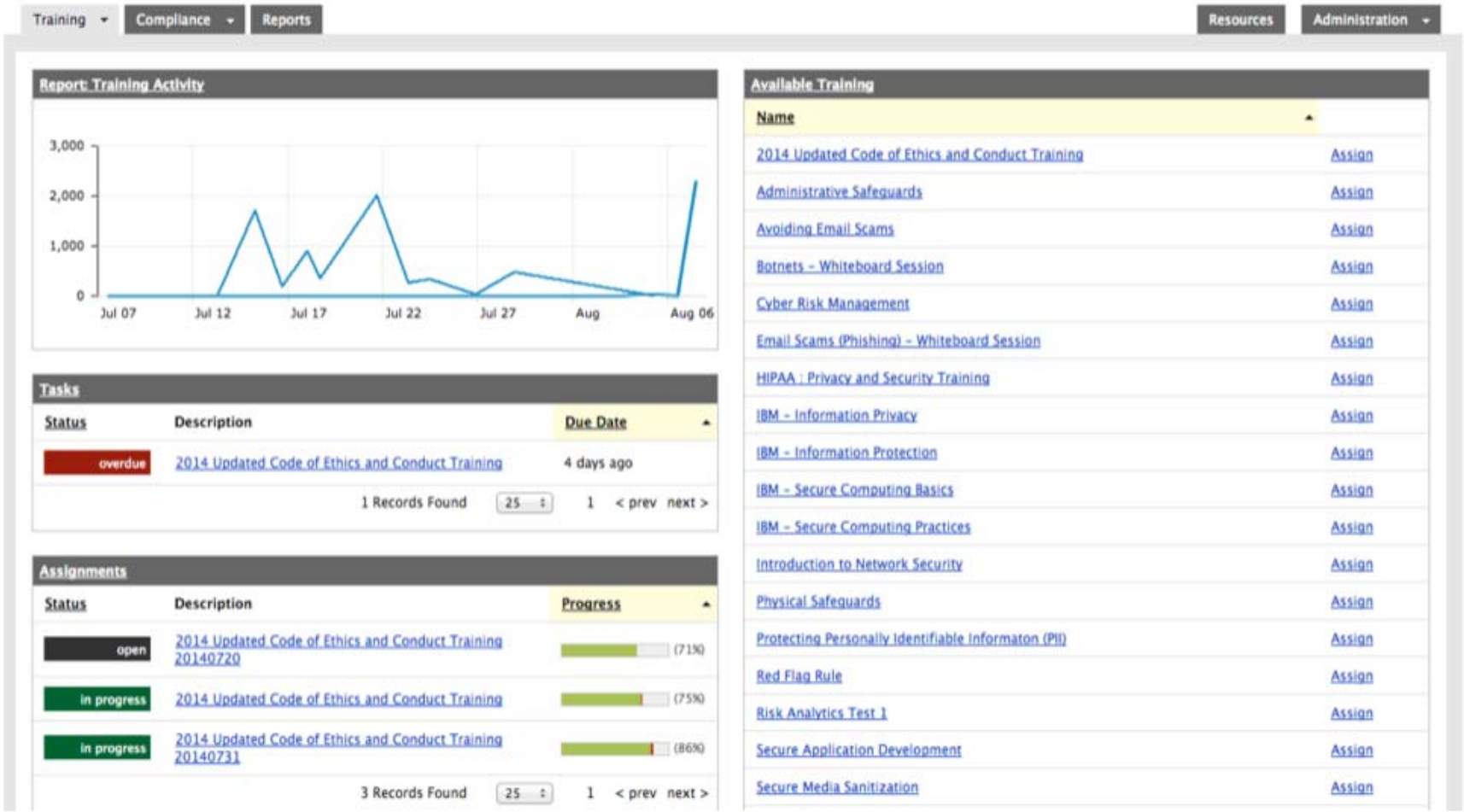
AIG

CYBEREDGE RISKTOOL

- Web-based customizable risk management platform
- Manage the human element of cyber risk and manage compliance
- Pre-populated with:
  - Corporate security policies
  - Training with exams
  - Self assessments and risk guides
- Simplifies and documents end user training
- Unlimited use

AIG

CYBEREDGE RISK TOOL



AIG

COMPLIANCE/LEGAL CONSULTATION

Lewis Brisbois- John Mullen

Greenberg Traurig – Lori Nugent

Wilson Elser – Melissa Ventrone

Consultation options include:

- **Two complimentary hours from a specialized law firm to provide on building and executing an incident response plan, as well as ensuring an organization is compliant with regulatory standards.**
- **One complimentary hour from a forensic firm on what an organization's technical response plan should include.**
- **One complimentary hour from a vetted public relations firm to discuss an effective crisis communication plan to handle and mitigate the potential reputational and brand risk an organization would face in event of a breach.**

AIG

COMPLIANCE/LEGAL CONSULTATION

Building Cybersecurity Compliance by Design: Using the **CyberEdge® RiskTool℠** Makes It Easier

Now that your **CyberEdge RiskTool** has been installed, it is time to tailor its resources to fit your needs, maximizing the strength of your Cybersecurity Compliance Plan and supporting compliance documentation.

What Is a **Cybersecurity Compliance Plan**?

A **Cybersecurity Compliance Plan** is a formalized way to reduce the likelihood that the sensitive data you hold, or entrust to another person or business, will be exposed without authorization in violation of cybersecurity regulations and individual privacy rights. A strong Cybersecurity Compliance Plan also protects you should sensitive data become exposed.

The key to a strong Cybersecurity Compliance Plan is documentation that establishes that your privacy and security practices and procedures are reasonable and appropriate. For ease of reference, we call this information **Key Compliance Documentation**. When a data breach happens, Key Compliance Documentation makes it easier to satisfy regulators and avoid fines; in addition, it becomes more difficult for a plaintiff to prove negligence or reckless disregard for the privacy and security of sensitive information. In other words, Key Compliance Documentation protects your organization and its reputation if a data breach happens.

Once Key Compliance Documentation is in place, it is easy to access and use when sensitive information may have been exposed without authorization. Everyone will know what to do and how to do it effectively and efficiently, making it much easier to successfully respond to a potential or actual breach situation. When Key Compliance Documentation is used, regulatory fines are less likely, litigation outcomes are better and reputation is protected.

AIG

AIG VALUE PROPOSITION

End-to-End 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.

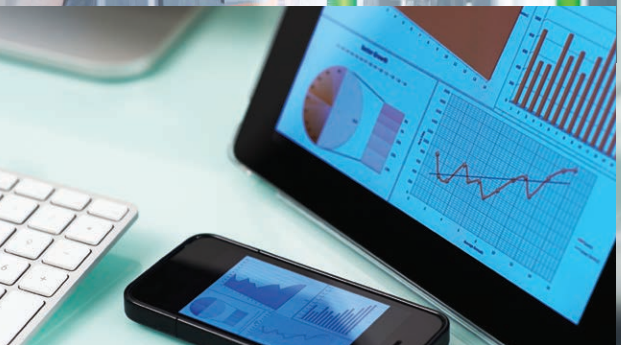
Loss Prevention Services	Insurance Coverage	Breach Resolution Team
Knowledge	Third-Party Loss Resulting From a Security or Data Breach	24/7 Guidance: 1-877-890-1259 Supported by **IBM**
Training and Compliance Solutions Powered by RiskAnalytics	Direct First-Party Costs of Responding to a Breach	Legal and Forensics Services
IT Security Assessment Services Powered by **IBM**	Lost Income and Operating Expense Resulting From a Security or Data Breach	Notification, Credit, and ID Monitoring
Consultation	Threats to Disclose Data or Attack a System to Extort Money	Crisis Communication Experts
Proactive Shunning Services Powered by RiskAnalytics	Online Defamation and Copyright and Trademark Infringement	Over 15 Years (Since 1999) Experience Handling Cyber-Related Claims

AIG

Bring on tomorrow

Bridget Sakach – Security & Privacy Specialist – Midwest Region

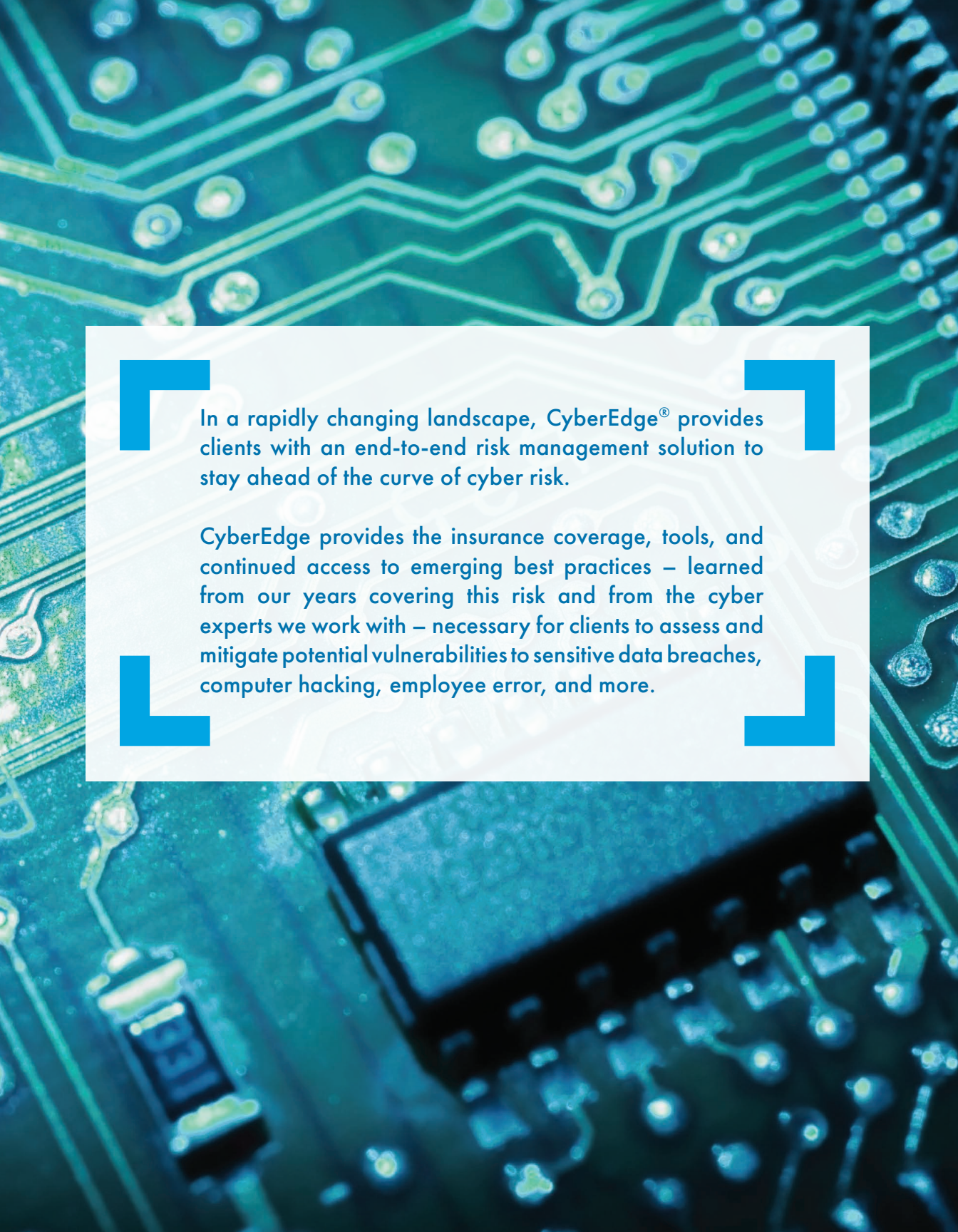
Tel +1 216 479 8951 | Cell +1 216 704 5852 | bridget.sakach@aig.com



CyberEdge®

End-to-End Cyber Risk Management Solutions

AIG



In a rapidly changing landscape, CyberEdge® provides clients with an end-to-end risk management solution to stay ahead of the curve of cyber risk.

CyberEdge provides the insurance coverage, tools, and continued access to emerging best practices – learned from our years covering this risk and from the cyber experts we work with – necessary for clients to assess and mitigate potential vulnerabilities to sensitive data breaches, computer hacking, employee error, and more.

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	Insurance Coverage	Breach Resolution Team
Education and Knowledge 	Third-Party Loss Resulting From a Security or Data Breach 	24/7 Guidance: **1-800-CYBR-345** 
Training and Compliance 	Direct First-Party Costs of Responding to a Breach 	Legal and Forensics Services 
Global Threat Intelligence and Assessment 	Lost Income and Operating Expense Resulting From a Security or Data Breach 	Notification, Credit, and ID Monitoring Call Center 
Shunning Services 	Threats to Disclose Data or Attack a System to Extort Money 	Crisis Communication Experts 
Expert Advice and Consultation 	Online Defamation and Copyright and Trademark Infringement 	Over 15 Years' Experience Handling Cyber-Related Claims 

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.

CyberEdge Mobile App for iPhone®, iPad®, and Android™

The CyberEdge Mobile App combines the latest cyber breach information, news, opinion, and risk analysis users want at their fingertips. With a sleek look and many features globalized, the app is the first-of-its-kind and available for iPhone, iPad, and Android.

Features include:

- Data Breach Threat Map that displays breaches occurring around the world, including information about breach notification laws in the U.S. state where the breach occurred.
- Claims narratives providing examples of real-world cyber breaches covered by CyberEdge.
- Breach calculator, allowing users to input their company's details to calculate the potential costs associated with a data breach.
- Majority of the content available in English, French, and Spanish.

RiskTool™ *Powered by RiskAnalytics*

The easy-to-use comprehensive web-based platform helps clients streamline the cybersecurity risk management process and address the human element of this risk.

Organizations can use RiskTool to:

- Build a culture of security through strong company policy and employee awareness.
- Educate employees with user-friendly training.
- Manage vendor security compliance with a streamlined process.
- Demonstrate appropriate diligence and compliance via fast, easy reporting and documentation.

Dark Net Intelligence *Powered by K2 Intelligence*

The ease and profitability of carrying out cyber crimes continues to increase for bad actors, especially with the continued shift organizations are making to operating in more of a digital, interconnected world.

K2 Intelligence can work with CyberEdge policyholders at preferred rates to stay apprised of what the latest chatter is inside the black hacker markets and forums known as the 'dark net' about their entity. The dark net is the staging ground, the safe haven, from which the most sophisticated cyber criminals launch their attacks.

K2 Intelligence mines the dark net for data using web crawlers and sophisticated human intelligence gathering. This type of customized intelligence is extremely valuable as organizations:

- Take a proactive approach in developing and refining their cybersecurity risk management program, ensuring the appropriate corporate governance standards and protocols are in place.
- Engage in M&A transactions. K2 Intelligence's experts and intelligence can be used to provide cybersecurity due diligence when organizations engage in a merger or acquisition.

Infrastructure Vulnerability Scanning *Powered by IBM*

Our qualified clients receive infrastructure vulnerability scanning powered by IBM. IBM conducts remote scanning for clients' web-facing external infrastructures, which helps to identify potential vulnerabilities that could be exploited by a remote hacker via the Internet. In addition, the infrastructure vulnerability scanning service:

- Detects and prioritizes hidden risks on public-facing network infrastructure.
- Provides a detailed view of a company's vulnerability status so clients can better track, understand, and report on their security posture.
- Prioritizes vulnerabilities so clients reduce their overall threat exposure.
- Includes unique reporting capabilities to help speed vulnerability identification and remediation.

BitSight Security Ratings

BitSight generates security ratings for organizations to measure and monitor their own network and those of their third-party vendors. The ratings are generated unobtrusively through BitSight's continuous measuring of externally observable data. Security ratings are based on evidence of the following:

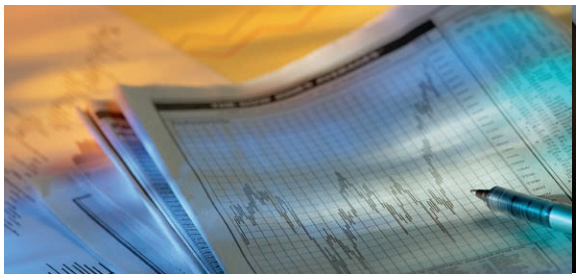
- Observed security events, or evidence of successful cyber attacks. This includes communication with botnets, spam, malware, and more.
- Diligence data points, or indicators of whether a company has taken steps to prevent an attack. This includes proper security configuration analysis.

Qualified CyberEdge insureds will be eligible to receive a complimentary BitSight Security Rating report to measure the organization's security performance. CyberEdge policyholders are also eligible for reduced rates on BitSight's products and services. Insureds can choose to arm themselves with daily ratings as part of their end-to-end cyber risk management program, allowing them to have insight into cybersecurity risk throughout their ecosystem.

Cybersecurity Maturity Assessment *Powered by RSA*

Insureds are eligible to receive a one-time six month complimentary pass to RSA's Governance, Risk, and Compliance (GRC) solution to assess their organization's cybersecurity risk. The assessment is built on the industry leading RSA Archer GRC solution.

- Leverages the NIST Cybersecurity Framework to assess an organization's cybersecurity maturity level and help identify areas of improvements in key functions.
- Upon completion of the assessment, an organization will have a view of gaps between their current and ideal risk posture.
- Insureds will have access to RSA's Advanced Cyber Defense (ACD) practice to provide operational expertise in closing the gaps and protecting the critical business assets.



Proactive Shunning Service *Powered by RiskAnalytics*

Qualified clients receive access to leading edge global threat intelligence and technology that isolates and shuns IP addresses currently being used by criminals. Before initiating an attack on a network, criminals first conduct reconnaissance to confirm that certain IP addresses are viable targets. Shunning prevents these criminal communications from reaching a network and confirming the IP addresses as viable targets. When the recon phase of the attack fails, the risk of follow-on intrusions is greatly reduced.

Shunning can also guard against attacks from within. If a computer on a network is already compromised by malware, shunning can prevent communication back to the criminal's command and control servers, effectively disarming the malware. Shunning occurs in real time at line speed, and it is scalable to protect a single location or a global enterprise.

Portfolio Analysis *Powered by Axio Global*

As a CyberEdge policyholder, clients can retain Axio Global (Axio) to assist in obtaining a holistic picture of their cyber exposure and more effectively harmonize their technological and operational controls with insurance coverage. Axio's method addresses the full range of potential cyber losses, including data theft, liability, property and environmental damage, bodily injuries, and operational disruption. Clients have access to the following services from Axio at reduced rates as a CyberEdge policyholder:

- One-day loss scenario workshop to estimate the financial impact of information technology and control systems loss scenarios customized for a client's particular needs and organized into a taxonomy that can be used to stress test insurance coverage.
- Analysis of a client's entire Property and Casualty insurance portfolio to identify how it would respond to a complex cyber event. Combined with the loss scenario workshop, this analysis stress tests a portfolio with realistic scenarios.
- Self-evaluation of a client's cybersecurity program based on the Cybersecurity Capability Maturity Model (C2M2), a recommended approach for deploying the NIST Cybersecurity Framework. A scoring report is generated and presented with the results of the evaluation. One of Axio's founders was the architect of the model and is well versed in helping organizations interpret the model content to achieve an effective and efficient cybersecurity program review.

Consultation

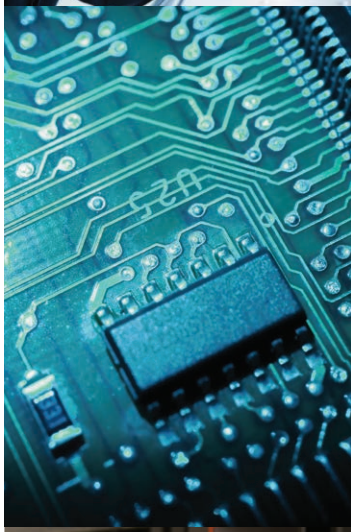
Clients have access to cybersecurity expert vendors and partners to help plan and prepare for a cyber breach. Consultation options include:

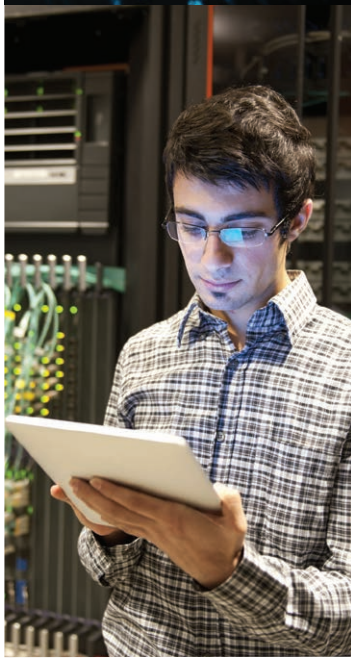
- Two complimentary hours from a specialized law firm to provide guidance on building and executing an incident response plan, as well as ensuring an organization is compliant with regulatory standards.
- One complimentary hour from a forensic firm on what an organization's technical response plan should include.
- One complimentary hour from a vetted public relations firm to discuss an effective crisis communication plan to handle and mitigate the potential reputational and brand risk an organization would face in the event of a breach.

Insurance Coverage

CyberEdge can provide companies with protection against the following:

- Third-party claims arising from a failure of the insured's network security or a failure to protect data. Insurance also responds to regulatory actions in connection with a security failure, privacy breach, or the failure to disclose a security failure or privacy breach.
- Direct first-party costs of responding to a security failure or privacy breach by paying costs of notifications, public relations, and other services to assist in managing and mitigating a cyber incident. Forensic investigations, legal consultations, and identity monitoring costs for victims of a breach are all covered.
- Business interruption caused by a network security failure by reimbursing for resulting lost income and operating expenses.
- Threats made against a company's computer network and confidential information by an outsider attempting to extort money, securities, or other valuables. Coverage includes monies paid to end the threat and the cost of an investigation to determine the cause of the threat.
- Liability faced by companies for content distributed on their website. Coverage is provided for numerous media perils including copyright infringement, trademark infringement, defamation, and invasion of privacy.





Breach Resolution Team

The CyberEdge Breach Resolution Team is ready to assist insureds as soon as they suspect a potential network breach. Our team has local presence supported by global resources, allowing our experts to manage unfolding events and quickly respond to inquiries.

If a breach is suspected to occur, insureds will be connected with our CyberEdge Breach Resolution Team with more than 15 years worth of experience in handling cyber-specific claims.

- Claims specialists have the authority to promptly make decisions and rapidly assist clients who may have just faced a breach.
- Since introducing cyber liability insurance in 1999, we have helped thousands of companies and more than twenty million individuals respond to a cyber attack.
- The breadth of our claims inventory means that we are uniquely positioned to identify and anticipate claim trends and settlement values.
- On average, our claims specialists have more than seven years of industry experience handling the most complex first-party and third-party cyber claims.

- 24/7 access to our call center for claim reporting and guidance supported by IBM.
- Single point of entry to report, acknowledge, and process claims in a timely fashion.
- Access to our local claims specialists on the ground around the world.
- Access to a panel of domestic and international attorneys with local expertise in handling cyber claims.

Backed by the strength of our extensive vendor network, the CyberEdge Breach Resolution Team provides the additional layer of support an IT department needs to face a cyber attack.

- Insureds have access to an IBM-supported hotline for IT professionals to consult on identifying key indicators of a breach.
- IBM and our expert network of legal firms, forensic investigators, public relations firms, and more offer immediate support for our insureds facing a cyber attack, anytime and anywhere.
- When a breach event occurs, time is of the essence. Having a response plan in place with access to third-party resources will help you efficiently and cost-effectively respond to and recover from a breach.

Cyber Risk Travels the World

Through our global service platform Passport, clients are provided an efficient and seamless way to stay ahead of the curve of cyber risk. Add the expertise of our local teams who have the know-how in the places where you do business. Count on the CyberEdge Breach Resolution Team for responsive guidance and assistance services that follow the sun. Our end-to-end risk management solution knows no borders.

Better, Faster, and More Efficient Global Protection

Passport is a simple, effective means to far-reaching global advantages, including:

- Coverage that is admitted locally and in sync with local laws, regulatory requirements, language, and customs.
- Access to local experts in underwriting, claims, and litigation management.
- Easy to understand coverage, coordinated worldwide.

A Less Complex Way to Address Global Cybersecurity Exposure

Passport makes securing the necessary protection against cyber risk around the world as simple as possible.

- A client receives one proposal detailing the terms of its global cyber program, including the worldwide policy and any requested locally admitted policies.
- The outlined coverage is accepted and it is done.
- Appropriate local policies are issued through our local offices around the world. Local policies are crafted in accordance with local regulations, industry practices, and exposures.[1]

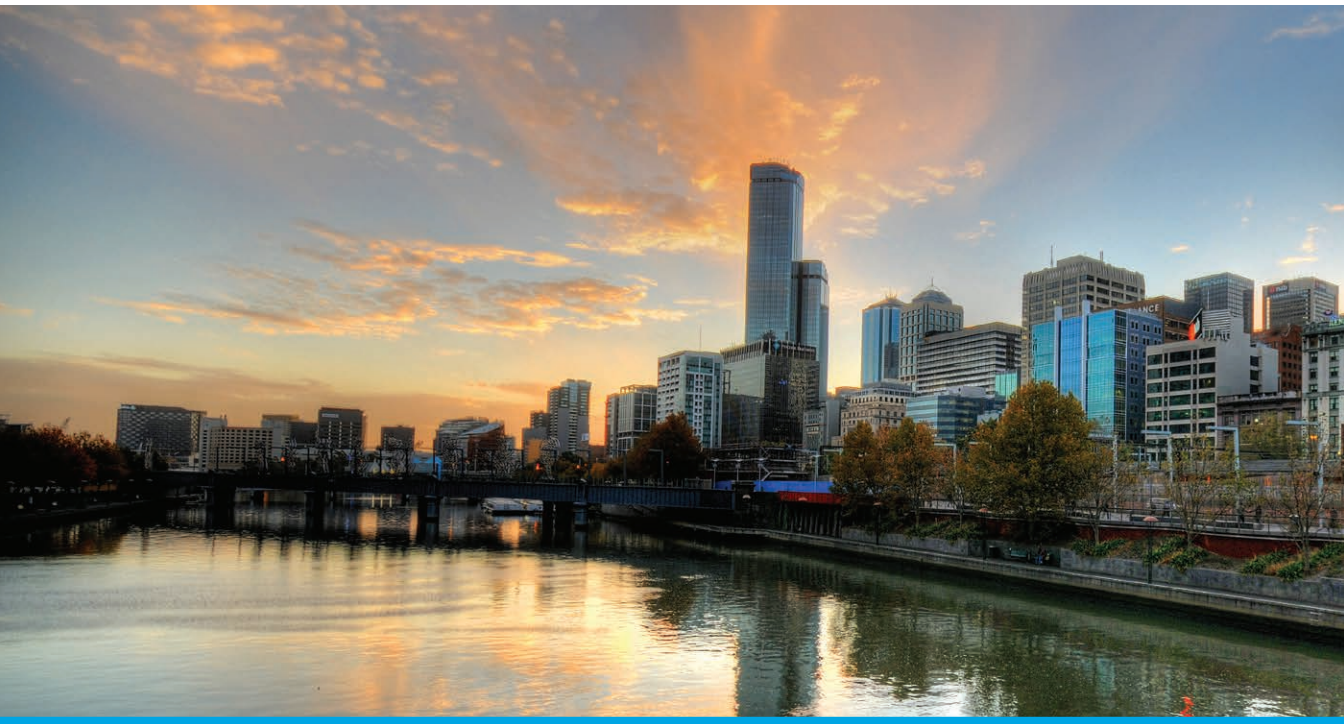
[1]Limits are subject to capacity management; certain countries may limit the availability of either a single aggregate or a separate world limit.

Passport for CyberEdge Destinations

- Australia
- Austria
- Bahrain
- Belgium
- Brazil*
- Bulgaria
- Canada
- Chile
- Colombia
- Cyprus
- Czech Republic
- Denmark
- Ecuador
- Finland
- France
- Germany
- Greece
- Hong Kong
- Hungary
- Ireland
- Israel
- Italy
- Japan
- Kuwait
- Lebanon
- Luxemburg
- Malaysia
- Mexico
- Netherlands
- New Zealand
- Norway
- Oman
- Panama
- Philippines
- Poland
- Portugal
- Puerto Rico
- Qatar
- Romania
- Russia*
- Singapore
- Slovakia
- Spain
- South Africa
- South Korea
- Sweden
- Switzerland
- Taiwan
- Turkey
- UAE
- United Kingdom
- United States
- Uruguay

New destinations are added constantly, so please check with a Passport representative for more information.

*Special handling and additional premium required for Brazil and Russia.



To learn more about CyberEdge:

Email us at CyberEdge@aig.com • Visit us at www.aig.com/CyberEdge

Download the CyberEdge Mobile App

Available on the App Store

ANDROID APP ON Google play

Follow CyberEdge

Follow@AIGinsurance

AIG Bring on tomorrow

American International Group, Inc. (AIG) is a leading global insurance organization serving customers in more than 100 countries and jurisdictions. AIG companies serve commercial, institutional, and individual customers through one of the most extensive worldwide property-casualty networks of any insurer. In addition, AIG companies are leading providers of life insurance and retirement services in the United States. AIG common stock is listed on the New York Stock Exchange and the Tokyo Stock Exchange.

Additional information about AIG can be found at www.aig.com | YouTube: www.youtube.com/aig | Twitter: @AIGinsurance | LinkedIn: http://www.linkedin.com/company/aig

AIG is the marketing name for the worldwide property-casualty, life and retirement, and general insurance operations of American International Group, Inc. For additional information, please visit our website at www.aig.com. All products and services are written or provided by subsidiaries or affiliates of American International Group, Inc. Products or services may not be available in all countries, and coverage is subject to actual policy language. Non-insurance products and services may be provided by independent third parties. Certain property-casualty coverages may be provided by a surplus lines insurer. Surplus lines insurers do not generally participate in state guaranty funds, and insureds are therefore not protected by such funds.

Apple, the Apple logo, iPhone and iPad are trademarks of Apple Inc., registered in the U.S. and other countries. App Store is a service mark of Apple Inc. Android and Google Play are trademarks of Google Inc.

No warranty, guarantee or representation, either express or implied, is made as to the appropriateness or sufficiency of any product, service or provider described herein for any specific organization or purpose. Use of the service providers discussed herein in no way guarantees any particular result, including the avoidance of loss, the fulfillment of any obligations under any insurance policy or contract or compliance with any law, rule or regulation. The information provided herein should not be construed as business, risk management or legal advice or opinion.

04/15

Library of Congress Summary for the Data Accountability and Trust Act (H.R. 580)

The summary below was written by the Congressional Research Service, which is a nonpartisan division of the Library of Congress.

1/28/2015--Introduced.

Data Accountability and Trust Act

Requires the Federal Trade Commission (FTC) to promulgate regulations requiring each person engaged in interstate commerce that owns or possesses data containing personal information to establish specified security policies and procedures to treat and protect such information.

Requires the regulations to include methods for disposing of both electronic and nonelectronic data.

Requires information brokers to submit their security policies to the FTC in conjunction with a notification of a security breach notification or upon the FTC's request. Authorizes the FTC to conduct information security practices audits of brokers who have had a security breach or require such brokers to conduct independent audits.

Requires information brokers to: (1) establish procedures to verify the accuracy of information that identifies individuals, (2) provide to individuals whose personal information it maintains a means to review it, (3) place a conspicuous notice on the Internet instructing individuals how to request access to such information, and (4) correct inaccurate information.

Directs the FTC to require information brokers to establish measures which facilitate the auditing or retracing of access to, or transmissions of, any data containing personal information.

Makes it unlawful for information brokers to obtain or disclose personal information by false pretenses (pretexting).

Requires such person to notify the FTC and affected individuals of information security breaches. Sets forth requirements concerning such notification, including method of notification requirements and timeliness requirements. Allows an exemption from notification requirements if such person determines that there is no reasonable risk of identity theft, fraud, or other unlawful conduct.

Preempts state information security laws.

Summary: S.177 (Data Security and Breach Notification Act of 2015) — 114th Congress (2015-2016)

Bill summaries are authored by the Congressional Research Service

Shown Here:
Introduced in Senate (01/13/2015)

Data Security and Breach Notification Act of 2015

Requires the Federal Trade Commission (FTC) to promulgate regulations requiring commercial entities, nonprofit and for-profit corporations, estates, trusts, cooperatives, and other specified entities that own or possess data containing personal information (covered entities), or that contract to have a third-party maintain or process such data for the entity, to implement information security policies and procedures for the treatment and protection of personal information.

Establishes procedures to be followed in the event of an information security breach. Requires a covered entity that discovers a breach to notify the FTC (unless the covered entity has already notified a federal entity designated by the Department of Homeland Security [DHS] to receive such information) and affected individuals. Sets forth requirements concerning such notification, including methods of notification and timeliness requirements. Allows an exemption from notification requirements if such entity reasonably concludes that there is no reasonable risk of identity theft, fraud, or other unlawful conduct. Establishes a presumption that there is no such risk for encrypted data.

Directs DHS to designate a federal entity that covered entities would be required to notify if a security breach involves: (1) the personal information of more than 10,000 individuals, (2) a database containing the personal information of more than 1 million individuals, (3) federal government databases, or (4) the personal information of federal employees or contractors known to be involved in national security or law enforcement.

Requires the designated entity to provide each notice it receives to:

- the U.S. Secret Service;
- the Federal Bureau of Investigation;
- the FTC;
- the U.S. Postal Inspection Service, if mail fraud is involved;
- attorneys general of affected states; and
- appropriate federal agencies for law enforcement, national security, or data security purposes.

Sets forth enforcement provisions for the FTC, state attorneys general, and the Attorney General.

Establishes criminal penalties of a fine, imprisonment for up to five years, or both, for concealment of a security breach that results in economic harm of at least $1,000 to an individual.

The White House
Office of the Press Secretary
For Immediate Release
January 12, 2015

FACT SHEET: Safeguarding American Consumers & Families

Today, President Obama will build on the steps he has taken to protect American companies, consumers, and infrastructure from cyber threats, while safeguarding privacy and civil liberties. These actions have included the President's 2012 comprehensive blueprint for consumer privacy, the BuySecure initiative—launched last year— to safeguard Americans' financial security, and steps the President took earlier this year by creating a working group of senior administration officials to examine issues related to big data and privacy in public services and the commercial sector.

In an increasingly interconnected world, American companies are also leaders in protecting privacy, taking unprecedented steps to invest in cybersecurity and provide customers with precise control over the privacy of their online content. But as cybersecurity threats and identity theft continue to rise, recent polls show that 9 in 10 Americans feel they have in some way lost control of their personal information — and that can lead to less interaction with technology, less innovation, and a less productive economy.

At the Federal Trade Commission offices today, President Obama will highlight measures he will discuss in the State of the Union and unveil the next steps in his comprehensive approach to enhancing consumers' security, tackling identity theft, and improving privacy online and in the classroom. These steps include:

Improving Consumer Confidence by Tackling Identity Theft

- **The Personal Data Notification & Protection Act**: The President is putting forward a new legislative proposal to help bring peace of mind to the tens of millions of Americans whose personal and financial information has been compromised in a data breach. This proposal clarifies and strengthens the obligations companies have to notify customers when their personal information has been exposed, including establishing a 30-day notification requirement from the discovery of a breach, while providing companies with the certainty of a single, national standard. The proposal also criminalizes illicit overseas trade in identities.

* * *

SEC. 1. DEFINITIONS.

In this title, the following definitions shall apply: * * *

(b) BUSINESS ENTITY.—The term "business entity" means any organization, corporation, trust, partnership, sole proprietorship, unincorporated association, or venture, whether or not established to make a profit.

* * *