CINCO DE CYBER

Gareth Tungatt (Ascent Underwriting LLP),

SESSION 1

Setting the Scene

ASCENT™ UNDERWRITING

WHAT IS CYBER?

Cyber- is derived from "cybernetic," which comes from the Greek word κυβερνητικός meaning *skilled in steering or governing*. It is mainly used in the terms *cyberspace*, *cyberlaw*, *cyberbullying*, *cybercrime*, *cyberwarfare*, *cyberterrorism*, *cybersex*, and *cyberdelic* among others. Although it is more commonly used to describe policies and politics regarding computer systems and networks (as demonstrated in the above cases) but it is also widely used by many information technology industries. Cyber is now considered as a recent term in the internet era.

Non Specific?

ASCENT™
UNDERWRITING

WHAT'S IN A NAME?

- Cyber Risk?? – Non Specific
  - Network Security
  - Data Breach
  - IT Insurance
  - Enterprise risk
  - Breach Coverage

ASCENT™
UNDERWRITING

WHAT IS “CYBER” RISK

Exposures emanating from computer networks and the internet

“non physical”

ASCENT™
UNDERWRITING

Isn't it just breach response?

- Policies now wider in coverage
- Fully comprehensive e-commerce policies
- Coverage being expanded
  - Crime / social engineering
  - Rep Harm
  - BI
  - Outside Vendors
  - Bodily injury
  - Physical damage

ASCENT™ UNDERWRITING

CYBER LIFE-LINE

- 1990's Focused on general merits of cyber insurance
  - Business perspective more apparent
  - Hindered by exposures and Y2K
- 1998 – First Policies Written! First Party
  - Hindered by exposures and Y2K
- 2000 – Technology forms
  - Included "cyber"
  - Limited coverage
  - Lack of legislation
- 2004 – US privacy liability enacted
- 2006 – Insurance Market Responds – Privacy Liability
  - Many false dawns
  - Unsophisticated buyers
  - Uncertainty of coverage
  - Insurer fear of entering a new market
  - Conservative forecast in 2002, which predicted a global market for cyber-insurance worth $2.5 billion in 2005, turned out to be five times higher than the size of the market in 2008 (three years later).
- 2009 – New forms start to take shape
  - Second generation of coverage developed
  - Lloyd's leads the way
- 2009>2017 – Full non-tangible risks products developed
  - Over 50 insurers competing in this space
  - Cyber insurance premiums expected to grow from around $2 billion in 2015 to an estimated $20 billion or more by 2025

ASCENT™
UNDERWRITING

Emergence of Coverage

- 10yrs + Underwriting experience
- Soft market
- Short tail business
- Claims made
- Profitable?
- Emerging Market

Lots of new capacity – coverage not always comprehensive

ASCENT™ UNDERWRITING

Aggregation concerns

- Major operating platform could again be exposed to vulnerability.
- Malicious code
- Terrorism
- Large scale network breach on a cloud provider
- Natural Disaster
- Emerging legislation
- Terrorism
- National outages

ASCENT™ UNDERWRITING

OPERATING IN THE 21ST CENTURY

Critical Networks

- Increased reliance on connectivity of IT Networks (Internet)
- E-commerce operations
- Automated Billing
- Data Processing
- On-Line offices and booking system
- Paperless environment
- Critical and Sensitive Personally Identifiable Information (PII) and Data
- Point of Sale (PCI Information)

ASCENT™ UNDERWRITING

EXPOSURES

First Party Exposures

- Your own losses

Third Party Exposures

- Your liability to others

ASCENT™
UNDERWRITING

AREAS OF EXPOSURE – FIRST PARTY

Risk to own networks

(automated real-time business critical networks)

- System Failure
- Forensic Costs
- Customer Notification / Credit Monitoring
- Crisis Management
- Damage to Reputation
- Regulatory Actions/Awards
- Increased Cost of Working
- Loss of Business Revenue (BI)

ASCENT™
UNDERWRITING

AREAS OF EXPOSURE – THIRD PARTY

Third Party Legal Liability

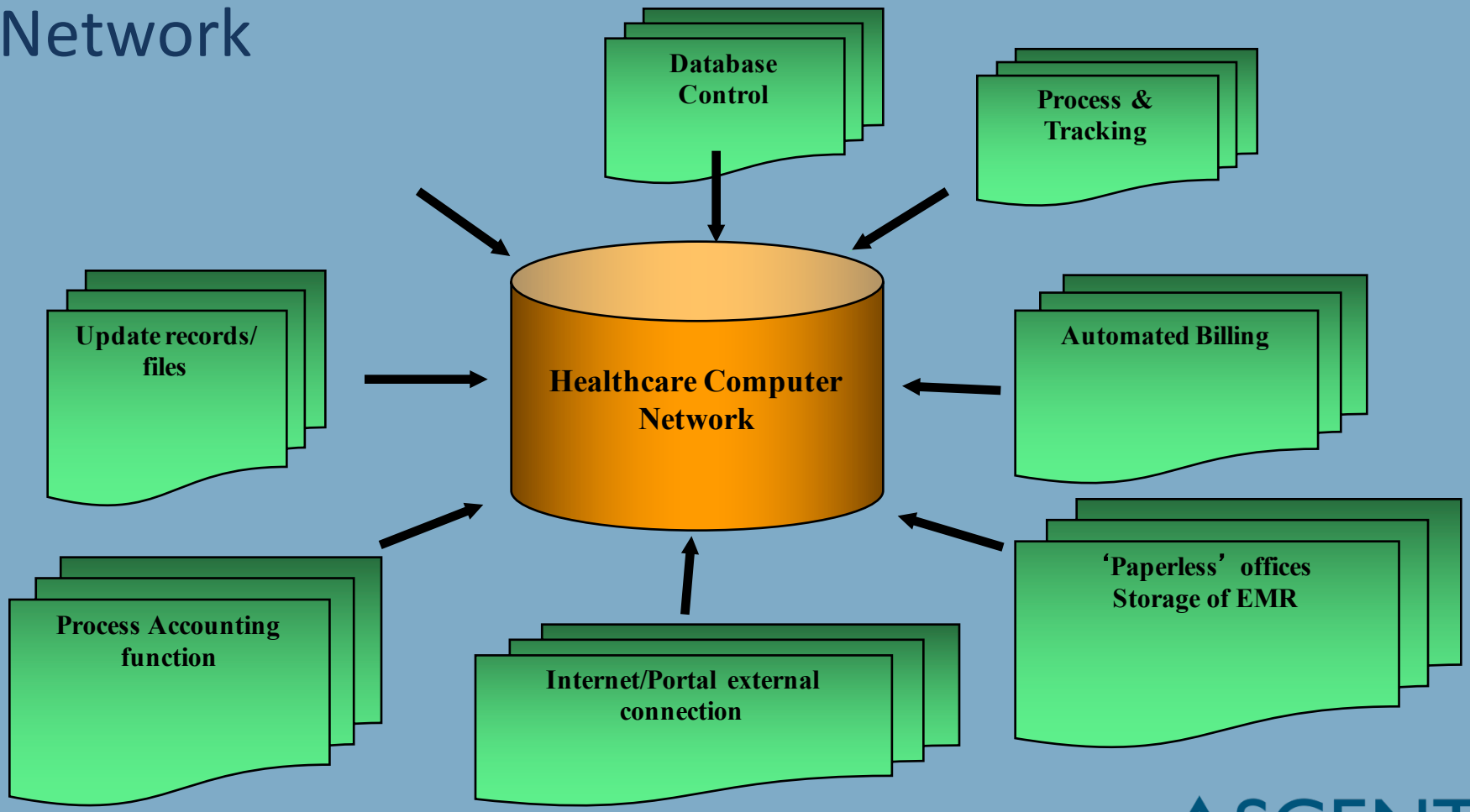
(Many of the same legal responsibilities as a publisher)

- Third Party Actions (Class)
- Breach of Confidentiality
- Invasion of Privacy Rights
- Defamation, Libel and Slander (Media)
- Misleading Advertising
- Virus Transmission

ASCENT™
UNDERWRITING

NETWORK FUNCTIONALITY

Network



ASCENT™ UNDERWRITING

Isn't it just breach response?

- Policies now wider in coverage
- Fully comprehensive e-commerce policies
- Coverage being expanded
  - Crime / social engineering
  - Rep Harm
  - BI
  - Outside Vendors
  - Bodily injury
  - Physical damage

ASCENT™ UNDERWRITING

GAPS IN TRADITIONAL COVERAGE

- Many practices are NOT fully insured for their “cyber” exposures

- The trigger for most standard “property” or “BI” policies is physical loss, or damage to tangible property

ASCENT™
UNDERWRITING

SESSION 2

REAL LIFE EXAMPLES OF ACTUAL DATA BREACHES

ASCENT™
UNDERWRITING

CRIMINAL ACTIVITY – FINANCIAL GAIN

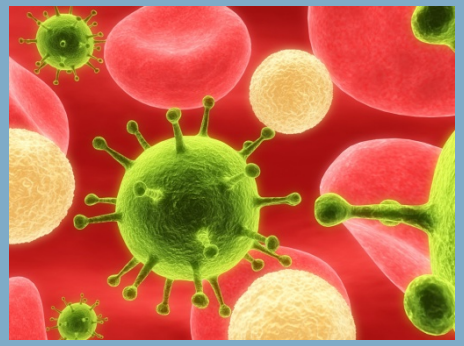
Criminals use the internet as a launch pad or channel for their activity (little regulation)

- Cyber Extortion (blackmail demands)
- Phishing / Pharming
- Fraud

ASCENT™ UNDERWRITING

Electronic Security Breaches

- Hackers
- Time or logic bombs
- Trojan Horses
- Computer Viruses



ASCENT™
UNDERWRITING

Internal Sabotage

- Malicious Insiders

- Disgruntled Employees causing system sabotage

ASCENT™ UNDERWRITING

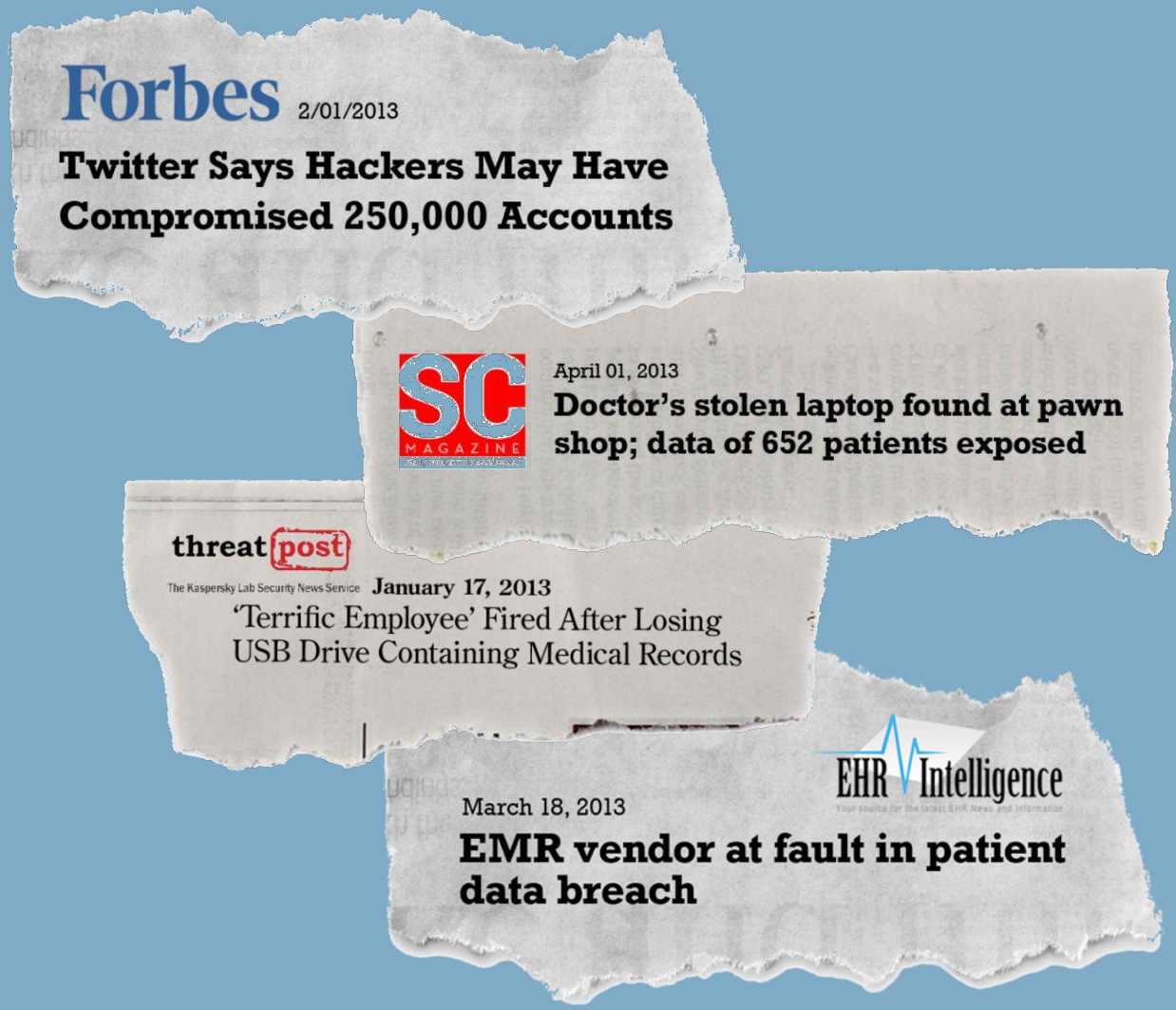
Traditional Risks

- Accidental Damage / Destruction / Loss
- Lost paper files
- Programming Error
- Human Error
- Natural Disaster

ASCENT™
UNDERWRITING

BREACH SCENARIOS – REAL CASES

1. Hacking
2. Stolen Laptop
3. Lost USB
4. Breach Caused by Vendor



ASCENT™ UNDERWRITING

BREACH SCENARIOS – REAL CASES

5 Hard Drive Disposal

6 Document Disposal

7 Employee Error

8 Unauthorized Access

41 WMGT
MACON • WARNER ROBINS
January 09, 2013
Davis: Personal Info Left on City Computer Hard Drives Sold to Computer Repair Shop

LOCAL NEWS 8 abc | KIDK 3 NEWS | KXPI FOX
Dec 19, 2012
Children's medical records found in Dumpster to be shredded

September 17, 2012
2 Investigators: Clinic's Email Blunder Compromises Privacy Of AIDS Patient
CHICAGO (CBS) — A local medical facility is in hot water with patients over a mass e-mail sent this summer.
cbs2chicago.com

StarTribune | local January 16, 2013
5,000 alerted of records breach in abuse of drivers' data by DNR employee
Worker's unauthorized search of thousands of records is largest so far and led to state alerts.

ASCENT™ UNDERWRITING

Healthcare Data Breaches

HIPAA breach is bad news for 729,000

Health system now to 'expedite' encryption

Advocate Medical Group Notifies Patients, Offers Protection Following Office Burglary

Advocate Medical Group (AMG) leaders announced today that they have been working internally and with law enforcement to investigate the July 15 burglary of an Advocate administrative office in Park Ridge, Ill., that may have affected their patients.

Fort Worth hospital reports huge data breach

Indiana Agency Notifies 188,000 of Breach

Business Associate's Programming Error Apparent Cause

Site flaw puts patient data on Google

Vendor oversight brings HIPAA breach to 32,000

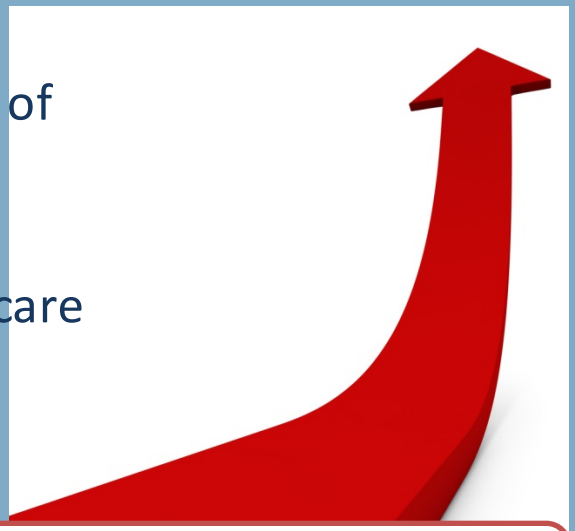
New health data breach at Lucile Packard Children's Hospital

ASCENT™
UNDERWRITING

New Findings

Medical Identity Theft Is On the Rise*

- Medical identity theft accounted for 43% of all identity theft reported in 2013
- Reports estimate that somewhere in excess of 250 million people's medical records have been breached since 2013
- 100% increase in criminal attacks on healthcare organizations since 2015



What Are the Contributing Factors?

ASCENT™ UNDERWRITING

Privacy Risk

- **Computer Hacks**: Out of 855 hacking incidents, two-thirds occurred at companies with 11 to 100 employees[1]
- **Computer Outages**: A company that experiences a computer outage lasting more than 10 days will never fully recover financially. 50% will be out of business within five years[2]
- **Data Loss**: 70% of small firms that experience a major data loss go out of business within a year[3]
- **Disaster**: 80% of companies that do not recover from a disaster within one month are likely to go out of business[4]
- **Preventable**: 97% of data breaches are avoidable through simple or intermediate controls

Increase Use of Technology

Why data breaches may occur

Transmit PHI data via patient portals or personal healthcare record

Mobile access to Electronic Health Records

Inappropriate data access

ASCENT™ UNDERWRITING

Breach Response Costs

Legal

$300 - $600 per hour

Forensics

$250 - $600 per hour

Crisis Management

$150 per hour or legal rate

Notification

$1 -$3 per letter

Call Handling

$7 - $25 per call

Credit & Fraud Monitoring

$8 - $75 per person

Identity Theft Resolution

$400 per case

ASCENT™
UNDERWRITING

How changes to HIPAA complicate things

- How far downstream do Business Associates go?

  Changes to HIPAA memorialized in the Final Omnibus rule extend the Business Associate relationship much farther than previously thought.

- Movement to Electronic Health Records

  If you haven't switched to EHR's YET- you will be soon.

- Data Security Breach Notification

  New cemented obligations around notification to regulators, consumers, and even media following a breach of Protected Health Information.

*HealthIT.gov

ASCENT™ UNDERWRITING

CYBER CLAIM SCENARIOS

A part time hospital employee gained unauthorized access to confidential electronic patient records and discussed with co-workers an individual's HIV status. Individual sued hospital for lack of adequate IT security measures in protecting digital patient records. Hospital held liable for $250,000. Additional $85,000 spent on defense.

Medical records of woman posted on Internet without her knowledge or consent a few days after she was treated at a religiously affiliated medical center following complications from an abortion at a woman's health clinic. Anti-abortion activists posted records on line with photo of woman being transferred from clinic to hospital. Woman sued hospital, alleging it released her medical records without authorization. Defense costs and case settlement expenses exceeded $500,000.

ASCENT™
UNDERWRITING

BREACH OF PHYSICAL MEDICAL RECORDS – HEALTHCARE PROVIDER

This particular insured contracted with an outside vendor to dispose of old medical records in an incinerator. A potential privacy breach was suffered after the Insured discovered that the vendor disposed of private medical documents (in the care and custody of the insured) in a dumpster with the regular rubbish, rather than incinerating the documents separately. The information contained within the documents may have included names, addresses, birth dates, laboratory report results, and insurance information. The Insured indicated that some of the documents may have also included social security numbers.

Breach counsel were retained for the Insured. Breach counsel further investigated the facts and was able to conclude that the medical documents were properly disposed of in an incinerator, and breach counsel obtained attestations from several individuals of this fact. As such, this was not a reportable breach. Breach counsel prepared a memo for the Insured's file documenting the investigation, and has now closed the file in connection with this matter. Breach counsel's fees and costs totalled $5,000.

Had the documents not been incinerated, notification would have been necessary to all individuals who had their personal information potentially compromised by the event.

ASCENT™
UNDERWRITING

RANSOMWARE – PRIMARY CARE OFFICE

Ransomware was installed on the insured's computer network, which resulted in their files being externally encrypted. The Insured subsequently received a message with a ransom demand of 2.5 Bitcoin (approximately $1,500). Fortunately, the insured backs up all files daily. As a result, they were in a position to wipe their server clean of the malware and restore their data from the backups.

Breach counsel was retained to assess the potential need to notify any individuals who may have had personally identifiable information compromised. A forensics company, Crypsis Group, was retained to conduct a forensic examination of the event at a cost of approximately $20,000 (one server was impacted).

Approximately 1,000 patients to be notified as a result of this event. In addition to the cost of forensics, breach counsel incurred approximately $15,000, and notification and credit monitoring services totalled approximately $8,000.

ASCENT™
UNDERWRITING

STOLEN LAPTOP – HEALTHCARE PROVIDER (MULTI SPECIALTIES)

This insured utilizes a third party vendor to administer its billing and collecting. The insured has a valid Business Associate Agreement in place with vendor. The Insured was notified by the vendor that a laptop had been stolen from an employee on February 25, 2016.

The information on the laptop included patient names, name of the surgery centre, name of the insurance carrier and the case identifier. No social security numbers or credit card information were present on the laptop. The laptop in question was password protected at two levels, and certain files stored locally on the laptop were encrypted. Despite this, it was not clear that all healthcare information was encrypted. Approximately 19,500 individuals were impacted in 45 different states across the US. Individual located in Guam, Mexico and Canada were also infected.

The insured was required to notify Health and Human Services' Office of Civil Rights ("OCR") within 60 days as it involves more than 500 individuals.

Breach counsel was duly retained and a third party vendor retained to provide notification to the approximately 19,500 individuals. Breach counsel costs incurred totalled $30,734. Notification costs totalled $50,400 and the third party vendor ultimately agreed to indemnify the insured for the $50,400 in notification costs, with the assistance of breach counsel.

ASCENT™
UNDERWRITING

Loss of Data - Hospital

The insured's computer system crashed and resulted in the insured being unable to use hard drives and access data. As a result, the insured was only able to see approximately one quarter of the patients they normally see as they could not access online scheduling.

The insured lost data as a direct result of the computer crash. The lost data included clinical information and financial information on their practice management system. Data could not be recovered from backup tapes because the backup was not running properly. There was no indication any of the lost data has been compromised by an unauthorized entity. The Insured sent the hard drive to a third party vendor who was able to recover the lost data at a cost of $18,000.

The Insured is currently calculating loss of business income as a result of the outage.

ASCENT™
UNDERWRITING

THIRD PARTY PRIVACY CLAIM – MEDICAL CLINIC

This particular Insured employed a medical assistant who, while employed by the insured, used her login credentials to log into hospital database from the insured's computer network in order to access a patient's medical records without authorization and for personal reasons.

The patient discovered the breach and sued the insured and the medical assistant in Oklahoma state court for negligence and invasion of privacy. The patient claimed damages in excess of $75,000 in the lawsuit, and ultimately makes as settlement demand of $50,000. Defence costs were also incurred to defend the suit.

ASCENT™
UNDERWRITING

Network Security Claim - Clinic

Ransomware was installed on the Insured's computer network, which resulted in files being externally encrypted. One of the Insured's employees then received a message with a ransom demand of 2.5 Bitcoins (approximately $1,100). The insured paid the ransom and received a key to unlock the files. The key only unlocked some of the files, while others remained encrypted.

After payment of the ransom did not decrypt all of the files, the insured retained an IT solutions firm to assist in restoring the data. Breach counsel was also retained to assess the potential need to notify any individuals who may have had personally identifiable information compromised. Forensics decrypted all of the previously encrypted files and has wiped the infected servers clean and have removed all ransomware, restoring the Insured's data.

Forensics work and breach counsel fees covered under the policy. If notification is necessary, notification expenses would also covered under the policy.

ASCENT™
UNDERWRITING

HACK – HOSPITAL

The insured discovered that servers were hacked by an unauthorized entity using a prior employee's identification. The servers housed the Insured's membership database including encrypted credit card accounts.

A leading Forensics firm was retained to do an initial inspection and analysis of the Insured's servers to check for evidence of malware, and review the logs to see if data was exfiltrated. This investigation revealed that an attacker had accessed the Insured's App-1 server numerous times. At least two of the point of sale devices were compromised by memory scraping malware. Credit card numbers and cardholder names were copied, and the data may have been exfiltrated to the attacker. Forensics also discovered URL's for Dropbox, cloud storage, and other data storage arrangements, which indicates the attacker was taking and storing information. This information indicated that there was potential access to database, which stores the personal information for the insured's approximately 2,500 clients. The information accessed by the attacker included bank account information and, in limited circumstances, social security numbers.

Breach counsel were retained to oversee the forensics investigation and to draft notification letters to all of the Insured's approximately 2,500 clients. Notification vendor (AllClear ID) issued the letters, set up a call centre, and provided credit monitoring services on behalf of the Insured.
Breach counsel, forensics, and notification/credit monitoring costs were all covered under the policy. Costs incurred totalled approximately $100,000.

ASCENT™
UNDERWRITING

UNENCRYPTED LAPTOP

- Nurse's unencrypted laptop containing patient's medical records, explanation of benefits, social security numbers, dates of birth, and copies of checks is stolen
  - Breach counsel
  - Notification to affected individuals (within 30-60 days depending on jurisdiction)
    - Brief description of what happened, description of PHI involved, description of what is being done to investigate/mitigate breach, contact procedures for individuals to ask questions or learn additional information
  - Credit monitoring services

ASCENT™ UNDERWRITING

SESSION 3

RISK MANGEMENT AND PROTECTION

ASCENT™
UNDERWRITING

How we can help

PROACTIVE

ASCENT™
UNDERWRITING

VALUE ADDED PARTNERS

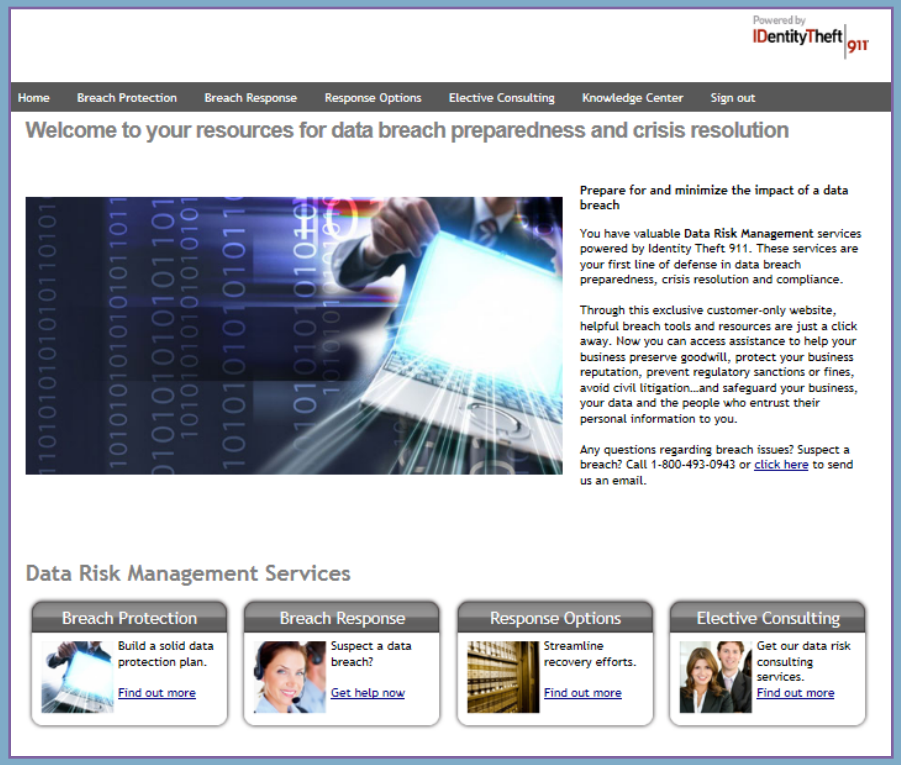
Founded in 2003, IDT911/CYBERSCOUT is the nation's premier consultative provider of identity and data risk management, resolution and education services.

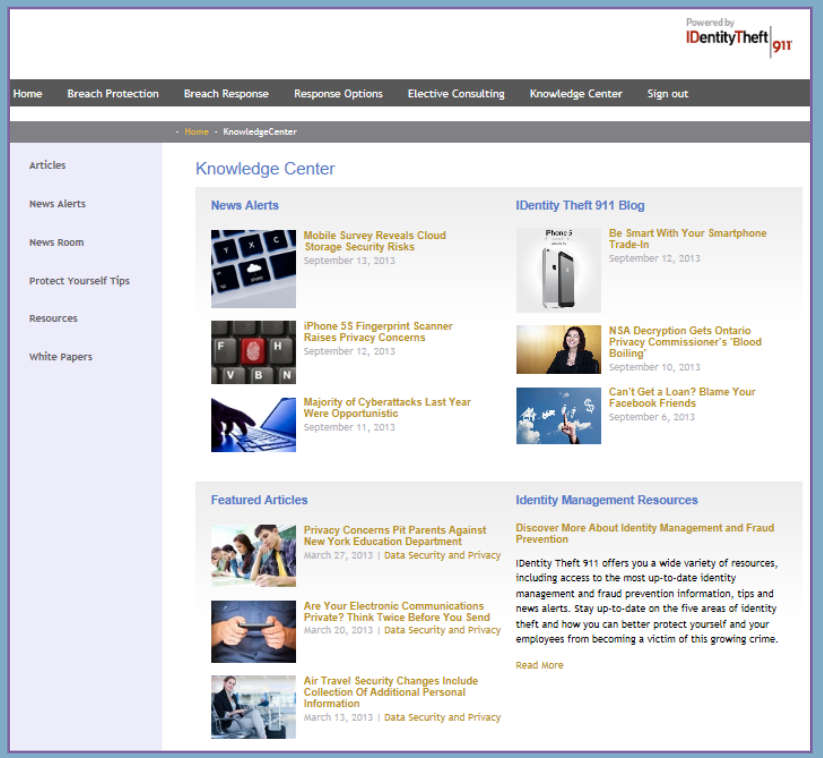
- Fraud resolution services are provided to more than **17.5 million households nationwide**
  - Nearly 45 million Americans
  - 15% of U.S. households
  - 45% of the P&C insurance marketplace
- More than **600,000 businesses** are helped by the data breach preparation and response services
- Partners with over **450 institutions**
- Insurance carriers, banks and financial institutions

ASCENT™
UNDERWRITING

Data Risk Management Website

- Services supported via a co-branded, secure website
- Includes a Knowledge Center





ASCENT™ UNDERWRITING

Breach Protection Services

Educational Resources

- Data protection tips
- Encryption guide
- Breach scenarios
- Knowledge Center

Data Breach Regulations

- US breach notification laws
- Third-party notification requirements

Customizable Templates

- Incident response plan
- Notification letter
- Call handling FAQs
- Helpline

ASCENT™ UNDERWRITING

BREACH RESPONSE SERVICES

Breach Counseling	• Determine if a privacy breach occurred • Assess severity of the event • Explain breach response requirements and best practices
Crisis Management	• Time-saving professional service to guide you in handling a breach • Work closely with policyholder and claims to outline an action plan • Public relations assistance to help restore your business' reputation
Notification Assistance	• Drafting and review service for creating notification letters • Support in drafting and delivering alternative forms of notification • Assistance in discussions with 3rd parties that need to be notified
Remediation Planning	• Service recommendations to impacted individuals such as call handling, monitoring products, and identity theft resolution services
Evidentiary Support	• Documentation of steps taken and remediation services provided to manage the privacy breach • Expert testimony witness if a claim goes to court

This image cannot currently be

How you can help

PREVENTATIVE

ASCENT™
UNDERWRITING

Ways You Can Help

- Guard against a data privacy loss incident with proactive measures that mitigate breach risks
- Offer a solution that delivers effective medical identity protection tools and swift resolution services
- Understand the details and ramifications of healthcare data breaches when they happen

ASCENT™
UNDERWRITING

Protecting Data

Utilize strong passwords and access controls on all computers, smart phones and network devices

Employ encryption (using built-in features and/or or enterprise solutions)

ASCENT™ UNDERWRITING

Protecting Data

Ensure policies prohibiting removal of unencrypted personal data and unsecured technologies are followed and enforced

Destroy or delete all paper and digital files once retention criteria is met

Destroy all equipment/device memory once taken out of service

ASCENT™
UNDERWRITING

PROTECTING DATA

Educate and train on data handling and privacy best practices to ensure a high awareness level

Consider the use of analytics to fight fraud. The volume and velocity of transactions passing through organizations today is too large and too fast for manual oversight.

ASCENT™
UNDERWRITING

TAKEAWAYS:

YOU WILL NEVER STOP BREACHES - BUT

- Guard against a data privacy loss incident with proactive measures that mitigate breach risks.
- Use the tools to educate yourself.
- If you suspect an incident occurred, be proactive, use our services to help assess and plan an appropriate response.
- You not in this alone! We are hear with all your partners to help you and help you minimize your risks.

ASCENT™
UNDERWRITING

THE SOLUTION

MODULAR CHOICE FORM

- Security and privacy liability
- Multimedia and IP
- Technology Services
- Network Interruption and Recovery
- Event Support Expenses
- Privacy Regulatory Defense & Penalties
- Network Extortion
- Electronic Theft, Computer Fraud & Telecoms Fraud
- Social Engineering Fraud
- Reputational Damage

ASCENT™
UNDERWRITING

COVERAGE

UNDERWRITING PROCESS

ASCENT™
UNDERWRITING

Questions / Concerns

ASCENT™
UNDERWRITING