THE EVOLUTION OF CYBER RISK

insured.®

Cyber attacks or data breach incidents seem to make headlines daily. Although these events may feel commonplace, their triggers are changing, as are the risk management strategies to address them. ACE has handled data breach incidents and underwritten exposures for policyholders for more than 15 years, and has cataloged a considerable amount of loss data. A careful analysis of this proprietary data shows a shift in data breach triggers over the years...and a correlating rise in the cost to investigate these incidents. What ACE has learned from past cyber incidents can help our insureds take steps to prevent or mitigate future ones. Understanding the threats and proactively taking action can help you protect your organization's network, balance sheet and reputation.

ACE HISTORY

ACE has extensive experience in this market:

- Launched first cyber product in 1998
- Helped policyholders notify over 300 million individuals of a privacy breach
- Experienced more than 20% growth in cyber premium year over year since 2007

GENERAL CYBER MARKET

$2 billion
Cyber insurance market is estimated at $2 billion in gross written premiums[1]

2.6 billion
Currently 2.6 billion Internet users - compared to less than 1 billion 10 years ago[2]

200%
Amount of data online doubles every two years[3]

DATA BREACH TRIGGERS

Hacking captures headlines...but it's only part of the problem. Human error and other triggers can also have a significant impact on your security.

TRIGGER	
Lost or stolen device	20%
Network security attack	25%
Rogue employee	15%
Human error	16%
Company policies	9%
Paper	6%
Software error	3%
Unknown	6%

TYPE OF LOST OR STOLEN DEVICE

70% Laptop
28% Tape/CD/USB
2% Smartphone

11%
of all cyber claims involved a liability suit

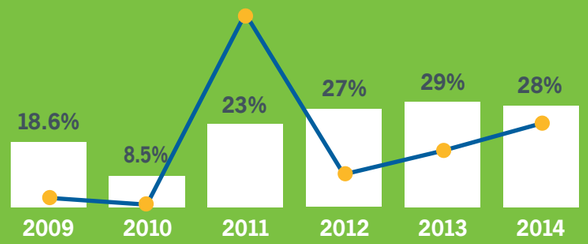
TRIGGERS ARE CHANGING AND FORENSIC COSTS ARE GOING UP

ACE's data shows an increase in criminal activity...and this is likely to become a larger risk factor as loss mitigation services address the other triggers:

- Hacking and rogue employees were the cause of 40% of the data breaches insured by ACE in 2014 – up 10% since 2009
- Lost/stolen devices were the cause of only 20% of data breaches in 2014 – down from 41% in 2008
- Former employees account for 24% of insider misuse[4]
- Financial incentive is the motive of 72% of insider misuse[5]
- Top assets affected by insider misuse are desktops (26%) and databases/servers (25%)[6]

As criminal activity increases, so do the forensics costs. Why? Because criminal incidents are more complex in the nature of the attack and malware incidents are more costly to investigate.

As shown in the graph below, the cost of investigating a breach once it does occur is escalating substantially year over year.



DATA BREACH TEAM

ACE policyholders have access to ACE's Data Breach Team, a pool of independent third-party professional service providers who have the capabilities and experience to help organizations and businesses execute their data breach response. When combined with one of the Data Breach Team Endorsement options, ACE's Data Breach Team bridges the gap between risk transfer and purchased loss control, creating a comprehensive risk management program for privacy, data breach and network security risk.

Regulatory Fines =

$0 Policyholders using ACE's Data Breach Team

$4 million Policyholders not using ACE's Data Breach Team

HOW CAN YOU PROTECT YOUR DATA?

ACE has thoroughly analyzed our proprietary claims data to identify the most common threat trends and ultimate financial loss, and is pleased to offer the following recommendations to help you protect your network, balance sheet and reputation.

CORE

- Identify and address the information that needs to be secured
- Encrypt all private and/or sensitive information
- Separate networks into multiple segments to minimize access to sensitive information
- Establish ongoing compliance management procedures
- Develop a thoroughly tested incident response plan

TACTICAL

- Deploy an anti-malware solution across all network devices (e.g., PCs, laptops and servers)
- Implement an intrusion detection solution that provides an active response to persistent threats
- Enforce proper user account access controls and privileges (e.g., password management)
- Patch and configure systems based on published vulnerabilities
- Prevent unauthorized access to information on mobile devices

CULTURAL

- Establish a cyber-risk management culture from the top down
- Educate employees on their responsibilities for protecting information
- Conduct regular system security reviews of vendors and others who access your network
- Clearly document and catalog all implemented security solutions to ensure proper level of innovation against current threats
- Participate in security leadership communities outside of your company, such as industry associations

LEARN MORE

www.acegroup.com/us/privacyprotection

CONTACT US

ACE USA
436 Walnut Street
Philadelphia, PA 19106,
United States
www.acegroup.com/us

ACE Group is one of the world's largest multiline property and casualty insurers. With operations in 54 countries, ACE provides commercial and personal property and casualty insurance, personal accident and supplemental health insurance, reinsurance and life insurance to a diverse group of clients. ACE Limited, the parent company of ACE Group, is listed on the New York Stock Exchange (NYSE: ACE) and is a component of the S&P 500 index. Additional information can be found at www.acegroup.com.

This information is a summary only. Insurance is provided by insurance companies within ACE Group. All products or services may not be available in all jurisdictions. Surplus lines products are only available through licensed surplus lines brokers.

04/2015

Endnotes:

Unless otherwise referenced, all data is derived from ACE's proprietary claims data as of March 2015.

1 Hemenway, Chad. Guy Carpenter: cyber attacks, terrorism among most serious emerging risks. AdvisenRiskNetwork.com (2014). http://www.advisenrisknetwork.com/2014/09/17/guy-carpenter-cyber-attacks-terrorism-among-serious-emerging-risks/

2 Marks, Gene. Why The Anthem Breach Just Doesn't Matter Anymore. Forbes.com (2015). http://www.forbes.com/sites/quickerbettertech/2015/02/09/why-the-anthem-breach-just-doesnt-matter-anymore/

3 Gantz, John & Reinsel, David. (2012). The Digital Universe in 2020: Big Data, Bigger Digital Shadows, and Biggest Growth in the Far East. (IDC Go-to-Market Services). Framingham, MA

4 Verizon. (2014). 2014 Data Breach Investigations Report. Retrieved from: http://www.verizonenterprise.com/DBIR/2014/

6 Ibid.

7 Ibid.

ACE insured.®